Job Management Partner 1 Version 10

Job Management Partner 1/IT Desktop Management 2 Overview and System Design Guide

3021-3-368(E)

Notices

■ Relevant program products

P-2642-78AL Job Management Partner 1/IT Desktop Management 2 - Manager 10-50

The above product includes the following:

• P-CC2642-7AAL Job Management Partner 1/IT Desktop Management 2 - Manager (for Windows Server 2012, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003)

• P-CC2642-7BAL Job Management Partner 1/IT Desktop Management 2 - Agent (for Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003)

• P-CC2642-7CAL Job Management Partner 1/IT Desktop Management 2 - Network Monitor (for Windows 8.1 Enterprise, Windows 8.1 Pro, Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003 (x86))

• P-CC2642-7DAL Job Management Partner 1/IT Desktop Management 2 - Asset Console (for Windows Server 2012, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003)

■ Trademarks

Acrobat is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States and/or other countries.

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

Adobe and Flash Player are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Android is a trademark of Google Inc.in the United States, other countries, or both.

Citrix XenApp is a trademark of Citrix Systems, Inc.in the United States and/or other countries.

ESET and NOD32 are trademarks or registered trademarks of ESET spol. s r.o. or ESET North America.

F-Secure is a registered trademark of F-Secure Corporation in the United States.

Firefox is a registered trademark of the Mozilla Foundation.

Intel and vPro are trademarks of Intel Corporation in the U.S. and/or other countries.

Intel and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

Intel Core is a trademark of Intel Corporation in the U.S. and/or other countries.

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

Kaspersky is a registered trademark of Kaspersky Lab in the United States.

Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mac OS is a trademark of Apple Inc.

McAfee is a trademarks or a registered trademark of McAfee, Inc. in the United States and other countries.

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

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

Windows Media 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.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by IAIK of Graz University of Technology.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

RSA SECURED®

Job Management Partner1/IT Desktop Management 2 includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

HITACHI
Inspire the Next

Hitachi, Ltd.

Java™ COMPATIBLE ENTERPRISE EDITION

Java™ COMPATIBLE

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.

■ Issued

Apr. 2015: 3021-3-368(E)

■ Copyright

Preface

This manual provides an overview of Job Management Partner 1/IT Desktop Management 2 - Manager (abbreviated hereafter to JP1/IT Desktop Management 2). The manual also describes how to design a JP1/IT Desktop Management 2 system and explains the functions of the system.

Job Management Partner 1 is abbreviated in this manual as *JP1*.

■ Intended readers

This manual is intended for:

- Those who are considering installing JP1/IT Desktop Management 2 or who want to design JP1/IT Desktop Management 2 systems.
- Those who want to gain an overview of JP1/IT Desktop Management 2 products and function details

■ Organization of this manual

This manual is organized into the following chapters and appendixes:

1. Product Overview

   This chapter provides an overview of JP1/IT Desktop Management 2, and describes its system components.

2. Features of JP1/IT Desktop Management 2

   This chapter explains JP1/IT Desktop Management 2 functions.

3. About Product Licenses

   This chapter describes the product licenses of JP1/IT Desktop Management 2.

4. System Design

   This chapter provides an overview of how to design a system and start operation. This chapter also describes the issues that must be considered during system design.

Appendix A. Miscellaneous Information

This appendix provides reference information on using JP1/IT Desktop Management 2.

Appendix B. Glossary

This appendix explains terms used in JP1/IT Desktop Management 2.

Contents

1 Product Overview

JP1/IT Desktop Management 2 enables organizations to enforce security policies and manage IT assets. This chapter provides an overview of JP1/IT Desktop Management 2 and its system components.

1.1 Product overview

With information technology used so widely today, there is greater need for IT equipment that will help organizations to operate efficiently and reduce administrative costs. However, as information technology progresses, it is increasingly difficult to manage complex systems, to understand the operating status, detailed security settings and security procedures of all the devices. In this situation, the question of how to manage IT devices efficiently and accurately becomes all the more pressing.

JP1/IT Desktop Management 2 provides intuitive operations aligned to the task at hand, and automation functions based on simple settings and scheduling to support the security and asset management aspects of IT device management. Deploying JP1/IT Desktop Management 2 lessens the administrator's workload in managing a complex system and facilitates smooth running of the organization.

1.1.1 Product benefits

JP1/IT Desktop Management 2 provides a means of managing an organization's security infrastructure and assets. To manage device security in an organization, rules must be laid down and users required to comply. Administrators must keep track of security issues and respond appropriately.

JP1/IT Desktop Management 2 supports security and asset management as follows:

- Full picture of IT device status
- Enforcement of security rules for IT devices
- Identification and resolution of security vulnerabilities
- IT network monitoring
- Software installation and maintenance
- Remote control of user computers

Full picture of IT device status

To properly manage the security of IT devices, the administrator must first understand which devices are subject to security rules. To manage the devices as assets within the organization, the administrator must know what hardware and software is being used and how everything is currently configured. JP1/IT Desktop Management 2 has functionality to periodically search and discover devices in the network and collect information about them automatically. Information is acquired about any new device discovered in the search, allowing IT equipment to be managed using accurate, up-to-date information. This reduces the administrator's workload in data collection.

Enforcement of security rules for IT devices

One of the options for determining organizational security rules is an Information Security Management System (ISMS). To manage security under an ISMS, users must comply with rules relating to settings and operations. In JP1/IT Desktop Management 2, the rules determined by the organization are applied to IT devices as security policies, and degrees of compliance with those policies can be monitored. This allows rules to be enforced on the devices. If any computer violates a security policy, action can be taken or the offender sent a warning message automatically, relieving the administrator and senior staff from having to deal with users directly.

Identification and resolution of security vulnerabilities

To run an organization's computers securely, vulnerable computers must be identified and response measures quickly put in place to forestall virus infections and information leaks. Getting to the root of a problem by manually checking an array of measures, such as the computer's security settings, application of anti-virus products or Windows updates, and protection against information leaks can be extremely time-consuming and costly. With JP1/IT Desktop Management 2, you can check through a listing of the security status of each computer, and immediately spot any security issues. If there is a problem, the security of the whole system can be managed efficiently by automatically applying anti-virus products and Windows updates and isolating insecure devices from the network.

IT network monitoring

The widespread use of mobile computing poses the risk that people may bring their own computers into the organization. Connection of unauthorized equipment into the network can result in information leaks and virus infections. To prevent such damage, the organization's network is monitored so that newly connected devices are immediately discovered. JP1/IT Desktop Management 2 can check for unauthorized connections and automatically isolate any device that has no security provision. By using this network monitoring functionality, you can see all the network connections within the organization and better safeguard the system security.

Software installation and maintenance

For computer-based business tasks, the required software needs to be installed on the computers. This takes time if users have to do their own installations. Using JP1/IT Desktop Management 2, in a single operation you can install software on all the computers where it is required. Upgrades can be performed promptly, however frequently they are needed. Updated programs designed to fix a bug or correct a security issue can be distributed and applied automatically.

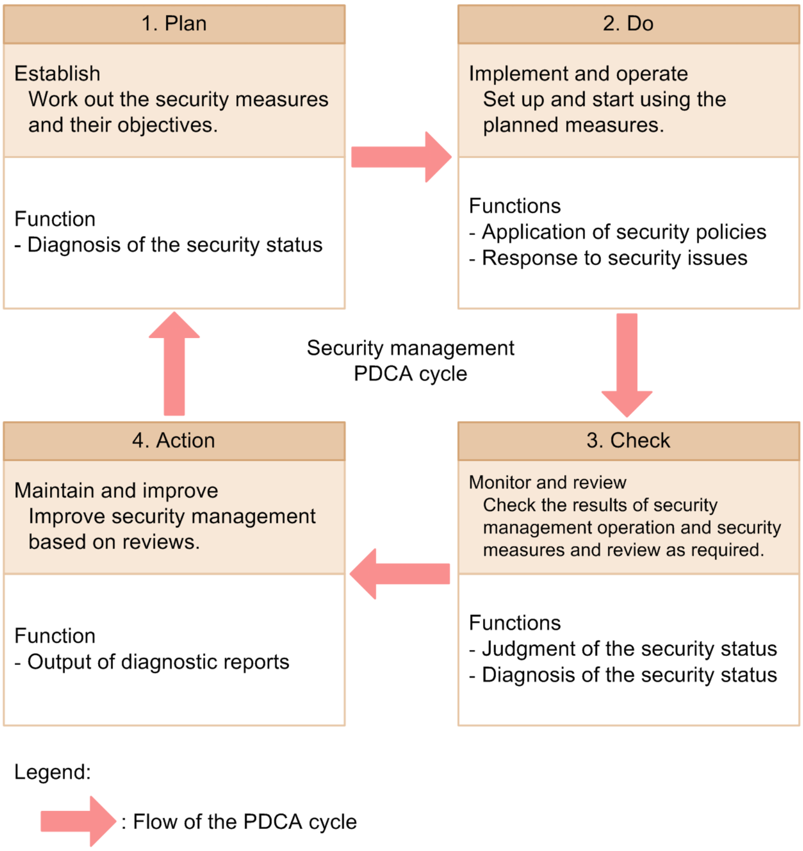
Remote control of user computers

With the rapid advance in information technology in recent years, users who are not equipped to set up applications or troubleshoot problems are increasingly common. To handle their computer problems, organizations typically rely on a system administrator with specialist knowledge. If workplaces are dispersed, it becomes difficult to respond in a timely manner. Using JP1/IT Desktop Management 2, when a problem occurs on a computer in another location, the system administrator can take immediate action from his or her own computer, enabling fast response by remote control.

1.1.2 Functionality to support security management using a PDCA cycle

ISMS recommends the PDCA cycle approach to run and improve a security management system. The functionality provided by JP1/IT Desktop Management 2 supports controls determined by the organization in each of the processes of a PDCA cycle for security management.

The following figure shows JP1/IT Desktop Management 2 functions and support for security management through the PDCA cycle.


1. Plan
Establish
Work out the security measures and their objectives.
Function
- Diagnosis of the security status
2. Do
Implement and operate
Set up and start using the planned measures.
Functions
- Application of security policies
- Response to security issues
Security management PDCA cycle
4. Action
Maintain and improve
Improve security management based on reviews.
Function
- Output of diagnostic reports
3. Check
Monitor and review
Check the results of security management operation and security measures and review as required.
Functions
- Judgment of the security status
- Diagnosis of the security status
Legend:
: Flow of the PDCA cycle

JP1/IT Desktop Management 2 operation (actions performed by the administrator) through the PDCA cycle for security management is as follows:

1. Plan: Establish

   Diagnose the security status of the computers in the organization using JP1/IT Desktop Management 2

   From the diagnostic results, evaluate the system security status and work out potential issues. From this evaluation, devise the organization's security rules and consider how to implement them.

2. Do: Implement and operate

   Set security policies and apply them to the computers using JP1/IT Desktop Management 2.

   If any computers with vulnerabilities are discovered, take measures using JP1/IT Desktop Management 2.

3. Check: Monitor and review

   Using JP1/IT Desktop Management 2, judge whether any device poses a security risk.

   Diagnose the system security from the results of this judgment process, using JP1/IT Desktop Management 2.

   From the diagnostic results, determine trends and identify unresolved issues.

4. Action: Maintain and improve

   Implement measures for identified issues.

   Using JP1/IT Desktop Management 2, output a security diagnostics report and review results.

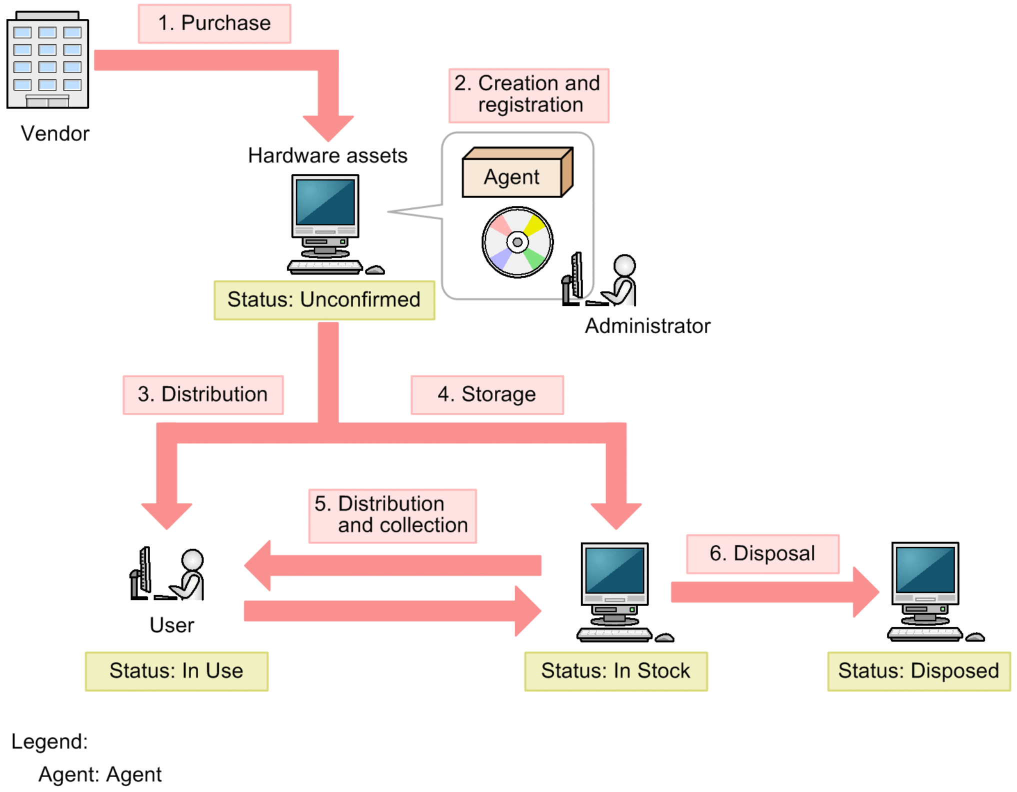
   Based on the review, plan how to improve the security rules in the next cycle.

1.1.3 Flow of asset management

JP1/IT Desktop Management 2 can collectively manage the IT resources in an organization (hardware assets and software licenses). Asset contracts can also be included.

From purchase to disposal of hardware assets

The following figure shows the flow from purchase to disposal of a hardware asset.



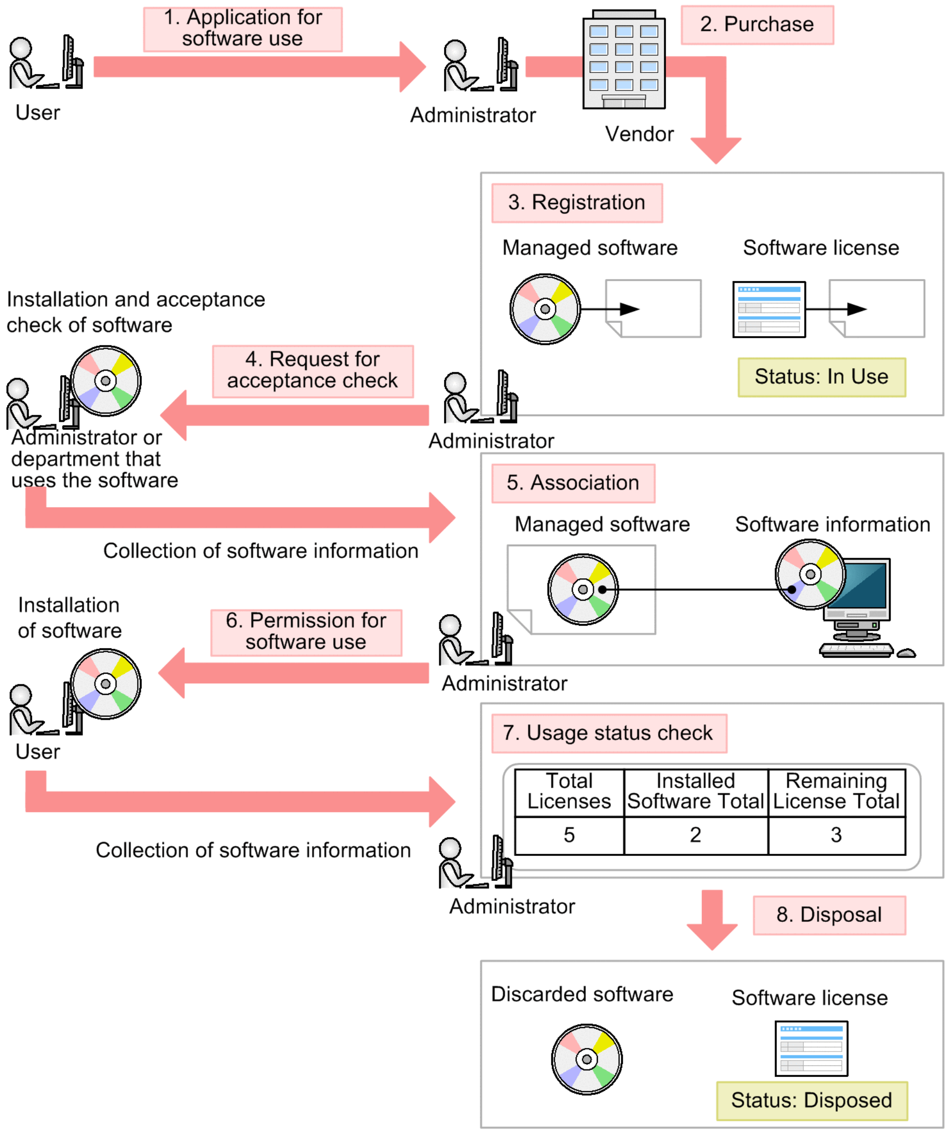
On purchasing a hardware asset, the administrator must build the hardware asset environment and register hardware asset information in JP1/IT Desktop Management 2. (steps 1 and 2)

The hardware asset is then delivered to the user or stored as stock if not immediately deployed. As the need arises for replacement or temporary use of hardware assets, stock may be distributed to users and items collected from users after use. The hardware asset information in JP1/IT Desktop Management 2 is updated accordingly. (steps 3 to 5)

When a hardware asset is no longer needed, it is disposed of and the hardware asset information in JP1/IT Desktop Management 2 is updated accordingly. (step 6)

From purchase to disposal of software assets

The following figure shows the flow from purchase to disposal of a software asset.



Total Licenses	Installed Software Total	Remaining License Total
5	2	3

When a user applies to use software, the request is checked and the software license is purchased. The administrator decides the software name (managed software name) under which usage of the purchased software will be managed, and registers the managed software information and license information in JP1/IT Desktop Management 2. (steps 1 to 3)

Before delivering the purchased software to the user, the administrator or department in which the software will be used performs the acceptance processing. If the software undergoing the acceptance process is installed on a computer managed by JP1/IT Desktop Management 2, software information will be acquired by the management server. The administrator then maps the collected software information with the managed software information. The administrator will then be able to view the installation status of the managed software from an operation window. Next, the administrator checks the user's application for software usage and grants approval. Once the software is installed, software information is acquired by the management server, allowing the administrator to keep track of software license usage from an operation window. (steps 4 to 6)

When the software is no longer needed, it is removed and eliminated. The software license information in JP1/IT Desktop Management 2 is updated accordingly. (steps 7 and 8)

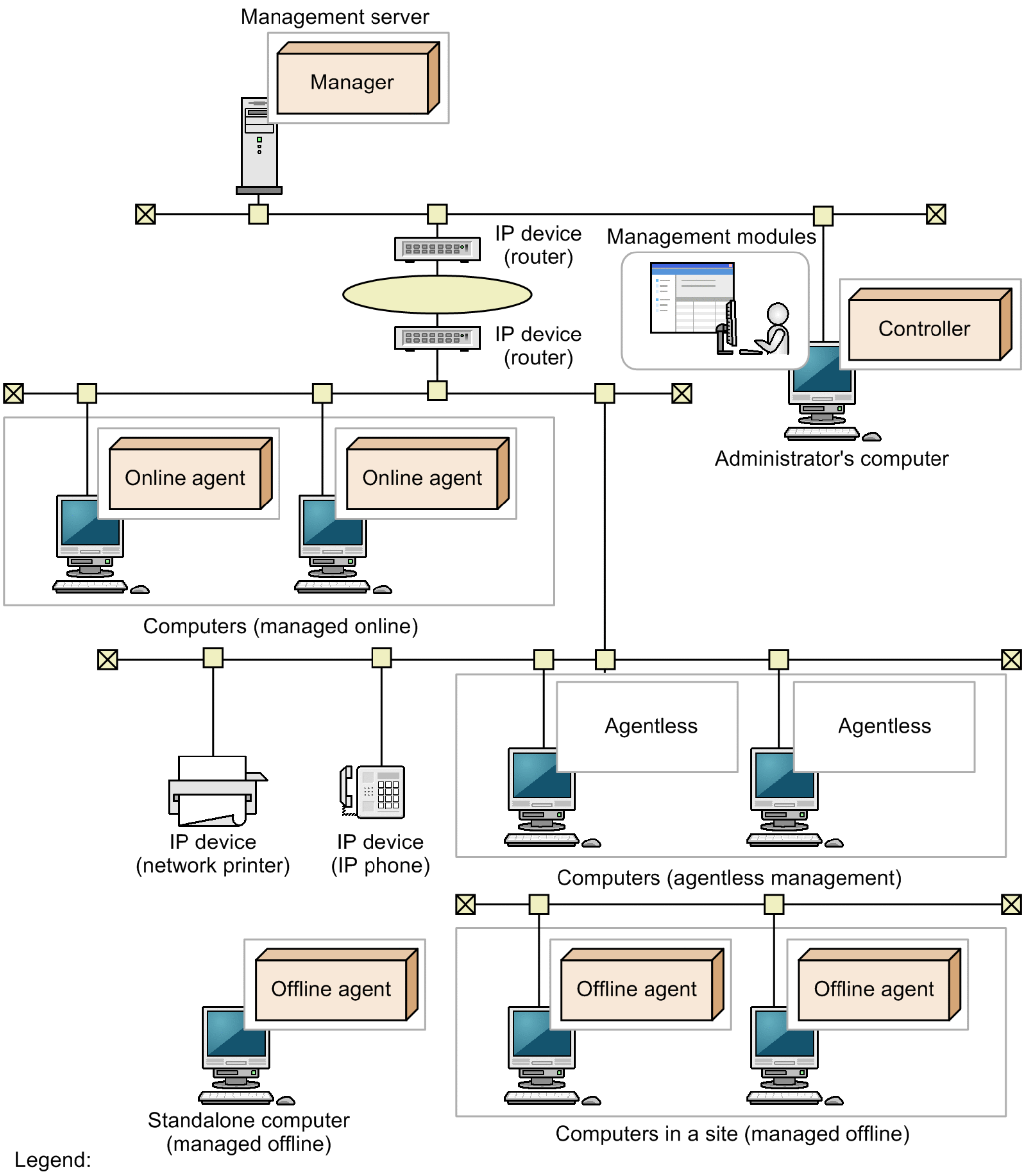
1.2 System components

In this manual, when referring to a system managed by JP1/IT Desktop Management 2, defined names are used for the system components such as network devices and the servers and computers on which JP1/IT Desktop Management 2 is installed.

Definitions used in JP1/IT Desktop Management 2 for basic system components are given in the following table.

Component name		Definition
Management server		The server on which JP1/IT Desktop Management 2 is installed as a relay system. A database for storing the various information managed by JP1/IT Desktop Management 2 is created on the management server. When distribution using Remote Installation Manager is described, this server might also be referred to as *distribution management system* or *manager*.
Administrator's computer		The computer on which the administrator performs management tasks using the JP1/IT Desktop Management 2 operation windows. JP1/IT Desktop Management 2 displays windows in a browser. This allows the administrator to work from any computer that can access the management server. The management server itself can be used as the administrator's computer. The administrator can download a program (controller) for remotely controlling computers from the operation windows and remotely control user computers. If you want to utilize distribution using Remote Installation Manager, Remote Install Manager must be installed,
Device	Computer	A computer on which an OS is installed. The types of computers are as follows: • A computer on which an agent is installed 　• A computer on which an agent for online management is installed (online managed computer) 　• A computer on which an agent for offline management is installed (offline managed computer) • A computer without any agent installed (agentless managed computer)
	IP device	A device other than a computer with an IP address. Examples include a router, network printer, or IP phone.
	Peripheral	A device without an IP address, such as a mouse, keyboard, or USB device.

The following figure shows an example of a basic system configuration consisting of these components and managed by JP1/IT Desktop Management 2.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Online agent: Agent for online management
Offline agent: Agent for offline management
Agentless: No agent installed

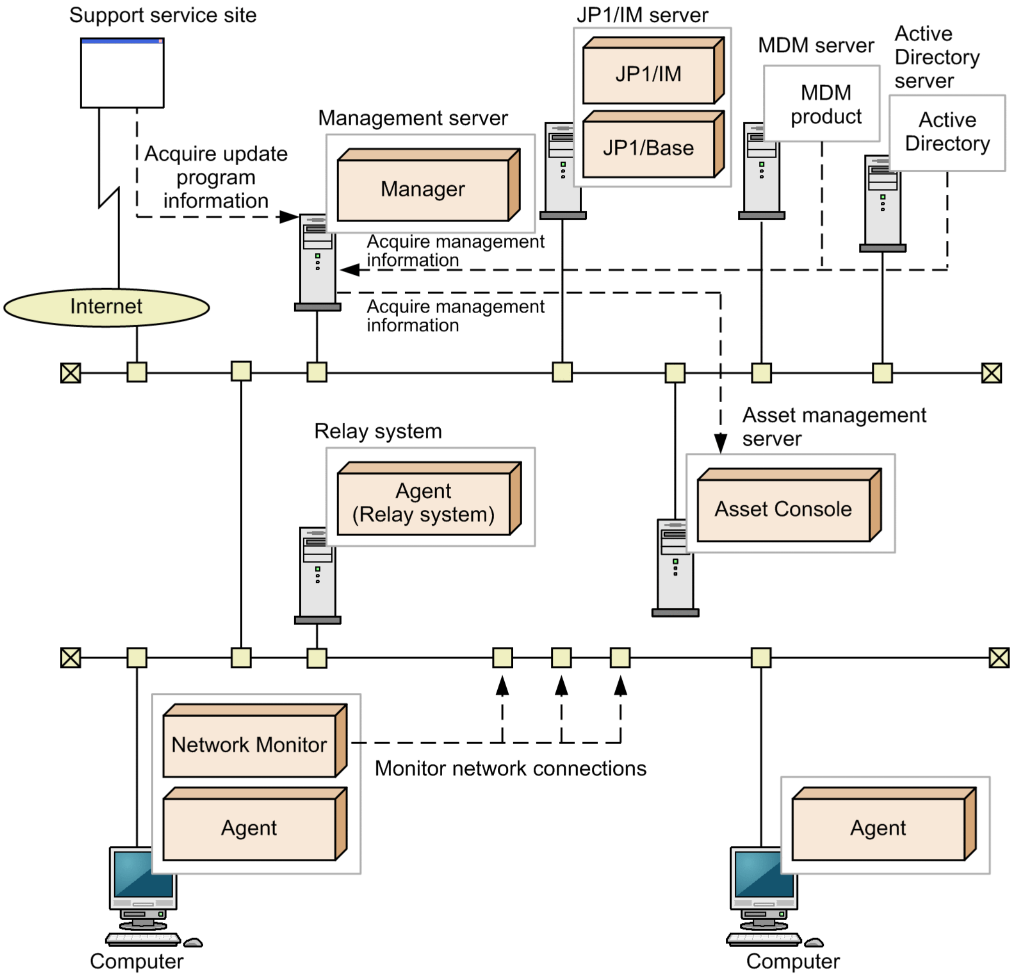
By adding another JP1/IT Desktop Management 2 component or linking JP1/IT Desktop Management 2 to another system, you can manage the system for a specific purpose, such as load balancing, enhanced security, or management of additional information.

Definitions of system components added for a specific purpose are given in the following table.

Component name	Definition
Relay system	A server on which JP1/IT Desktop Management 2 - Agent is installed. This server might also be called a *relaying system*. A relay system is installed when you utilize distribution using Remote Installation Manager. Installing a relay system can reduce loads on the Management server and network. A system that has a relay system is called a basic configuration system of JP1/IT Desktop Management 2.
Support service site	A website that provides support services. By connecting to this site via the Internet from JP1/IT Desktop Management 2, you can obtain information about the latest update programs. Based on

Component name	Definition
Support service site	this information, JP1/IT Desktop Management 2 determines whether the latest update programs installed on each computer are up to date. A system linked with a support service site is known as a *support service linkage configuration system*.
Asset management server	A server on which JP1/IT Desktop Management 2 - Asset Console (Asset Console) is installed. This server is installed when you want to perform detailed asset information management, including customizing an asset information search window, or performing an asset information management job using items.
Active Directory server	A server on which Active Directory is installed. The Active Directory program is required so that JP1/IT Desktop Management 2 can acquire information managed by Active Directory. A system linked with Active Directory is known as an *Active Directory linkage configuration system*.
MDM server	A server for managing smart devices using an installed MDM product. An MDM product is required so that JP1/IT Desktop Management 2JP1/IT Desktop Management 2 can acquire information about smart devices managed by the MDM product. A system linked with an MDM product is known as an *MDM linkage configuration system*.
Network monitoring agent	A JP1/IT Desktop Management 2 component for monitoring and controlling device network connections. The network monitoring agent is installed when a network monitor is enabled on an online managed computer. Once the agent is installed, JP1/IT Desktop Management 2 can monitor the network, detect connection by new devices and deny access. A network monitor-enabled system is known as a *network monitoring configuration system*.
Network control appliance	An appliance product on which JP1/NETM/NM is installed. By linking with JP1/NETM/NM - Manager, JP1/IT Desktop Management 2 can control the network connections monitored by a JP1/NETM/NM-installed appliance product. A system linked with JP1/NETM/NM - Manager is known as a *JP1/NETM/NM - Manager linkage configuration system*.
JP1/IM server	A server on which JP1/IM is installed for integrated monitoring of JP1 products and other programs. In addition to JP1/IT Desktop Management 2, the JP1/IM server requires JP1/IM and JP1/Base. Errors occurring on any of the managed computers can be centrally managed in JP1/IM as JP1 events. A system linked with JP1/IM is known as a *JP1/IM monitoring configuration system*.

The following figure shows an example of a purpose-built system configuration managed by JP1/IT Desktop Management 2.



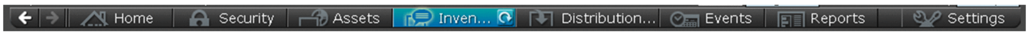
Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Agent (Relay system): JP1/IT Desktop Management 2 - Agent installed as a relay system
Agent: JP1/IT Desktop Management 2 - Agent installed as an agent
Network Monitor: Network monitor agent

For details about the system configuration, see 4.4 Examining the system configuration.

1.3 Program modules

In JP1/IT Desktop Management 2 you can access functions by clicking the buttons at the top and opening a different module. Choose the appropriate module for the operation you want to perform.



The operations you can perform in each module are described next.

Home module

In the Home module, you have an overview of the information managed by JP1/IT Desktop Management 2, presented in the panels. From each panel you can navigate to another module to perform a management operation.

Security module

In the Security module, you can allocate security policies to computers, manage their security status and take action if any computer poses a security risk. You can also investigate suspicious operations from the operation logs.

Assets module

In the Assets module, you can manage the status and stocktaking dates of hardware assets and software licenses, and keep track of costs by mapping this information against contract details. Assets in the organization can be presented as a listing, enabling efficient asset usage.

Device module

In the Device module, you can check device information and software information for a managed device, and perform operations on the device.

Distribution (ITDM-compatible) module

In the Distribution (ITDM-compatible) module, you can distribute and install required software on computers, and uninstall redundant software. Required files can be distributed as well as software.

Events module

In the Events module, you can check events that occurred during JP1/IT Desktop Management 2 operation.

Reports module

In the Reports module, you can view digest reports, security diagnostic reports, detailed security reports, detailed device reports, and detailed asset reports.

Settings module

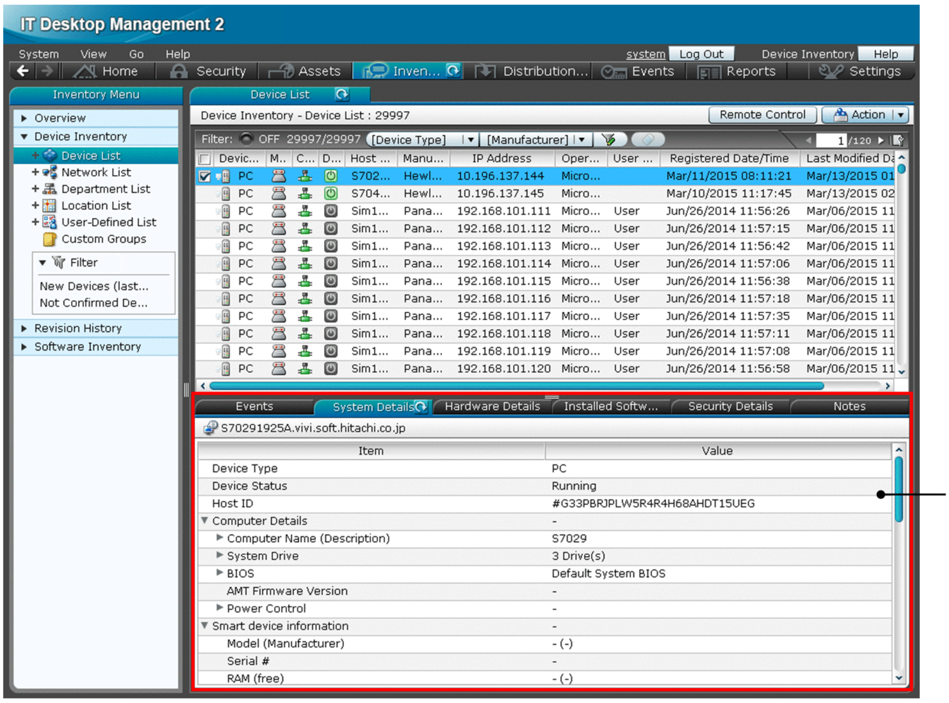
In the Settings module, you can customize JP1/IT Desktop Management 2 settings such as user account settings and agent configurations. You can also search for devices and distribute agents from this module.

Related Topics:

- 1.3.2 Working with the Home module
- 1.3.3 Working with the Security module
- 1.3.4 Working with the Assets module
- 1.3.5 Working with the Device module
- 1.3.6 Working with the Distribution (ITDM-compatible) module
- 1.3.7 Working with the Events module
- 1.3.8 Working with the Reports module
- 1.3.9 Working with the Settings module

1.3.1 Basic module layout

The following describes the basic layout of the JP1/IT Desktop Management 2 modules and the terminology used for the module components.



Device Inventory - Device List : 29997

Filter: OFF 29997/29997 [Device Type] [Manufacturer] 1/120

☐	Devic...	M..	C...	D...	Host ...	Manu...	IP Address	Oper...	User ...	Registered Date/Time	Last Modified Da
☑	PC				S702...	Hewl...	10.196.137.144	Micro...		Mar/11/2015 08:11:21	Mar/13/2015 01
	PC				S704...	Hewl...	10.196.137.145	Micro...		Mar/10/2015 11:17:45	Mar/13/2015 02
	PC				Sim1...	Pana...	192.168.101.111	Micro...	User	Jun/26/2014 11:56:26	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.112	Micro...	User	Jun/26/2014 11:57:15	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.113	Micro...	User	Jun/26/2014 11:56:42	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.114	Micro...	User	Jun/26/2014 11:57:06	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.115	Micro...	User	Jun/26/2014 11:56:38	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.116	Micro...	User	Jun/26/2014 11:57:18	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.117	Micro...	User	Jun/26/2014 11:57:35	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.118	Micro...	User	Jun/26/2014 11:57:11	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.119	Micro...	User	Jun/26/2014 11:57:08	Mar/06/2015 11
	PC				Sim1...	Pana...	192.168.101.120	Micro...	User	Jun/26/2014 11:56:58	Mar/06/2015 11

S70291925A.vivi.soft.hitachi.co.jp

Item	Value
Device Type	PC
Device Status	Running
Host ID	#G33PBRJPLW5R4R4H68AHDT15UEG
▼ Computer Details	-
▶ Computer Name (Description)	S7029
▶ System Drive	3 Drive(s)
▶ BIOS	Default System BIOS
AMT Firmware Version	-
▶ Power Control	-
▼ Smart device information	-
Model (Manufacturer)	- (-)
Serial #	-
RAM (free)	- (-)

Tabs

Menu area

Information area

Menu area

Menus are specific to the selected module. When you select an item here, corresponding information appears in the information area.

Information area

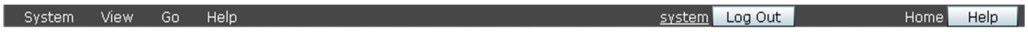
Displays information according to the item selected in the menu area.

Tabs

Tabs appear in the lower pane of the information area in the Security, Assets, Devices, and Distribution (ITDM-compatible) modules. Each tab shows detailed information relating to information selected in the upper pane.

Menu bar

The menus at the top of screen are common to all modules.



System

Logs the user out of JP1/IT Desktop Management 2.

View

Changes the panel layout, shows the display settings for the History back/forward buttons and check boxes, and initializes the display settings.

Go

Starts the **Getting Started** wizard and edits the user account of the logged-in user.

Help

Shows JP1/IT Desktop Management 2 help information, the module site map, related websites, and version information for each product.

Log Out button

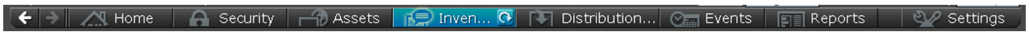
Logs the user out of JP1/IT Desktop Management 2. To the left of this button, the user ID of the logged-in user account appears. Click the user ID to edit your account information or change your password.

Help button

Describes the items in the open module and the operations you can perform from the module. To the left of this button, the name of the open module appears.

Buttons at the top of the window

These buttons allow you to access functions by switching to another module.

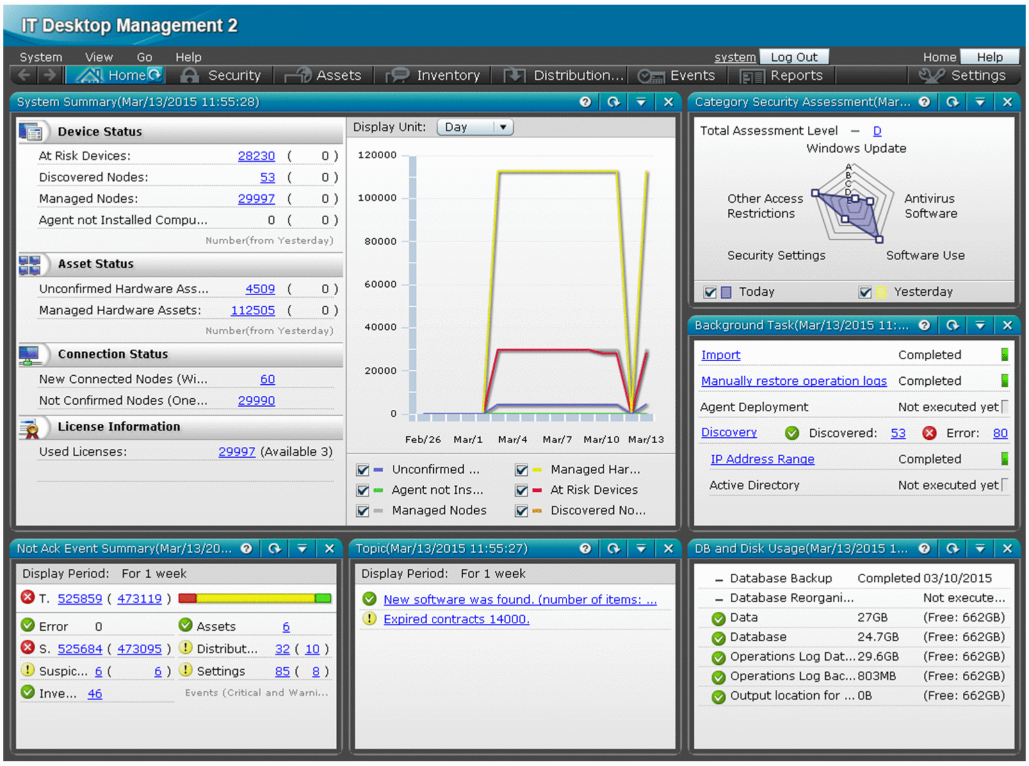


Related Topics:

- 1.3 Program modules

1.3.2 Working with the Home module

In the Home module, each of the panels presents an overview of information managed by JP1/IT Desktop Management 2. You can see the general situation relating to devices, assets, and product licenses, and check for events and notifications. You can also monitor device discoveries and asset importation, and check database and hard disk statuses.



System Summary(Mar/13/2015 11:55:28)

Device Status

At Risk Devices: 28230 (0)

Discovered Nodes: 53 (0)

Managed Nodes: 29997 (0)

Agent not Installed Compu... 0 (0)

Number(from Yesterday)

Asset Status

Unconfirmed Hardware Ass... 4509 (0)

Managed Hardware Assets: 112505 (0)

Number(from Yesterday)

Connection Status

New Connected Nodes (Wi... 60

Not Confirmed Nodes (One... 29990

License Information

Used Licenses: 29997 (Available 3)

Display Unit: Day

☑ Unconfirmed ... ☑ Managed Har...

☑ Agent not Ins... ☑ At Risk Devices

☑ Managed Nodes ☑ Discovered No...

Category Security Assessment(Mar...

Total Assessment Level – D

Windows Update

Other Access Restrictions

Antivirus Software

Security Settings

Software Use

☑ Today ☑ Yesterday

Background Task(Mar/13/2015 11:...

Import	Completed
Manually restore operation logs	Completed
Agent Deployment	Not executed yet
Discovery ✓ Discovered: 53 ✕ Error: 80	
IP Address Range	Completed
Active Directory	Not executed yet

Not Ack Event Summary(Mar/13/20...

Display Period: For 1 week

✕ T. 525859 (473119)

✓ Error 0 ✓ Assets 6

✕ S. 525684 (473095) ! Distribut... 32 (10)

! Suspic... 6 (6) ! Settings 85 (8)

✓ Inve... 46 Events (Critical and Warni...

Topic(Mar/13/2015 11:55:27)

Display Period: For 1 week

✓ New software was found. (number of items: ...

! Expired contracts 14000.

DB and Disk Usage(Mar/13/2015 1...

– Database Backup	Completed 03/10/2015	
– Database Reorgani...	Not execute...	
✓ Data	27GB	(Free: 662GB)
✓ Database	24.7GB	(Free: 662GB)
✓ Operations Log Dat...	29.6GB	(Free: 662GB)
✓ Operations Log Bac...	803MB	(Free: 662GB)
✓ Output location for ...	0B	(Free: 662GB)

Tip

You can rearrange the panels by drag-and-drop operation. To change the panels displayed in the Home module or their basic layout, select **Panel Layout** in the **View** menu at the top of the screen.

After viewing the general situation, from the link in each panel you can navigate to another module and begin management tasks.

Related Topics:

- 2.2.1 List of Panels

1.3.3 Working with the Security module

In the Security module, you can create security policies (security rules). Once you assign security policies to computers, you can manage security throughout the system and take action if any computer is insecure. You can also manage operation logs and investigate suspicious operations, and check whether Windows updates have been applied.

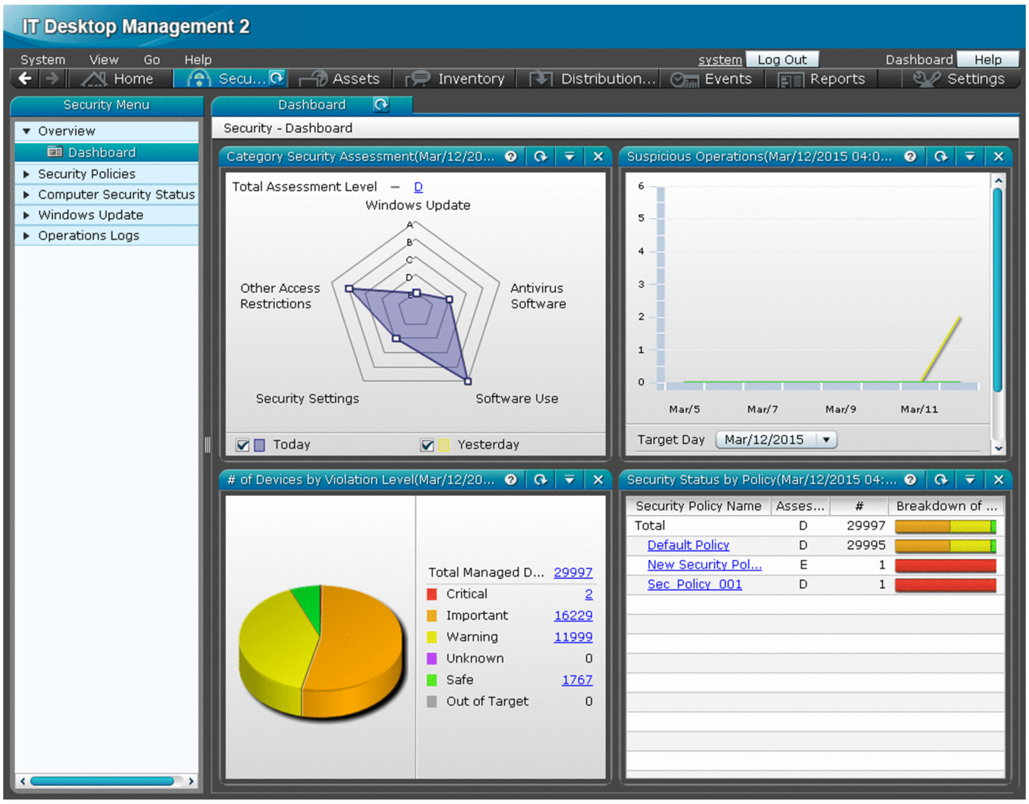
The Security module provides the following views:

- **Overview** view
- **Security Policies** view
- **Computer Security Status** view
- **Windows Update** view
- **Operation Logs** view

Each view is described next.

Overview view

The panels in this view provide a summary of the security of the managed computers in the organization.

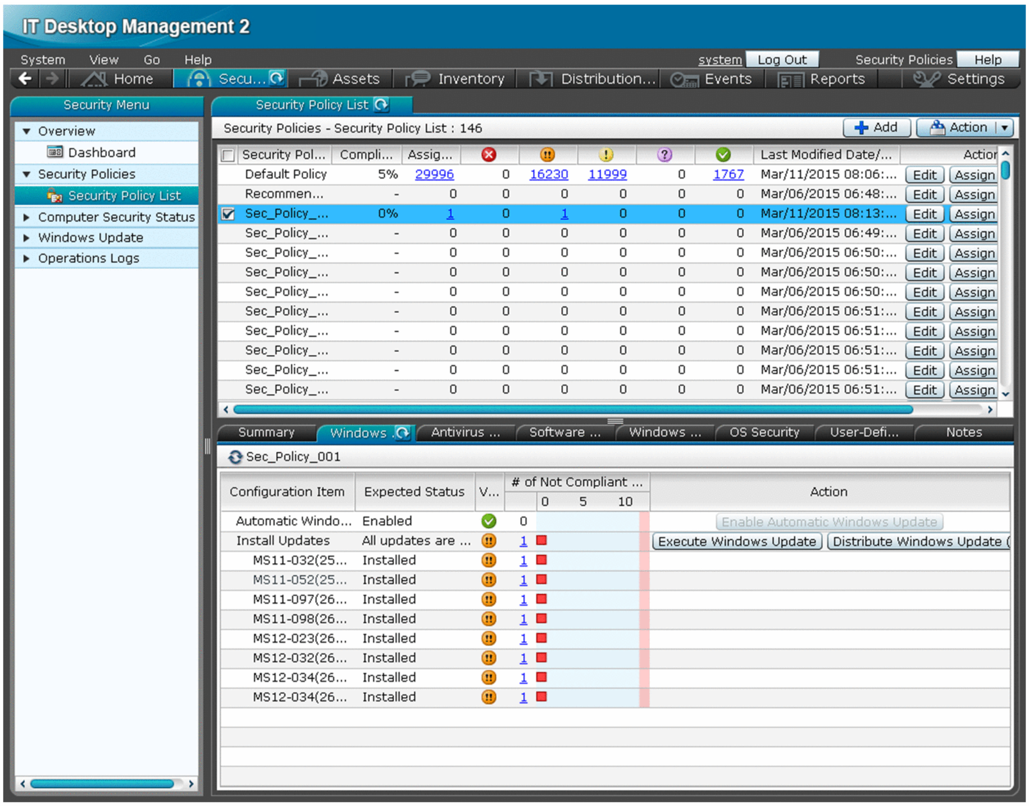

IT Desktop Management 2
System View Go Help
system Log Out Dashboard Help
Home Secu... Assets Inventory Distribution... Events Reports Settings
Security Menu
Overview
Dashboard
Security Policies
Computer Security Status
Windows Update
Operations Logs
Dashboard
Security - Dashboard
Category Security Assessment(Mar/12/20...
Total Assessment Level – D
Windows Update
A
B
C
D
Other Access Restrictions
Antivirus Software
Security Settings
Software Use
Today
Yesterday
Suspicious Operations(Mar/12/2015 04:0...
6
5
4
3
2
1
0
Mar/5
Mar/7
Mar/9
Mar/11
Target Day Mar/12/2015
# of Devices by Violation Level(Mar/12/20...
Security Status by Policy(Mar/12/2015 04:...

Total Managed D...	29997
🟥 Critical	2
🟧 Important	16229
🟨 Warning	11999
🟪 Unknown	0
🟩 Safe	1767
⬜ Out of Target	0

Security Policy Name	Asses...	#	Breakdown of ...
Total	D	29997	
Default Policy	D	29995	
New Security Pol...	E	1	
Sec_Policy_001	D	1	

Security Policies view

In this view you can create security policies and assign them to groups. By using computer policies you can manage the system security according to the assigned security rules.


IT Desktop Management 2
System View Go Help
system Log Out Security Policies Help
Home Secu... Assets Inventory Distribution... Events Reports Settings
Security Menu
Overview
Dashboard
Security Policies
Security Policy List
Computer Security Status
Windows Update
Operations Logs
Security Policy List
Add
Action
Summary Windows Antivirus ... Software ... Windows ... OS Security User-Defi... Notes

Security Policies - Security Policy List : 146

□	Security Pol...	Compli...	Assig...	✖	!!	!	?	✓	Last Modified Date/...	Actior
	Default Policy	5%	29996	0	16230	11999	0	1767	Mar/11/2015 08:06:...	Edit Assign
	Recommen...	-	0	0	0	0	0	0	Mar/06/2015 06:48:...	Edit Assign
☑	Sec_Policy_...	0%	1	0	1	0	0	0	Mar/11/2015 08:13:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:49:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:50:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:50:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:50:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:51:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:51:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:51:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:51:...	Edit Assign
	Sec_Policy_...	-	0	0	0	0	0	0	Mar/06/2015 06:51:...	Edit Assign

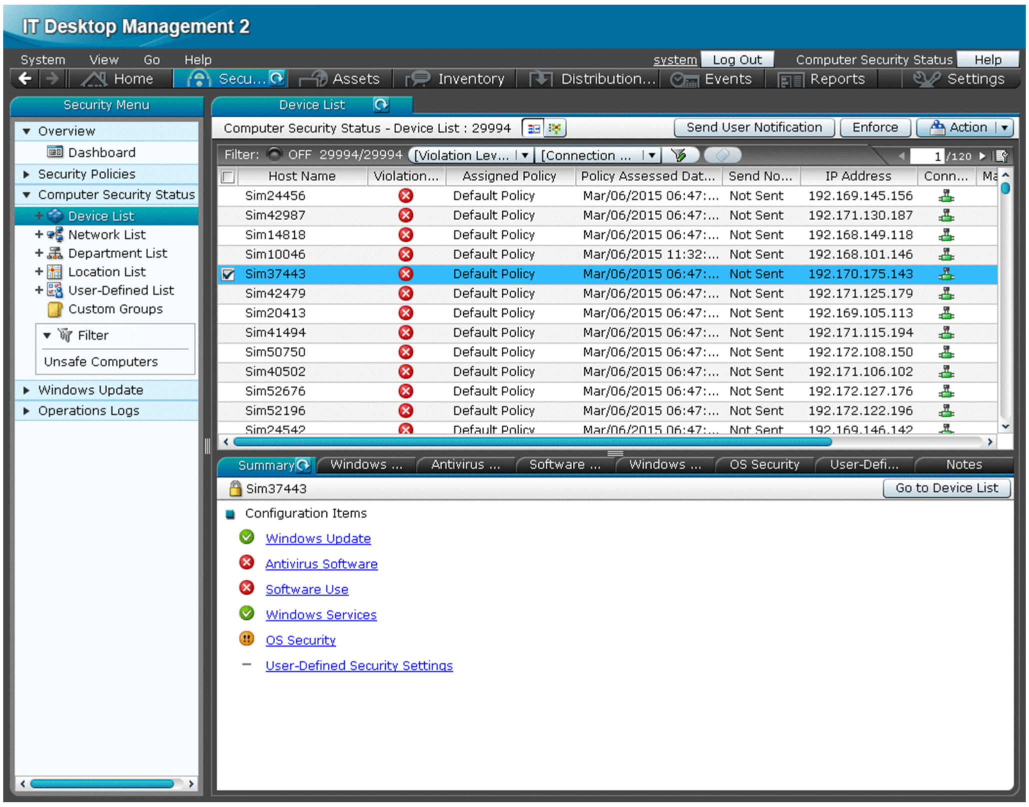
Sec_Policy_001

Configuration Item	Expected Status	V...	# of Not Compliant ...	Action
Automatic Windo...	Enabled	✓	0	Enable Automatic Windows Update
Install Updates	All updates are ...	!!	1 🟥	Execute Windows Update Distribute Windows Update (
MS11-032(25...	Installed	!!	1 🟥	
MS11-052(25...	Installed	!!	1 🟥	
MS11-097(26...	Installed	!!	1 🟥	
MS11-098(26...	Installed	!!	1 🟥	
MS12-023(26...	Installed	!!	1 🟥	
MS12-032(26...	Installed	!!	1 🟥	
MS12-034(26...	Installed	!!	1 🟥	
MS12-034(26...	Installed	!!	1 🟥	

Details about compliance with the security policy you select in the upper pane of the information area is shown in the tabs in the lower pane. You can check compliance with each security setting and take measures if any device has violated the security policy.

Computer Security Status view

In this view you can check the security of each computer, and send the user a message or enforce security measures if a computer violates the security policy. You can also assign security policies to individual computers.



Computer Security Status - Device List : 29994

□	Host Name	Violation...	Assigned Policy	Policy Assessed Dat...	Send No...	IP Address	Conn...	Ma
	Sim24456	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.169.145.156		
	Sim42987	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.171.130.187		
	Sim14818	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.168.149.118		
	Sim10046	☒	Default Policy	Mar/06/2015 11:32:...	Not Sent	192.168.101.146		
☑	Sim37443	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.170.175.143		
	Sim42479	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.171.125.179		
	Sim20413	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.169.105.113		
	Sim41494	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.171.115.194		
	Sim50750	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.172.108.150		
	Sim40502	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.171.106.102		
	Sim52676	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.172.127.176		
	Sim52196	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.172.122.196		
	Sim24542	☒	Default Policy	Mar/06/2015 06:47:...	Not Sent	192.169.146.142		

Sim37443

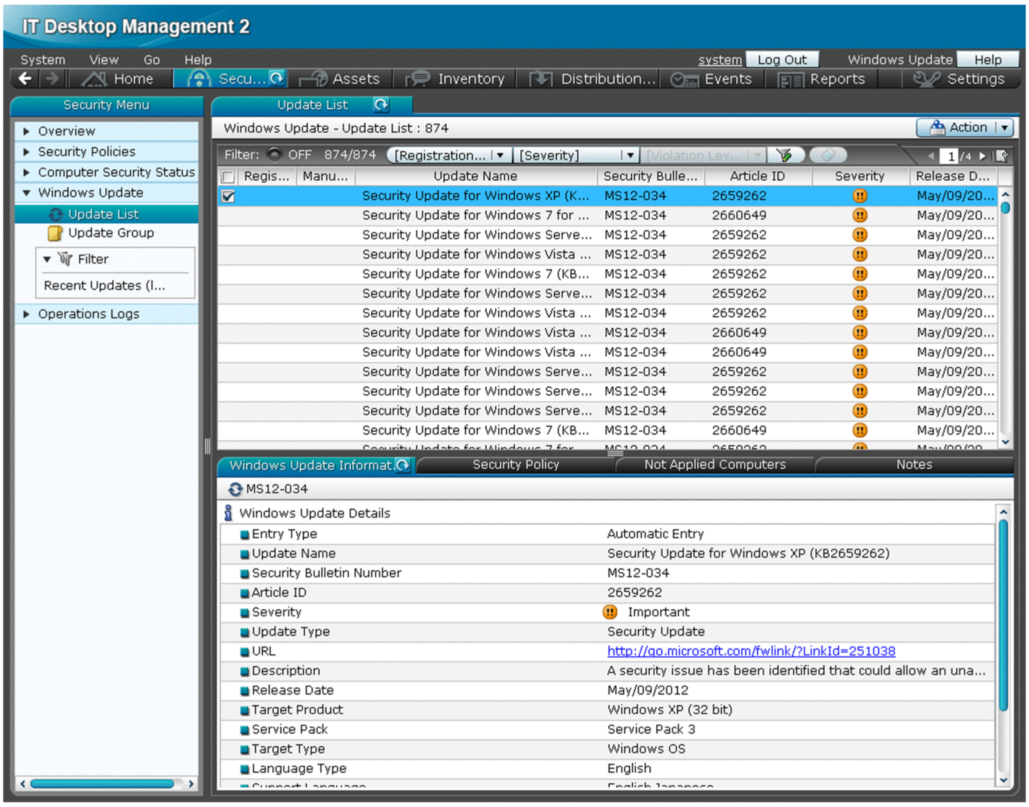
Configuration Items

- ✓ Windows Update
- ☒ Antivirus Software
- ☒ Software Use
- ✓ Windows Services
- ! OS Security
- – User-Defined Security Settings

Security compliance for the computer you select in the upper pane of the information area is shown in the tabs in the lower pane. You can check the computer's compliance with each security setting.

Windows Update view

In this view you can check whether Windows updates have been applied to computers. You can also manage the Windows updates that are required under the particular security policy and automatically distribute and apply Windows updates that have not been implemented.



Windows Update - Update List : 874

□	Regis...	Manu...	Update Name	Security Bulle...	Article ID	Severity	Release D...
☑			Security Update for Windows XP (K...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows 7 for ...	MS12-034	2660649	!!	May/09/20...
			Security Update for Windows Serve...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Vista ...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows 7 (KB...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Serve...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Vista ...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Vista ...	MS12-034	2660649	!!	May/09/20...
			Security Update for Windows Vista ...	MS12-034	2660649	!!	May/09/20...
			Security Update for Windows Serve...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Serve...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Serve...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows 7 (KB...	MS12-034	2660649	!!	May/09/20...

MS12-034

Windows Update Details

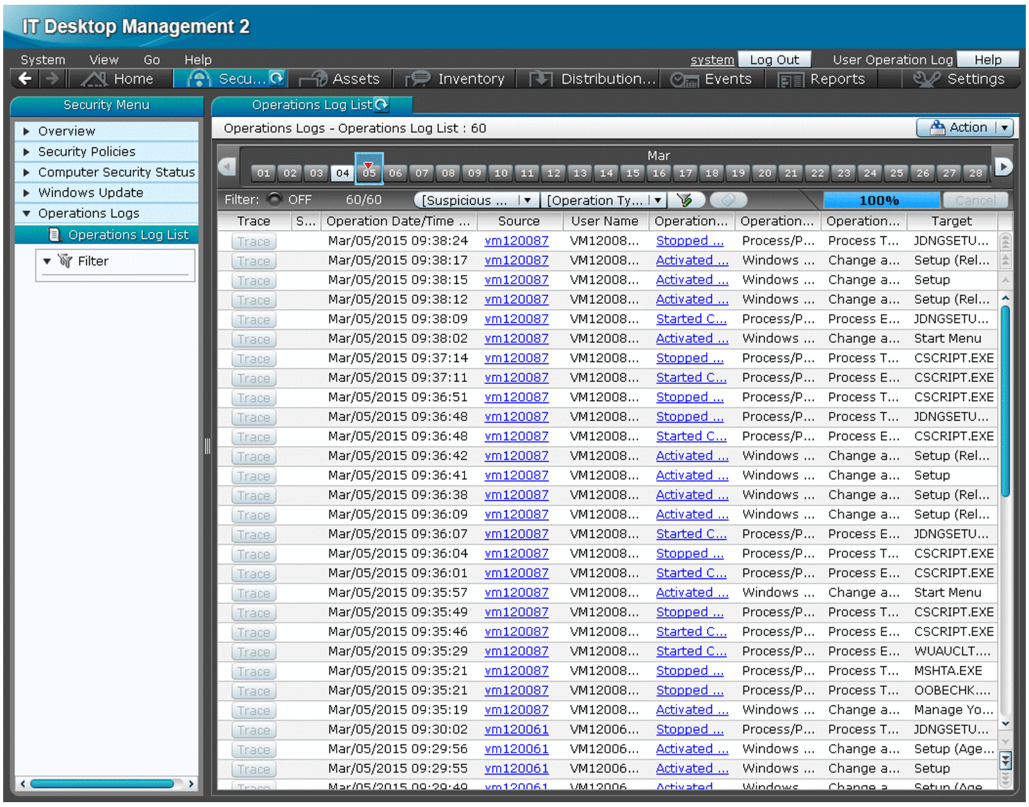
Entry Type	Automatic Entry
Update Name	Security Update for Windows XP (KB2659262)
Security Bulletin Number	MS12-034
Article ID	2659262
Severity	!! Important
Update Type	Security Update
URL	http://go.microsoft.com/fwlink/?LinkId=251038
Description	A security issue has been identified that could allow an una...
Release Date	May/09/2012
Target Product	Windows XP (32 bit)
Service Pack	Service Pack 3
Target Type	Windows OS
Language Type	English

Information about the Windows update you select in the upper pane of the information area is shown in the tabs in the lower pane. You can check whether the update is built into the security policy and identify computers where updates have not been applied.

Operation Logs view

In this view you can check the operation logs collected on the management server.

You can view a listing of operation logs and investigate suspicious operations. You can track file movements to and from the system and identify the computers involved, enabling early detection and response to information leaks.



Operations Logs - Operations Log List : 60

Trace	S...	Operation Date/Time ...	Source	User Name	Operation...	Operation...	Operation...	Target
Trace		Mar/05/2015 09:38:24	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	JDNGSETU...
Trace		Mar/05/2015 09:38:17	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup (Rel...
Trace		Mar/05/2015 09:38:15	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup
Trace		Mar/05/2015 09:38:12	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup (Rel...
Trace		Mar/05/2015 09:38:09	vm120087	VM12008...	Started C...	Process/P...	Process E...	JDNGSETU...
Trace		Mar/05/2015 09:38:02	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Start Menu
Trace		Mar/05/2015 09:37:14	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	CSCRIPT.EXE
Trace		Mar/05/2015 09:37:11	vm120087	VM12008...	Started C...	Process/P...	Process E...	CSCRIPT.EXE
Trace		Mar/05/2015 09:36:51	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	CSCRIPT.EXE
Trace		Mar/05/2015 09:36:48	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	JDNGSETU...
Trace		Mar/05/2015 09:36:48	vm120087	VM12008...	Started C...	Process/P...	Process E...	CSCRIPT.EXE
Trace		Mar/05/2015 09:36:42	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup (Rel...
Trace		Mar/05/2015 09:36:41	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup
Trace		Mar/05/2015 09:36:38	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup (Rel...
Trace		Mar/05/2015 09:36:09	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Setup (Rel...
Trace		Mar/05/2015 09:36:07	vm120087	VM12008...	Started C...	Process/P...	Process E...	JDNGSETU...
Trace		Mar/05/2015 09:36:04	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	CSCRIPT.EXE
Trace		Mar/05/2015 09:36:01	vm120087	VM12008...	Started C...	Process/P...	Process E...	CSCRIPT.EXE
Trace		Mar/05/2015 09:35:57	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Start Menu
Trace		Mar/05/2015 09:35:49	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	CSCRIPT.EXE
Trace		Mar/05/2015 09:35:46	vm120087	VM12008...	Started C...	Process/P...	Process E...	CSCRIPT.EXE
Trace		Mar/05/2015 09:35:29	vm120087	VM12008...	Started C...	Process/P...	Process E...	WUAUCLT....
Trace		Mar/05/2015 09:35:21	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	MSHTA.EXE
Trace		Mar/05/2015 09:35:21	vm120087	VM12008...	Stopped ...	Process/P...	Process T...	OOBECHK....
Trace		Mar/05/2015 09:35:19	vm120087	VM12008...	Activated ...	Windows ...	Change a...	Manage Yo...
Trace		Mar/05/2015 09:30:02	vm120061	VM12006...	Stopped ...	Process/P...	Process T...	JDNGSETU...
Trace		Mar/05/2015 09:29:56	vm120061	VM12006...	Activated ...	Windows ...	Change a...	Setup (Age...
Trace		Mar/05/2015 09:29:55	vm120061	VM12006...	Activated ...	Windows ...	Change a...	Setup
Trace		Mar/05/2015 09:29:49	vm120061	VM12006...	Activated	Windows	Change a	Setup (Age

This view appears only if operation logs are being acquired on the management server.

1.3.4 Working with the Assets module

In the Assets module, you can collectively manage the devices, software licenses, contracts and so on managed in the organization. You can manage each type of asset in listings like a ledger. By defining relationships among asset information, you can immediately see what contracts are linked to devices and how software licenses are being used, helping to perform asset management tasks more efficiently.

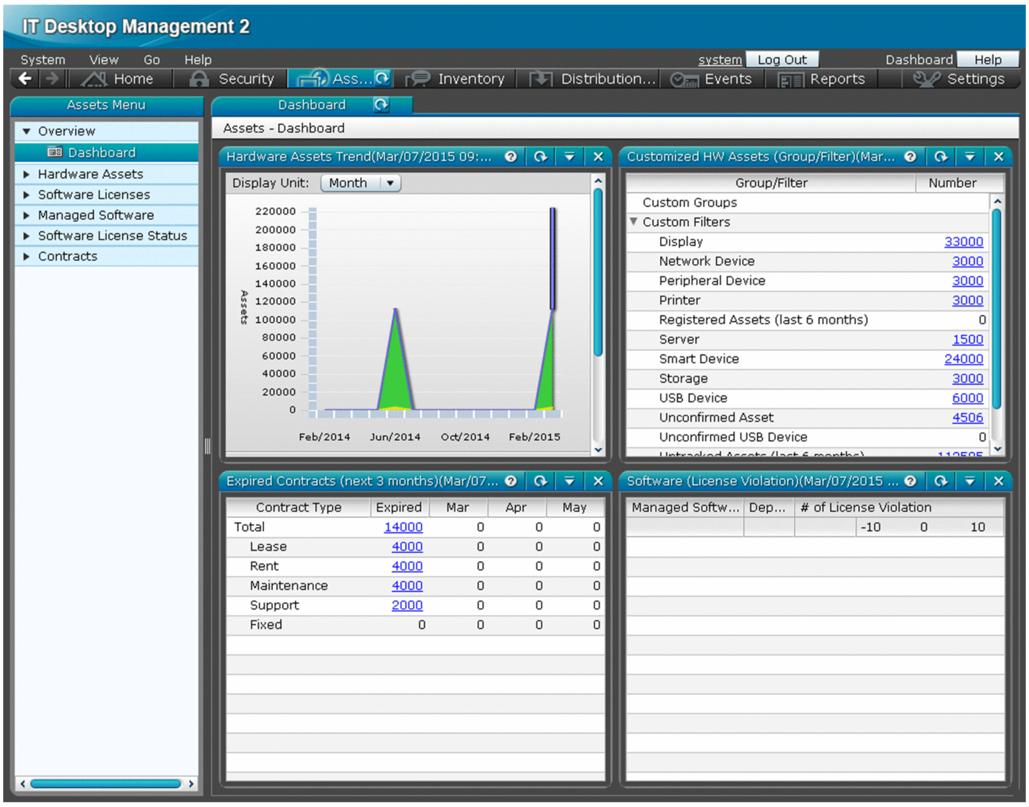
The Assets module provides the following views:

- **Overview** view
- **Hardware Assets** view
- **Software Licenses** view
- **Managed Software** view
- **Software License Status** view
- **Contracts** view

Each view is described next.

Overview view

The panels in this view provide a summary of the asset information managed by JP1/IT Desktop Management 2.



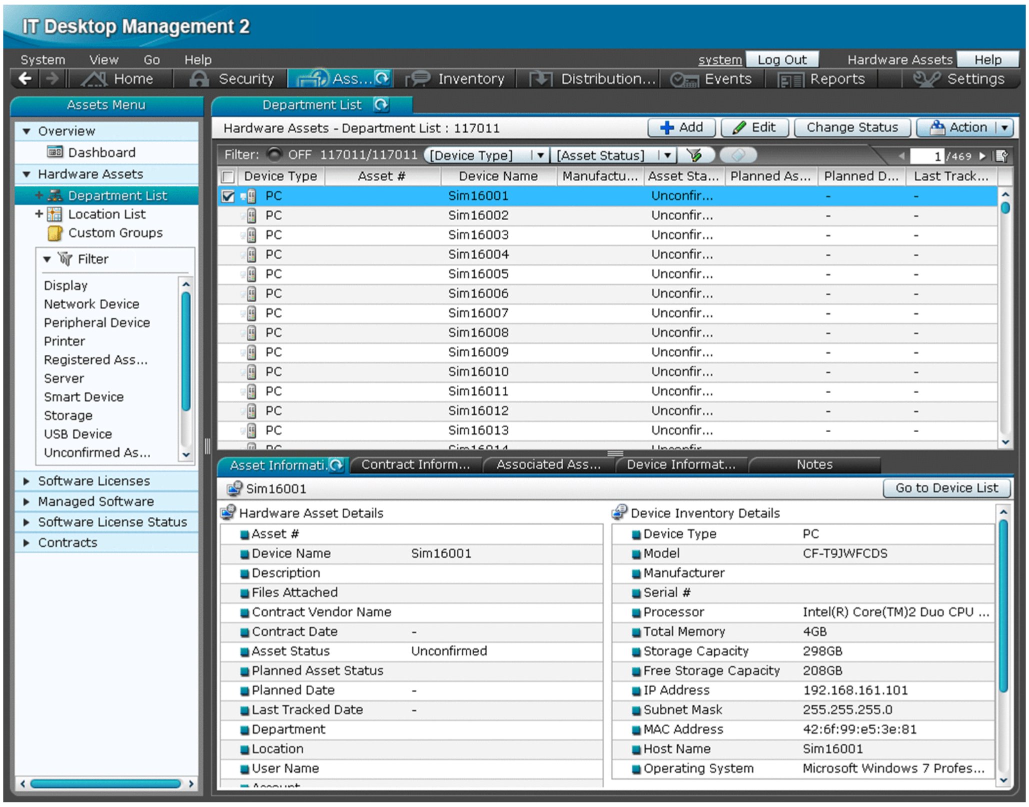
Group/Filter	Number
Custom Groups	
▼ Custom Filters	
Display	33000
Network Device	3000
Peripheral Device	3000
Printer	3000
Registered Assets (last 6 months)	0
Server	1500
Smart Device	24000
Storage	3000
USB Device	6000
Unconfirmed Asset	4506
Unconfirmed USB Device	0
Untracked Assets (last 6 months)	112505

Contract Type	Expired	Mar	Apr	May
Total	14000	0	0	0
Lease	4000	0	0	0
Rent	4000	0	0	0
Maintenance	4000	0	0	0
Support	2000	0	0	0
Fixed	0	0	0	0

Managed Softw...	Dep...	# of License Violation		
		-10	0	10

Hardware Assets view

In this view you can manage information about hardware assets in the organization such as computers, printers, and networking equipment. You can also map this information against contract details. By defining these relationships, you can immediately see the contract cost and contract period of hardware contracts.



Hardware Assets - Department List : 117011

□	Device Type	Asset #	Device Name	Manufactu...	Asset Sta...	Planned As...	Planned D...	Last Track...
☑	PC		Sim16001		Unconfir...		-	-
□	PC		Sim16002		Unconfir...		-	-
□	PC		Sim16003		Unconfir...		-	-
□	PC		Sim16004		Unconfir...		-	-
□	PC		Sim16005		Unconfir...		-	-
□	PC		Sim16006		Unconfir...		-	-
□	PC		Sim16007		Unconfir...		-	-
□	PC		Sim16008		Unconfir...		-	-
□	PC		Sim16009		Unconfir...		-	-
□	PC		Sim16010		Unconfir...		-	-
□	PC		Sim16011		Unconfir...		-	-
□	PC		Sim16012		Unconfir...		-	-
□	PC		Sim16013		Unconfir...		-	-

Sim16001

Hardware Asset Details

Asset #	
Device Name	Sim16001
Description	
Files Attached	
Contract Vendor Name	
Contract Date	-
Asset Status	Unconfirmed
Planned Asset Status	
Planned Date	-
Last Tracked Date	-
Department	
Location	
User Name	

Device Inventory Details

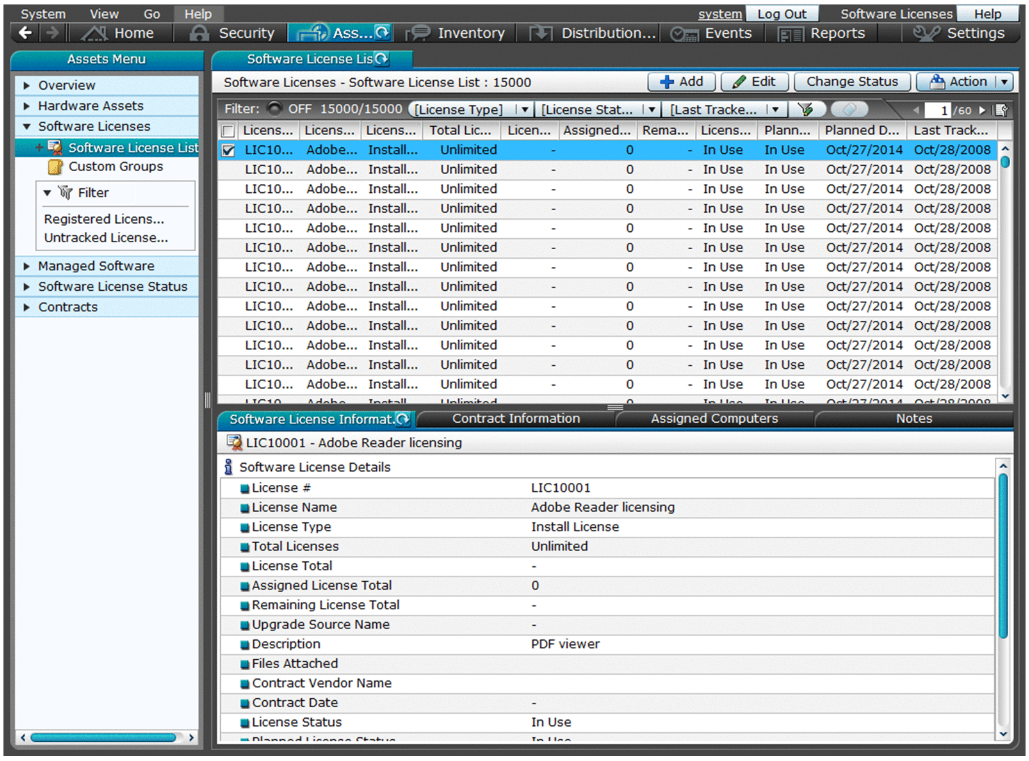
Device Type	PC
Model	CF-T9JWFCDS
Manufacturer	
Serial #	
Processor	Intel(R) Core(TM)2 Duo CPU ...
Total Memory	4GB
Storage Capacity	298GB
Free Storage Capacity	208GB
IP Address	192.168.161.101
Subnet Mask	255.255.255.0
MAC Address	42:6f:99:e5:3e:81
Host Name	Sim16001
Operating System	Microsoft Windows 7 Profes...

Details about the hardware assets selected in the upper pane of the information area is shown in the tabs in the lower pane. You can check the contracts associated with a hardware asset, related assets, associated devices, and other information.

When hardware asset information is mapped against device information, the **Device Information** area is updated automatically whenever new device information is collected.

Software Licenses view

In this view you can manage information about software licenses your organization has purchased. You can also give users permission to use a particular software product by assigning a software license to a computer.



Software Licenses - Software License List : 15000

□	Licens...	Licens...	Licens...	Total Lic...	Licen...	Assigned...	Rema...	Licens...	Plann...	Planned D...	Last Track...
☑	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008

LIC10001 - Adobe Reader licensing

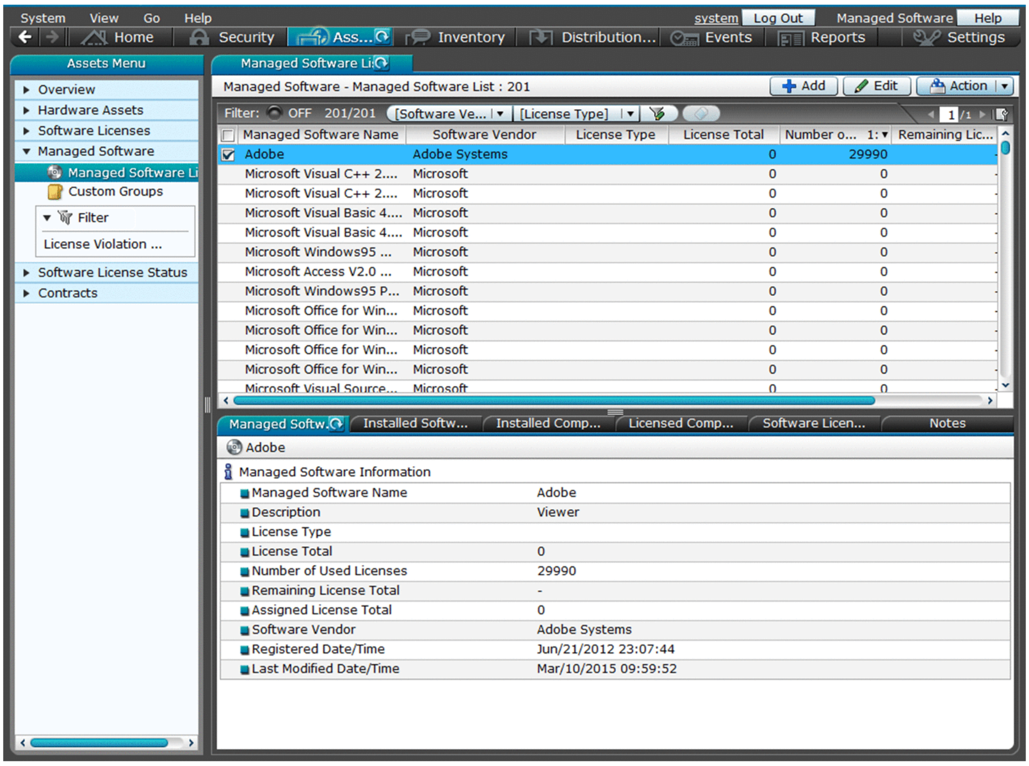
Software License Details

License #	LIC10001
License Name	Adobe Reader licensing
License Type	Install License
Total Licenses	Unlimited
License Total	-
Assigned License Total	0
Remaining License Total	-
Upgrade Source Name	-
Description	PDF viewer
Files Attached	
Contract Vendor Name	
Contract Date	-
License Status	In Use

Details about the software licenses assets selected in the upper pane of the information area is shown in the tabs in the lower pane. You can check the contract period for a software license, see which computers are allocated a particular license, and so on.

Managed Software view

In this view you can manage information about managed software (software for which JP1/IT Desktop Management 2 keeps track of licenses). By registering managed software, the system is able to keep track of the number of software licenses that are in use, providing a clear picture of how software is being used. If you also register software license information, the system can keep track of the number of software licenses purchased for each piece of managed software, and see how many of those licenses are in use. This makes you aware of the managed software for which you have too few licenses, and those for which you have a surplus.



Managed Software - Managed Software List : 201

Filter: OFF 201/201 [Software Ve...] [License Type] 1/1

	Managed Software Name	Software Vendor	License Type	License Total	Number o... 1:▾	Remaining Lic...
☑	Adobe	Adobe Systems		0	29990	-
	Microsoft Visual C++ 2....	Microsoft		0	0	-
	Microsoft Visual C++ 2....	Microsoft		0	0	-
	Microsoft Visual Basic 4....	Microsoft		0	0	-
	Microsoft Visual Basic 4....	Microsoft		0	0	-
	Microsoft Windows95 ...	Microsoft		0	0	-
	Microsoft Access V2.0 ...	Microsoft		0	0	-
	Microsoft Windows95 P...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Visual Source...	Microsoft		0	0	-

Adobe

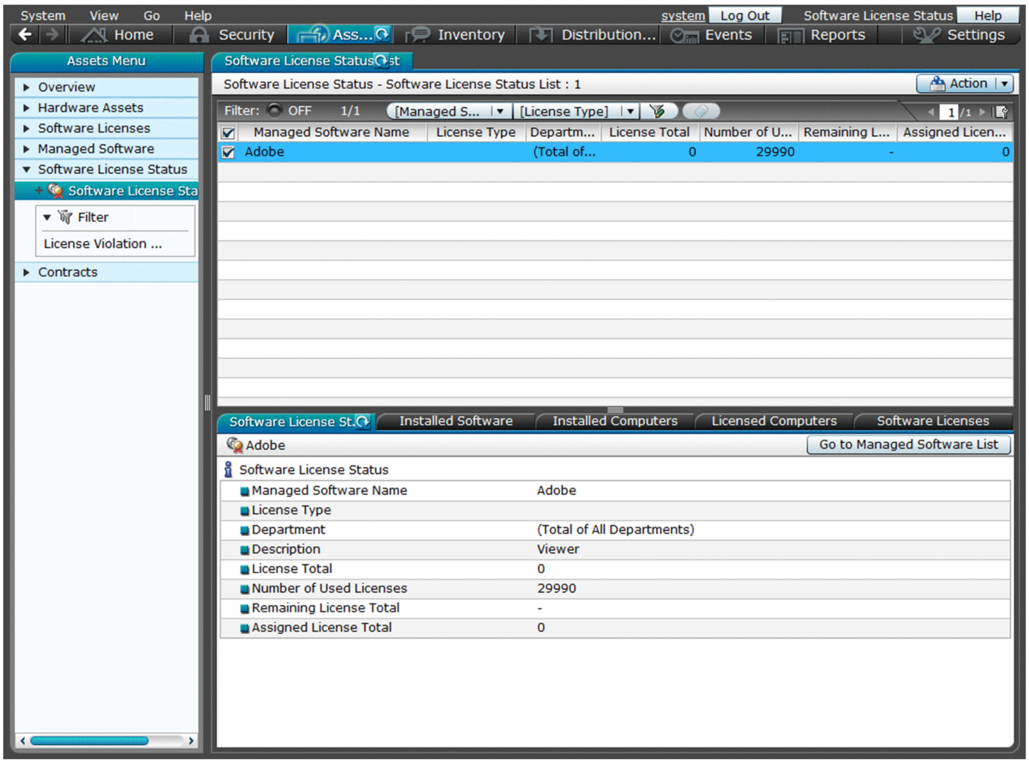
Managed Software Information

Managed Software Name	Adobe
Description	Viewer
License Type	
License Total	0
Number of Used Licenses	29990
Remaining License Total	-
Assigned License Total	0
Software Vendor	Adobe Systems
Registered Date/Time	Jun/21/2012 23:07:44
Last Modified Date/Time	Mar/10/2015 09:59:52

Details about the managed software selected in the upper pane of the information area is shown in the tabs in the lower pane. You can view a list of computers with the software installed, computers allocated a software license, software licenses associated with the software, and other information.

Software License Status view

In this view you can check the usage of software licenses for each managed software product. This view shows the number of owned software licenses, the number of remaining software licenses, and other information by license type and by department. This makes you aware of the managed software products that have too few licenses, and those that have excess licenses.



Software License Status - Software License Status List : 1

Filter: OFF 1/1 [Managed S...] [License Type] 1/1

☑	Managed Software Name	License Type	Departm...	License Total	Number of U...	Remaining L...	Assigned Licen...
☑	Adobe		(Total of...	0	29990	-	0

Adobe

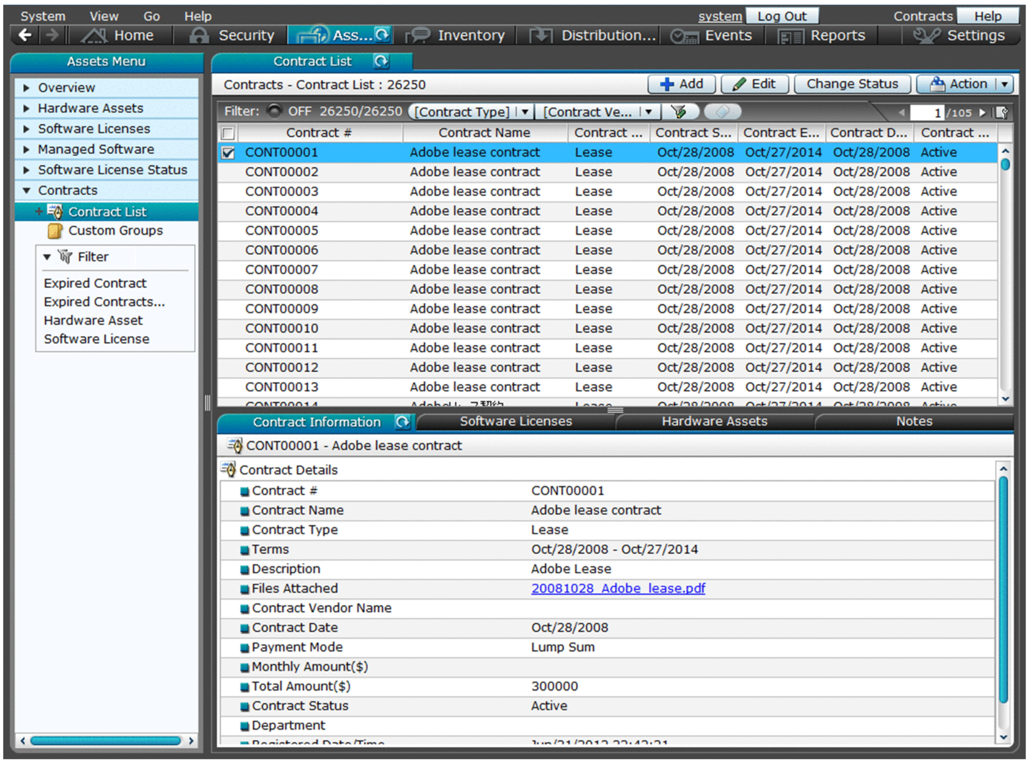
Software License Status

Managed Software Name	Adobe
License Type	
Department	(Total of All Departments)
Description	Viewer
License Total	0
Number of Used Licenses	29990
Remaining License Total	-
Assigned License Total	0

Details about the managed software selected in the upper pane of the information area is shown in the tabs in the lower pane. You can view a list of computers with the software installed, computers allocated a software license, software licenses associated with the software, and other information.

Contracts view

In this view you can manage contract information in relation to hardware assets and software licenses. By adding contract information, you can gain a clear picture of the costs and contract periods associated with asset contracts.



Contracts - Contract List : 26250

Filter: OFF 26250/26250 [Contract Type] [Contract Ve... 1 /105

	Contract #	Contract Name	Contract ...	Contract S...	Contract E...	Contract D...	Contract ...
☑	CONT00001	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00002	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00003	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00004	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00005	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00006	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00007	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00008	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00009	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00010	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00011	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00012	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00013	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active

CONT00001 - Adobe lease contract

Contract Details

Contract #	CONT00001
Contract Name	Adobe lease contract
Contract Type	Lease
Terms	Oct/28/2008 - Oct/27/2014
Description	Adobe Lease
Files Attached	20081028_Adobe_lease.pdf
Contract Vendor Name	
Contract Date	Oct/28/2008
Payment Mode	Lump Sum
Monthly Amount($)	
Total Amount($)	300000
Contract Status	Active
Department	

Details about the contract selected in the upper pane of the information area is shown in the tabs in the lower pane. You can check the software licenses, hardware assets, and other items associated with the selected contract.

1.3.5 Working with the Device module

In the Device module, you can check the current status of managed devices by viewing device information, installed software information, and other information. If the agent is installed on a computer, you can turn the computer on or off from the Device module and send messages to the user.

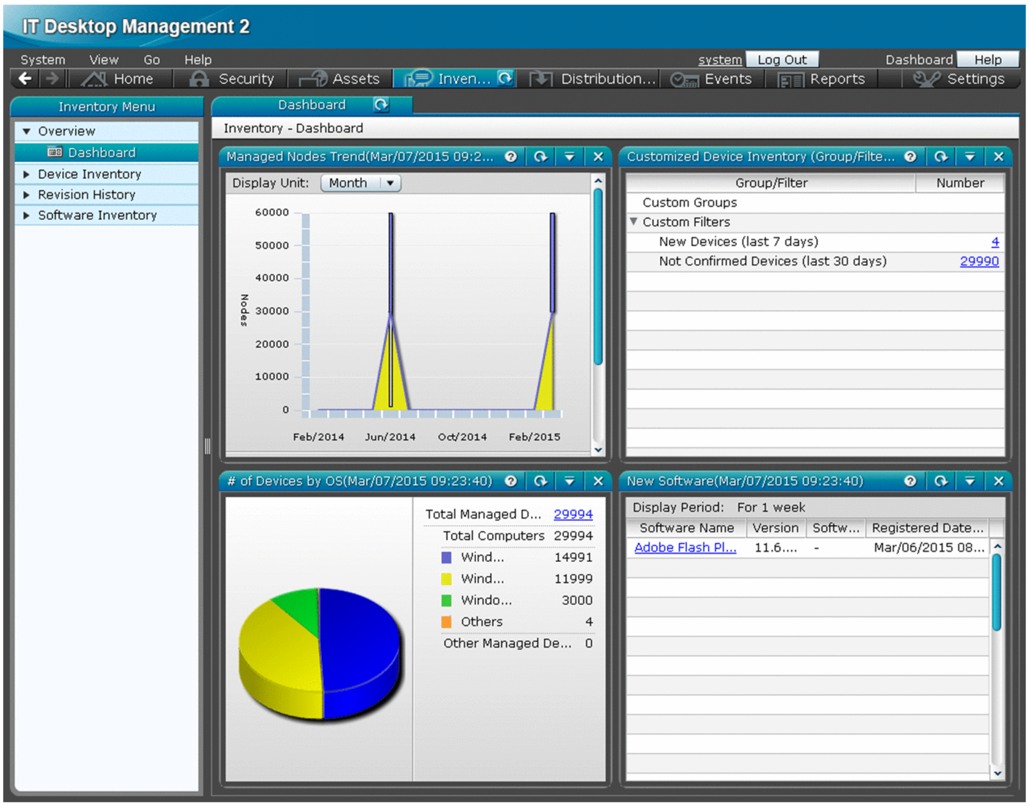
The Device module provides the following views:

- **Overview** view
- **Device Inventory** view
- **Revision History** view
- **Software Inventory** view

Each view is described next.

Overview view

The panels in this view provide a summary of the devices and software managed by JP1/IT Desktop Management 2.


IT Desktop Management 2
System View Go Help
system Log Out Dashboard Help
Home Security Assets Inven... Distribution... Events Reports Settings
Inventory Menu
Overview
Dashboard
Device Inventory
Revision History
Software Inventory
Dashboard
Inventory - Dashboard
Managed Nodes Trend(Mar/07/2015 09:2...
Display Unit: Month
60000
50000
40000
30000
20000
10000
0
Nodes
Feb/2014
Jun/2014
Oct/2014
Feb/2015
Customized Device Inventory (Group/Filte...
# of Devices by OS(Mar/07/2015 09:23:40)
New Software(Mar/07/2015 09:23:40)

Group/Filter	Number
Custom Groups	
▼ Custom Filters	
New Devices (last 7 days)	4
Not Confirmed Devices (last 30 days)	29990

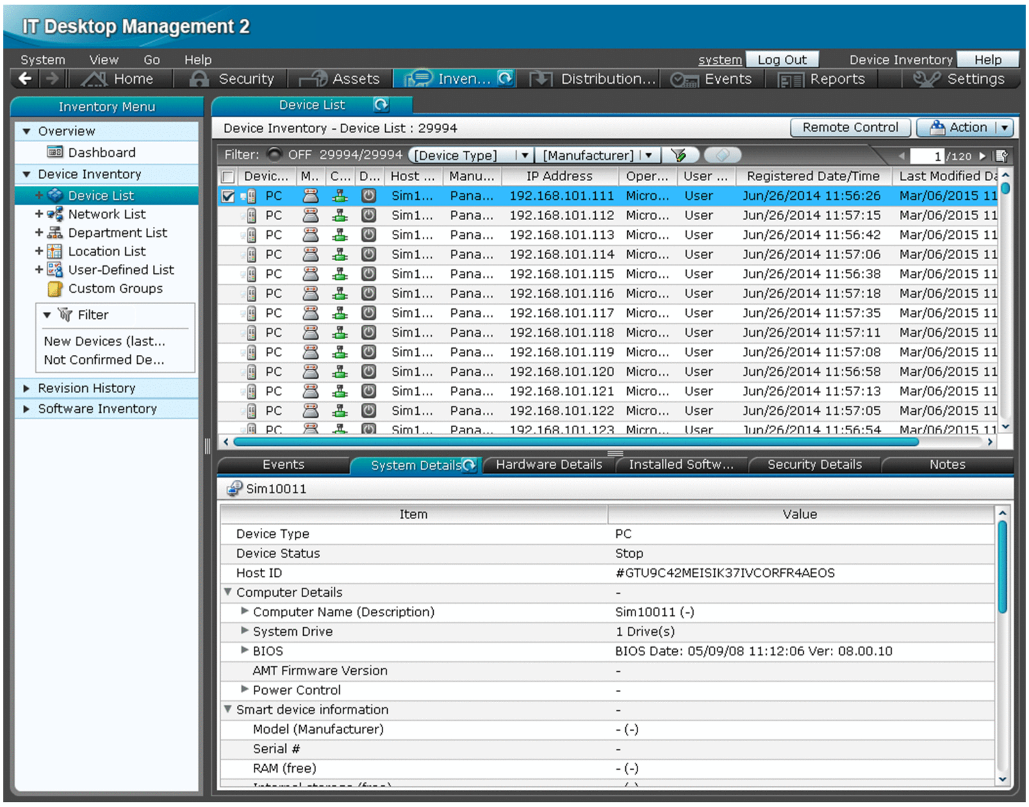
Total Managed D...	29994
Total Computers	29994
🟦 Wind...	14991
🟨 Wind...	11999
🟩 Windo...	3000
🟧 Others	4
Other Managed De...	0

Display Period: For 1 week

Software Name	Version	Softw...	Registered Date...
Adobe Flash Pl...	11.6....	-	Mar/06/2015 08...

Device Inventory view

In this view, you can view information about managed devices, check whether a device is on or off, and so on. You can also perform operations on managed devices, such as sending messages to users, turning computers on and off, and controlling computers remotely.



Device Inventory - Device List : 29994

Filter: OFF 29994/29994 [Device Type] [Manufacturer] 1 /120

Devic...	M..	C...	D...	Host ...	Manu...	IP Address	Oper...	User ...	Registered Date/Time	Last Modified Da
☑ PC				Sim1...	Pana...	192.168.101.111	Micro...	User	Jun/26/2014 11:56:26	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.112	Micro...	User	Jun/26/2014 11:57:15	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.113	Micro...	User	Jun/26/2014 11:56:42	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.114	Micro...	User	Jun/26/2014 11:57:06	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.115	Micro...	User	Jun/26/2014 11:56:38	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.116	Micro...	User	Jun/26/2014 11:57:18	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.117	Micro...	User	Jun/26/2014 11:57:35	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.118	Micro...	User	Jun/26/2014 11:57:11	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.119	Micro...	User	Jun/26/2014 11:57:08	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.120	Micro...	User	Jun/26/2014 11:56:58	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.121	Micro...	User	Jun/26/2014 11:57:13	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.122	Micro...	User	Jun/26/2014 11:57:05	Mar/06/2015 11
PC				Sim1...	Pana...	192.168.101.123	Micro...	User	Jun/26/2014 11:56:54	Mar/06/2015 11

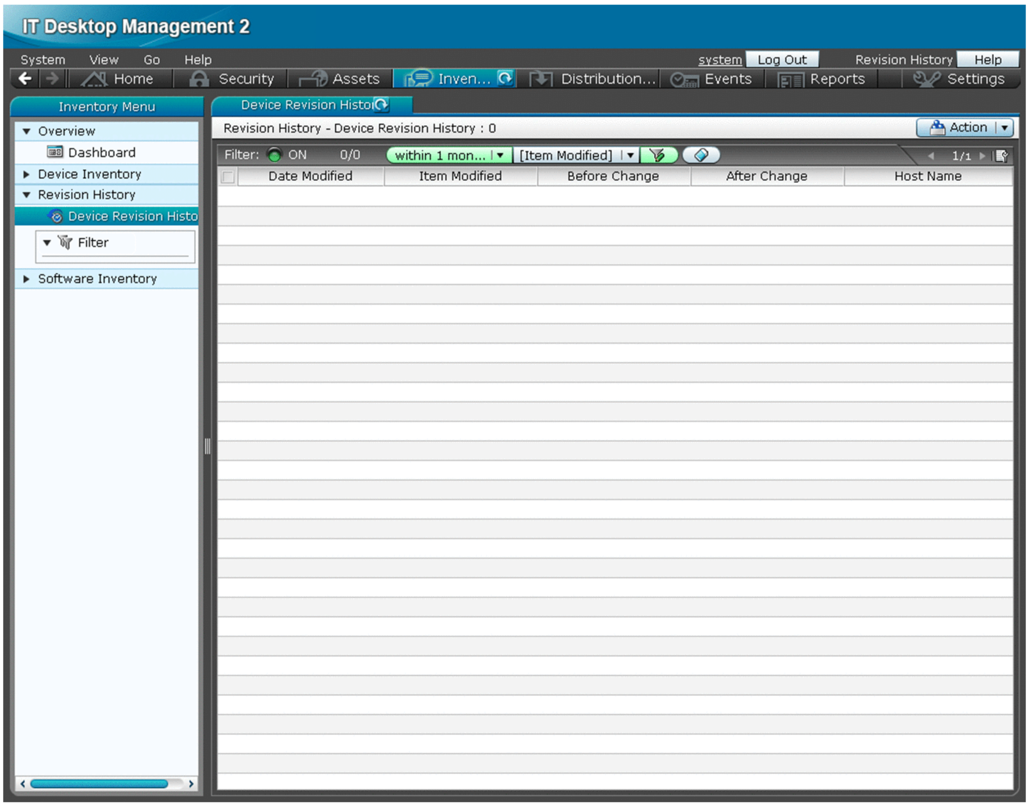
Sim10011

Item	Value
Device Type	PC
Device Status	Stop
Host ID	#GTU9C42MEISIK37IVCORFR4AEOS
▼ Computer Details	-
▶ Computer Name (Description)	Sim10011 (-)
▶ System Drive	1 Drive(s)
▶ BIOS	BIOS Date: 05/09/08 11:12:06 Ver: 08.00.10
AMT Firmware Version	-
▶ Power Control	-
▼ Smart device information	-
Model (Manufacturer)	- (-)
Serial #	-
RAM (free)	- (-)
Internal storage (free)	- (-)

Details about the device you select in the upper pane of the information area is shown in the tabs in the lower pane. This includes system information, hardware information, information about installed software, and security information.

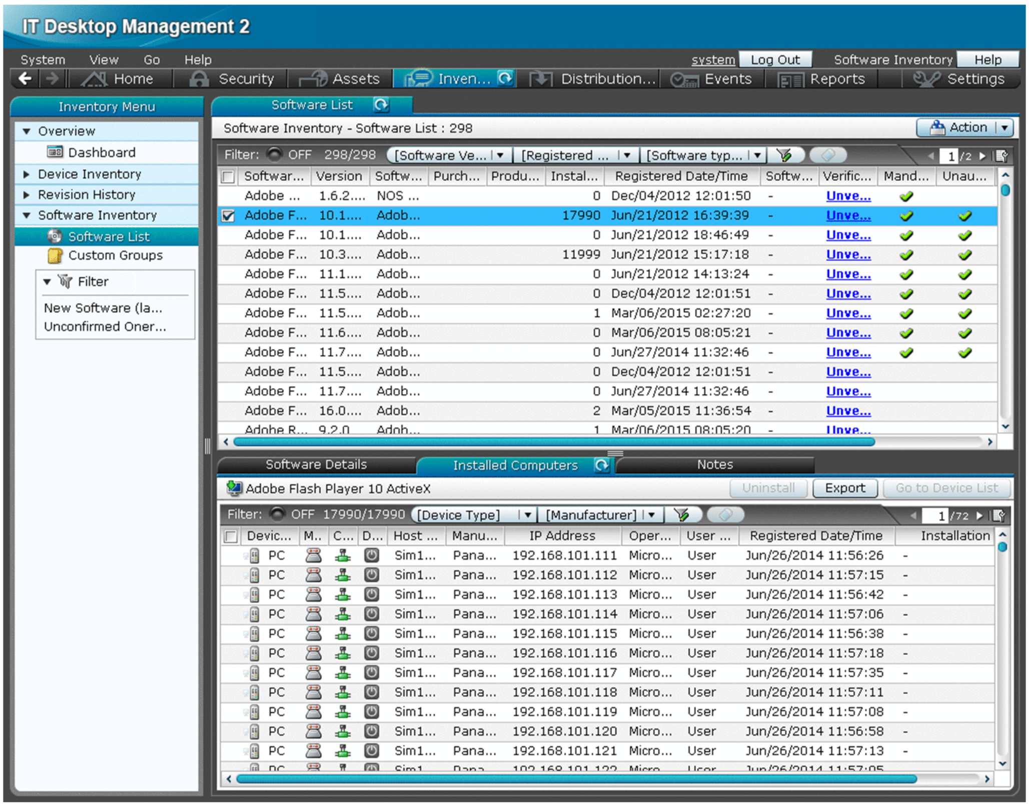
Revision History view

This view displays changes in the configuration of managed devices, including the CPU, memory, and IP addresses. By checking the revision history, you can easily find invalid configuration changes.



Software Inventory view

In this view, you can manage software installed on managed computers. This allows you to view a list of computers on which a particular software product is installed, designate software as prohibited software in a security policy, and so on.



Software Inventory - Software List : 298

Filter: OFF 298/298 [Software Ve... ▾ [Registered ... ▾ [Software typ... ▾ 1/2

□	Softwar...	Version	Softw...	Purch...	Produ...	Instal...	Registered Date/Time	Softw...	Verific...	Mand...	Unau...
	Adobe ...	1.6.2....	NOS ...			0	Dec/04/2012 12:01:50	-	Unve...	✓	
☑	Adobe F...	10.1....	Adob...			17990	Jun/21/2012 16:39:39	-	Unve...	✓	✓
	Adobe F...	10.1....	Adob...			0	Jun/21/2012 18:46:49	-	Unve...	✓	✓
	Adobe F...	10.3....	Adob...			11999	Jun/21/2012 15:17:18	-	Unve...	✓	✓
	Adobe F...	11.1....	Adob...			0	Jun/21/2012 14:13:24	-	Unve...	✓	✓
	Adobe F...	11.5....	Adob...			0	Dec/04/2012 12:01:51	-	Unve...	✓	✓
	Adobe F...	11.5....	Adob...			1	Mar/06/2015 02:27:20	-	Unve...	✓	✓
	Adobe F...	11.6....	Adob...			0	Mar/06/2015 08:05:21	-	Unve...	✓	✓
	Adobe F...	11.7....	Adob...			0	Jun/27/2014 11:32:46	-	Unve...	✓	✓
	Adobe F...	11.5....	Adob...			0	Dec/04/2012 12:01:51	-	Unve...		
	Adobe F...	11.7....	Adob...			0	Jun/27/2014 11:32:46	-	Unve...		
	Adobe F...	16.0....	Adob...			2	Mar/05/2015 11:36:54	-	Unve...		
	Adobe R...	9.2.0	Adob...			1	Mar/06/2015 08:05:20	-	Unve...		

Adobe Flash Player 10 ActiveX

Filter: OFF 17990/17990 [Device Type] ▾ [Manufacturer] ▾ 1/72

□	Devic...	M..	C...	D...	Host ...	Manu...	IP Address	Oper...	User ...	Registered Date/Time	Installation
	PC				Sim1...	Pana...	192.168.101.111	Micro...	User	Jun/26/2014 11:56:26	-
	PC				Sim1...	Pana...	192.168.101.112	Micro...	User	Jun/26/2014 11:57:15	-
	PC				Sim1...	Pana...	192.168.101.113	Micro...	User	Jun/26/2014 11:56:42	-
	PC				Sim1...	Pana...	192.168.101.114	Micro...	User	Jun/26/2014 11:57:06	-
	PC				Sim1...	Pana...	192.168.101.115	Micro...	User	Jun/26/2014 11:56:38	-
	PC				Sim1...	Pana...	192.168.101.116	Micro...	User	Jun/26/2014 11:57:18	-
	PC				Sim1...	Pana...	192.168.101.117	Micro...	User	Jun/26/2014 11:57:35	-
	PC				Sim1...	Pana...	192.168.101.118	Micro...	User	Jun/26/2014 11:57:11	-
	PC				Sim1...	Pana...	192.168.101.119	Micro...	User	Jun/26/2014 11:57:08	-
	PC				Sim1...	Pana...	192.168.101.120	Micro...	User	Jun/26/2014 11:56:58	-
	PC				Sim1...	Pana...	192.168.101.121	Micro...	User	Jun/26/2014 11:57:13	-
	PC				Sim1...	Pana...	192.168.101.122	Micro...	User	Jun/26/2014 11:57:05	

Details about the software you select in the upper pane of the information area is shown in the tabs in the lower pane. This includes software information and a list of computers on which the software is installed.

1.3.6 Working with the Distribution (ITDM-compatible) module

In the Distribution (ITDM-compatible) module, you can distribute and install required software on managed computers, uninstall redundant software, and so on. Besides software, you can also distribute individual files.

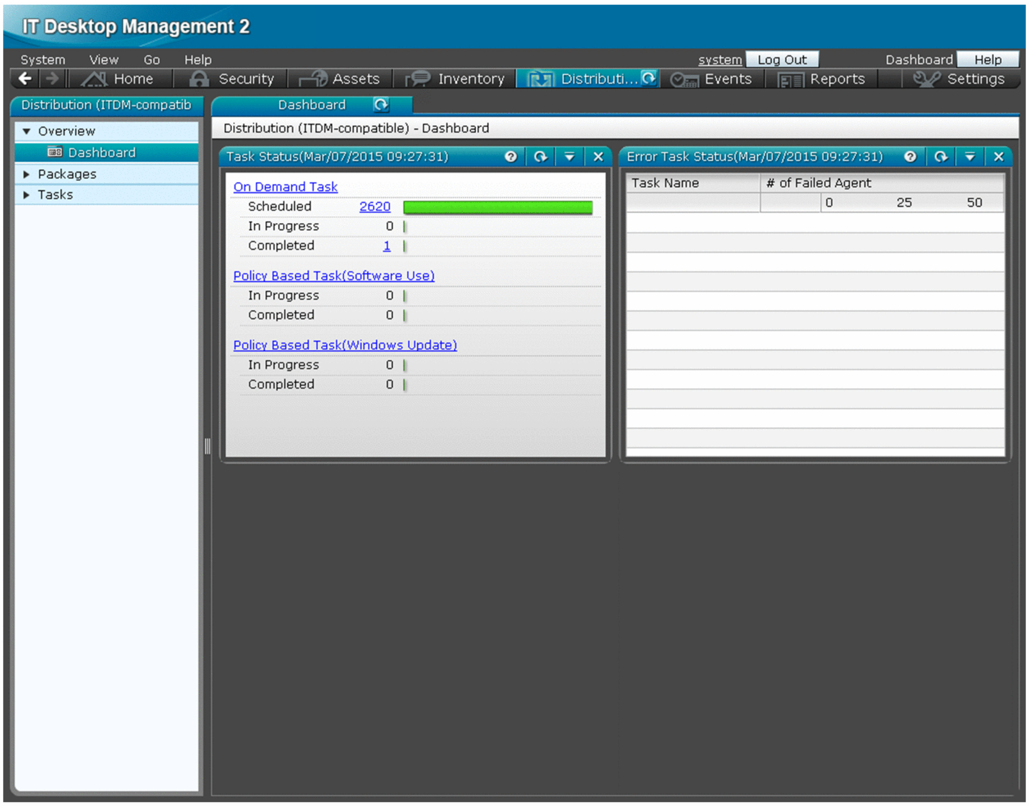
The Distribution (ITDM-compatible) module provides the following views:

- **Overview** view
- **Packages** view
- **Tasks** view

Each view is described next.

Overview view

The panels in this view show the status of tasks and a list of tasks where errors have occurred.



Distribution (ITDM-compatible) - Dashboard

Task Status(Mar/07/2015 09:27:31)

On Demand Task

Scheduled	2620
In Progress	0
Completed	1

Policy Based Task(Software Use)

In Progress	0
Completed	0

Policy Based Task(Windows Update)

In Progress	0
Completed	0

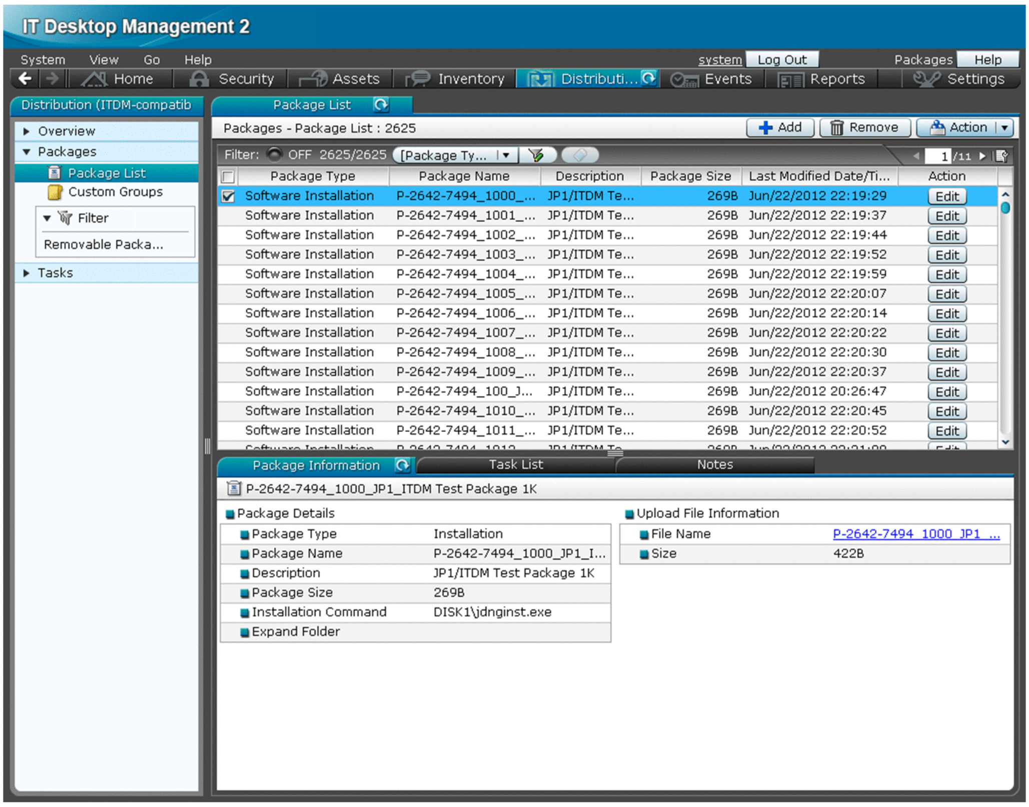
Error Task Status(Mar/07/2015 09:27:31)

Task Name	# of Failed Agent
	0 25 50

Packages view

You can manage the packages that encapsulate distributed software and files. In this view, you can add and edit packages, and rerun or suspend package distribution operations.

You can also open a wizard that guides you through the process of installing or uninstalling software and distributing files.



Packages - Package List : 2625

Filter: OFF 2625/2625 [Package Ty...

1 /11

☐	Package Type	Package Name	Description	Package Size	Last Modified Date/Ti...	Action
☑	Software Installation	P-2642-7494_1000_...	JP1/ITDM Te...	269B	Jun/22/2012 22:19:29	Edit
	Software Installation	P-2642-7494_1001_...	JP1/ITDM Te...	269B	Jun/22/2012 22:19:37	Edit
	Software Installation	P-2642-7494_1002_...	JP1/ITDM Te...	269B	Jun/22/2012 22:19:44	Edit
	Software Installation	P-2642-7494_1003_...	JP1/ITDM Te...	269B	Jun/22/2012 22:19:52	Edit
	Software Installation	P-2642-7494_1004_...	JP1/ITDM Te...	269B	Jun/22/2012 22:19:59	Edit
	Software Installation	P-2642-7494_1005_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:07	Edit
	Software Installation	P-2642-7494_1006_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:14	Edit
	Software Installation	P-2642-7494_1007_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:22	Edit
	Software Installation	P-2642-7494_1008_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:30	Edit
	Software Installation	P-2642-7494_1009_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:37	Edit
	Software Installation	P-2642-7494_100_J...	JP1/ITDM Te...	269B	Jun/22/2012 20:26:47	Edit
	Software Installation	P-2642-7494_1010_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:45	Edit
	Software Installation	P-2642-7494_1011_...	JP1/ITDM Te...	269B	Jun/22/2012 22:20:52	Edit

P-2642-7494_1000_JP1_ITDM Test Package 1K

Package Details

Package Type	Installation
Package Name	P-2642-7494_1000_JP1_I...
Description	JP1/ITDM Test Package 1K
Package Size	269B
Installation Command	DISK1\jdnginst.exe
Expand Folder	

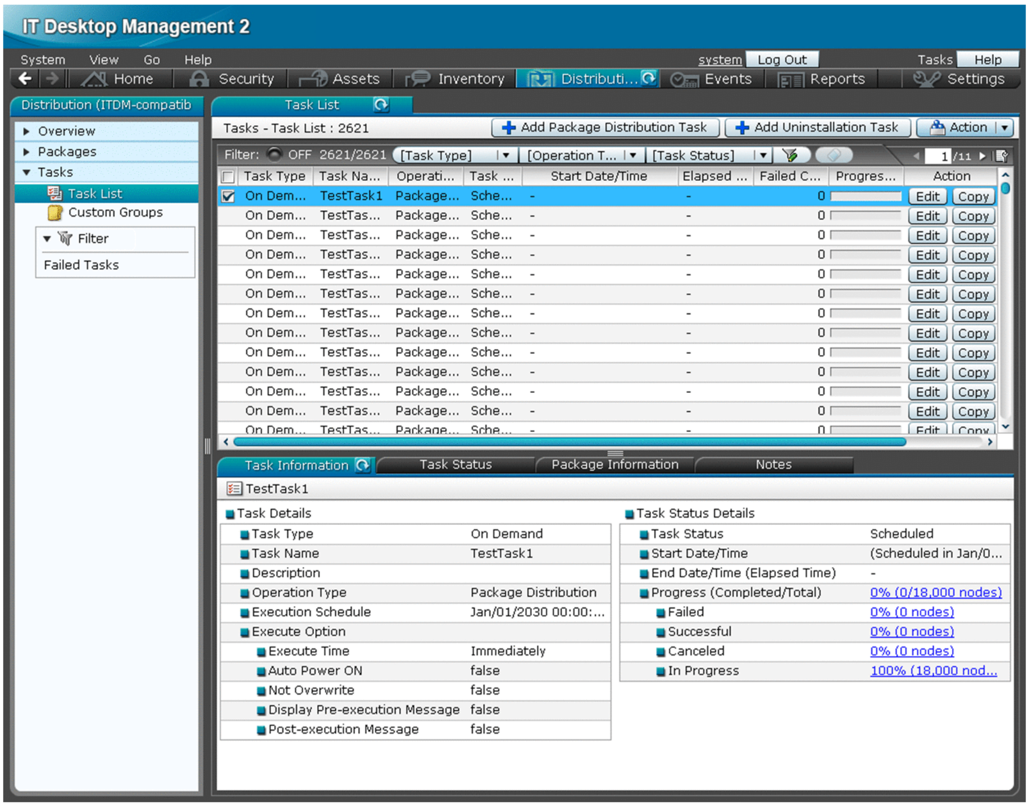
Upload File Information

File Name	P-2642-7494_1000_JP1_...
Size	422B

Details about the package you select in the upper pane of the information area is shown in the tabs in the lower pane. You can check package information, tasks that distribute packages, and so on.

Tasks view

You can manage tasks that distribute packages and uninstall software, among others. In this view, you can add and edit tasks, and rerun or cancel tasks.



Tasks - Task List : 2621

Filter: OFF 2621/2621

□	Task Type	Task Na...	Operati...	Task ...	Start Date/Time	Elapsed ...	Failed C...	Progres...	Action
☑	On Dem...	TestTask1	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy
	On Dem...	TestTas...	Package...	Sche...	-	-	0		Edit Copy

TestTask1

Task Details

Task Type	On Demand
Task Name	TestTask1
Description	
Operation Type	Package Distribution
Execution Schedule	Jan/01/2030 00:00:...
Execute Option	
Execute Time	Immediately
Auto Power ON	false
Not Overwrite	false
Display Pre-execution Message	false
Post-execution Message	false

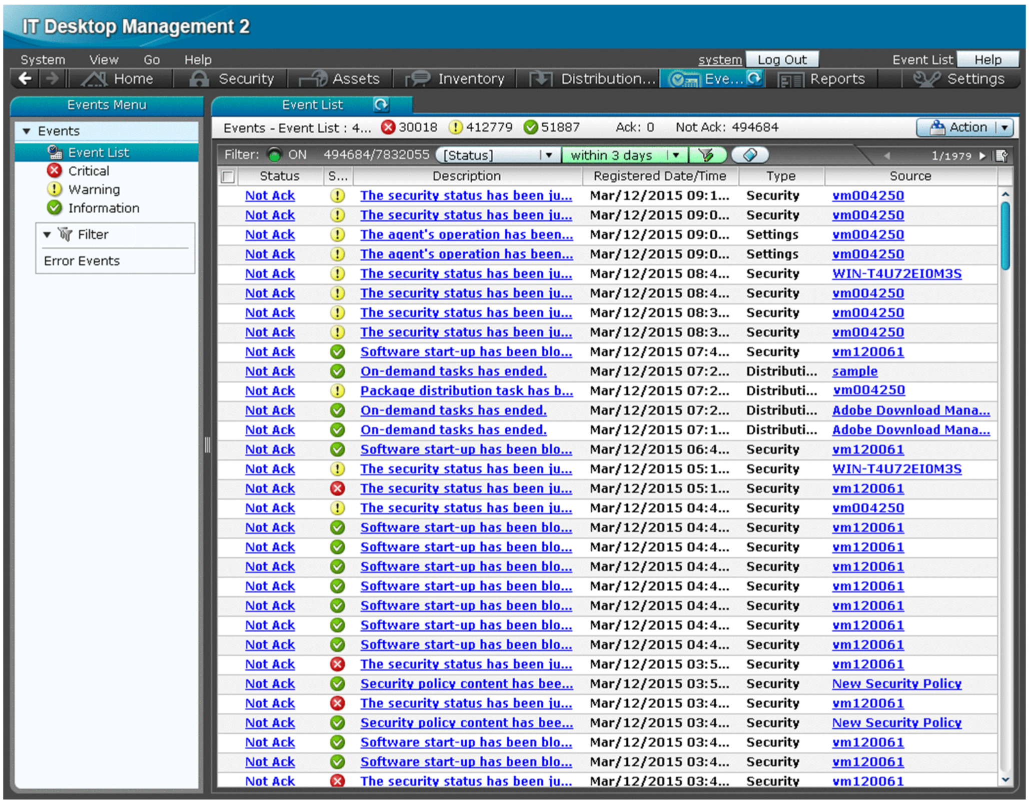
Task Status Details

Task Status	Scheduled
Start Date/Time	(Scheduled in Jan/0...
End Date/Time (Elapsed Time)	-
Progress (Completed/Total)	0% (0/18,000 nodes)
Failed	0% (0 nodes)
Successful	0% (0 nodes)
Canceled	0% (0 nodes)
In Progress	100% (18,000 nod...

Details about the task you select in the upper pane of the information area is shown in the tabs in the lower pane. You can view task information, task statuses, package information and so on.

1.3.7 Working with the Events module

In the Events module, you can check events that occurred during JP1/IT Desktop Management 2 operation. Events include activity such as security judgment and device discovery ending normally.

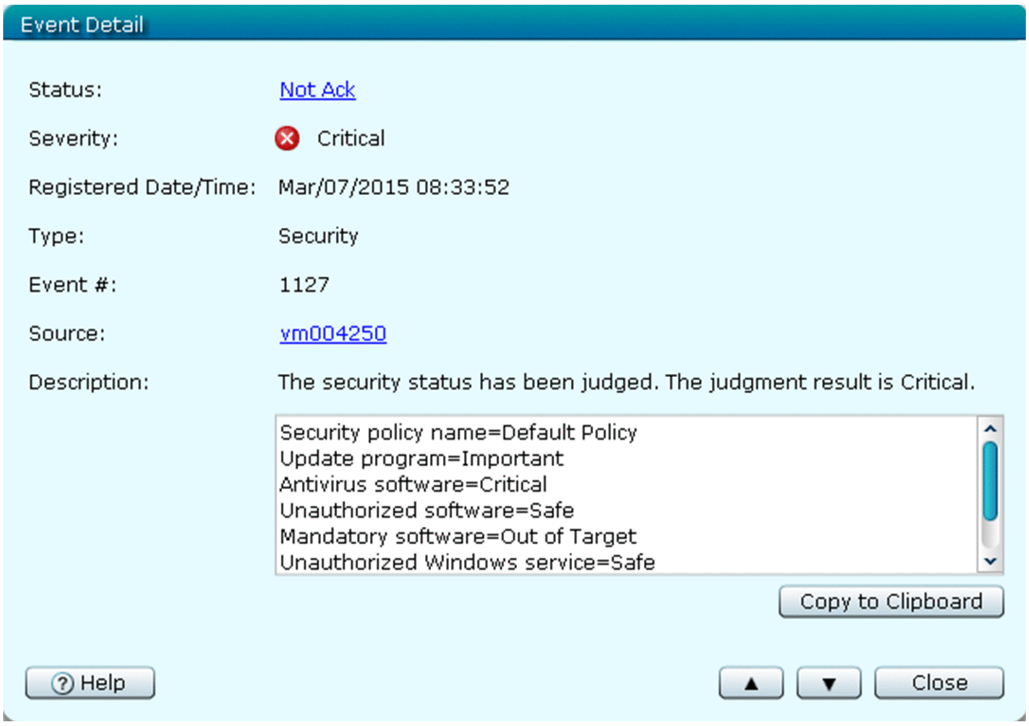


Events - Event List : 4... ✕ 30018 ! 412779 ✓ 51887 Ack: 0 Not Ack: 494684

Filter: ● ON 494684/7832055 [Status] within 3 days 1/1979

□	Status	S...	Description	Registered Date/Time	Type	Source
	Not Ack	!	The security status has been ju...	Mar/12/2015 09:1...	Security	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 09:0...	Security	vm004250
	Not Ack	!	The agent's operation has been...	Mar/12/2015 09:0...	Settings	vm004250
	Not Ack	!	The agent's operation has been...	Mar/12/2015 09:0...	Settings	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:4...	Security	WIN-T4U72EI0M3S
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:4...	Security	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:3...	Security	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:3...	Security	vm004250
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 07:4...	Security	vm120061
	Not Ack	✓	On-demand tasks has ended.	Mar/12/2015 07:2...	Distributi...	sample
	Not Ack	!	Package distribution task has b...	Mar/12/2015 07:2...	Distributi...	vm004250
	Not Ack	✓	On-demand tasks has ended.	Mar/12/2015 07:2...	Distributi...	Adobe Download Mana...
	Not Ack	✓	On-demand tasks has ended.	Mar/12/2015 07:1...	Distributi...	Adobe Download Mana...
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 06:4...	Security	vm120061
	Not Ack	!	The security status has been ju...	Mar/12/2015 05:1...	Security	WIN-T4U72EI0M3S
	Not Ack	✕	The security status has been ju...	Mar/12/2015 05:1...	Security	vm120061
	Not Ack	!	The security status has been ju...	Mar/12/2015 04:4...	Security	vm004250
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✕	The security status has been ju...	Mar/12/2015 03:5...	Security	vm120061
	Not Ack	✓	Security policy content has bee...	Mar/12/2015 03:5...	Security	New Security Policy
	Not Ack	✕	The security status has been ju...	Mar/12/2015 03:4...	Security	vm120061
	Not Ack	✓	Security policy content has bee...	Mar/12/2015 03:4...	Security	New Security Policy
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 03:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 03:4...	Security	vm120061
	Not Ack	✕	The security status has been ju...	Mar/12/2015 03:4...	Security	vm120061

You can view an event in detail by clicking the link in **Description**.



Status: Not Ack

Severity: ✕ Critical

Registered Date/Time: Mar/07/2015 08:33:52

Type: Security

Event #: 1127

Source: vm004250

Description: The security status has been judged. The judgment result is Critical.

```
Security policy name=Default Policy
Update program=Important
Antivirus software=Critical
Unauthorized software=Safe
Mandatory software=Out of Target
Unauthorized Windows service=Safe
```

Some events require a quick response. Attend to **Critical** events first, followed by **Warning** events. Identify the cause of the event from the event details, and take the appropriate action.

When you have finished dealing with an event, change its status to **Ack**. By changing the event status, you can easily identify whether an event has been resolved.

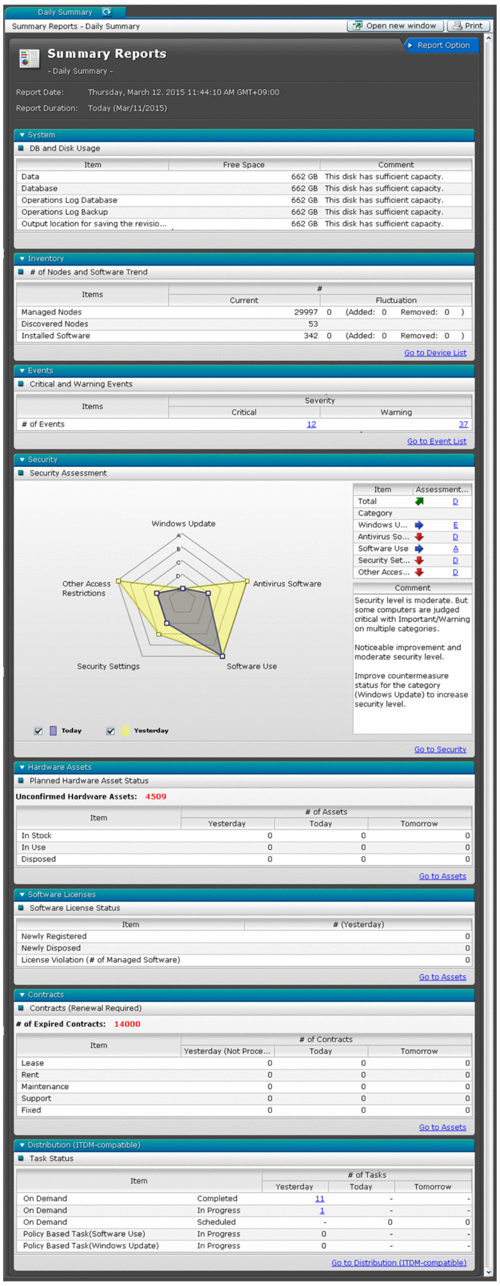
1.3.8 Working with the Reports module

In the Reports module, you can view information about managed devices, the security status of computers, and other information in the form of a report. Reports can also be printed and used as official documents.

Examples of reports are shown below.

Daily Summary report

This report displays the status of events, the number of assets scheduled to undergo a status change, the status of software licenses, the status of distribution tasks, and other information for a specific day.



Summary Reports

- Daily Summary -

Report Date: Thursday, March 12. 2015 11:44:10 AM GMT+09:00

Report Duration: Today (Mar/11/2015)

▼ System

DB and Disk Usage

Item	Free Space	Comment
Data	662 GB	This disk has sufficient capacity.
Database	662 GB	This disk has sufficient capacity.
Operations Log Database	662 GB	This disk has sufficient capacity.
Operations Log Backup	662 GB	This disk has sufficient capacity.
Output location for saving the revisio...	662 GB	This disk has sufficient capacity.

▼ Inventory

# of Nodes and Software Trend

Items	#	
	Current	Fluctuation
Managed Nodes	29997	0 (Added: 0 Removed: 0)
Discovered Nodes	53	
Installed Software	342	0 (Added: 0 Removed: 0)

Go to Device List

▼ Events

Critical and Warning Events

Items	Severity	
	Critical	Warning
# of Events	12	37

Go to Event List

▼ Security

Security Assessment

Item	Assessment...	
Total	↖	D
Category		
Windows U...	→	E
Antivirus So...	↓	D
Software Use	→	A
Security Set...	↓	D
Other Acces...	↓	D

Comment

Security level is moderate. But some computers are judged critical with Important/Warning on multiple categories.

Noticeable improvement and moderate security level.

Improve countermeasure status for the category (Windows Update) to increase security level.

Go to Security

▼ Hardware Assets

Planned Hardware Asset Status

Unconfirmed Hardware Assets: 4509

Item	# of Assets		
	Yesterday	Today	Tomorrow
In Stock	0	0	0
In Use	0	0	0
Disposed	0	0	0

Go to Assets

▼ Software Licenses

Software License Status

Item	# (Yesterday)
Newly Registered	0
Newly Disposed	0
License Violation (# of Managed Software)	0

Go to Assets

▼ Contracts

Contracts (Renewal Required)

# of Expired Contracts: 14000

Item	# of Contracts		
	Yesterday (Not Proce...	Today	Tomorrow
Lease	0	0	0
Rent	0	0	0
Maintenance	0	0	0
Support	0	0	0
Fixed	0	0	0

Go to Assets

▼ Distribution (ITDM-compatible)

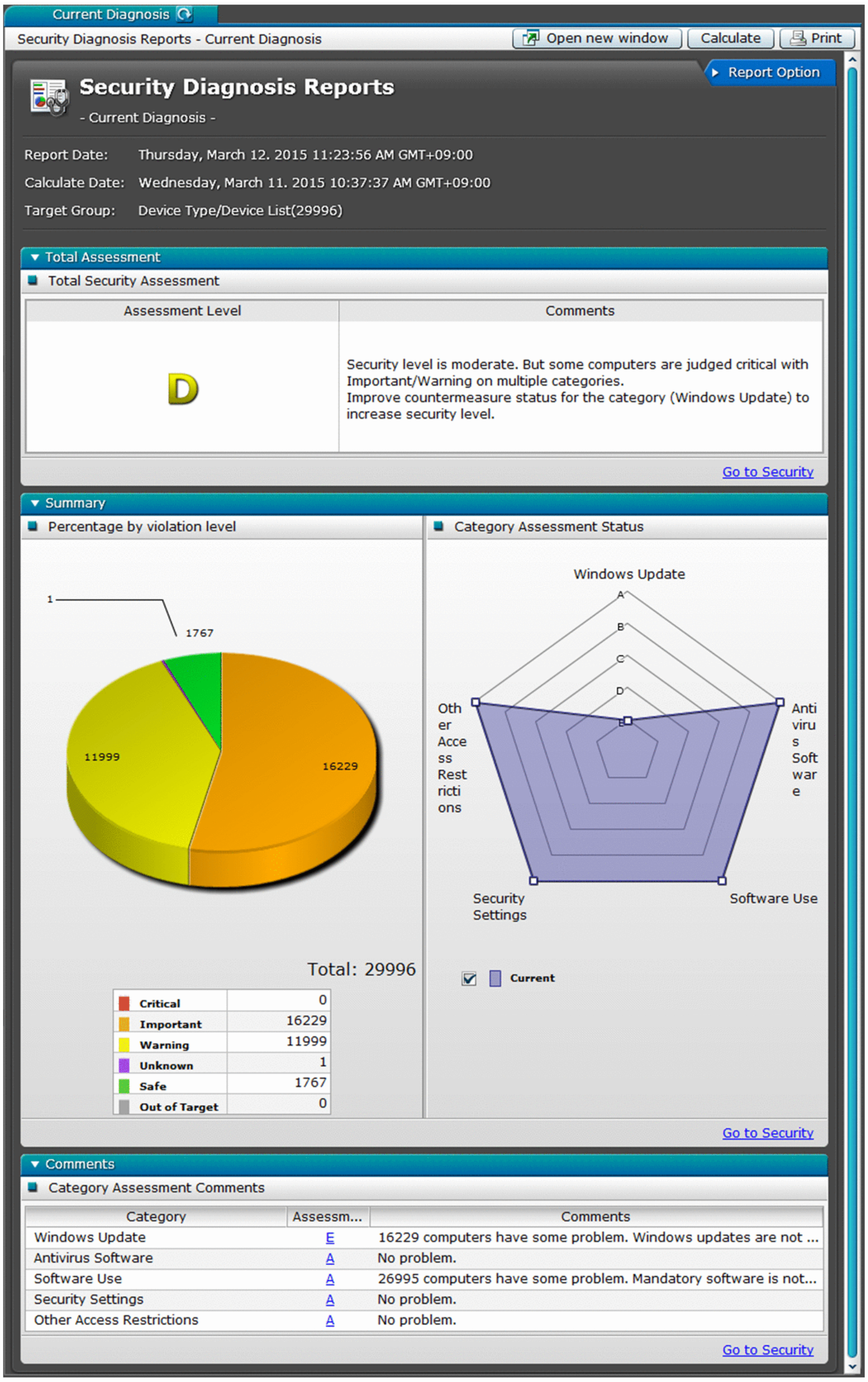
Task Status

Item		# of Tasks		
		Yesterday	Today	Tomorrow
On Demand	Completed	11	-	-
On Demand	In Progress	1	-	-
On Demand	Scheduled	-	0	0
Policy Based Task(Software Use)	In Progress	0	-	-
Policy Based Task(Windows Update)	In Progress	0	-	-

Go to Distribution (ITDM-compatible)

Current Diagnosis report

This report shows the results of diagnosing the current security status.



Security Diagnosis Reports - Current Diagnosis

Security Diagnosis Reports

- Current Diagnosis -

Report Date:	Thursday, March 12. 2015 11:23:56 AM GMT+09:00
Calculate Date:	Wednesday, March 11. 2015 10:37:37 AM GMT+09:00
Target Group:	Device Type/Device List(29996)

▼ Total Assessment

Total Security Assessment

Assessment Level	Comments
D	Security level is moderate. But some computers are judged critical with Important/Warning on multiple categories. Improve countermeasure status for the category (Windows Update) to increase security level.

Go to Security

▼ Summary

Percentage by violation level

Total: 29996

🟥 Critical	0
🟧 Important	16229
🟨 Warning	11999
🟪 Unknown	1
🟩 Safe	1767
⬜ Out of Target	0

Category Assessment Status

☑ Current

Go to Security

▼ Comments

Category Assessment Comments

Category	Assessm...	Comments
Windows Update	E	16229 computers have some problem. Windows updates are not ...
Antivirus Software	A	No problem.
Software Use	A	26995 computers have some problem. Mandatory software is not...
Security Settings	A	No problem.
Other Access Restrictions	A	No problem.

Go to Security

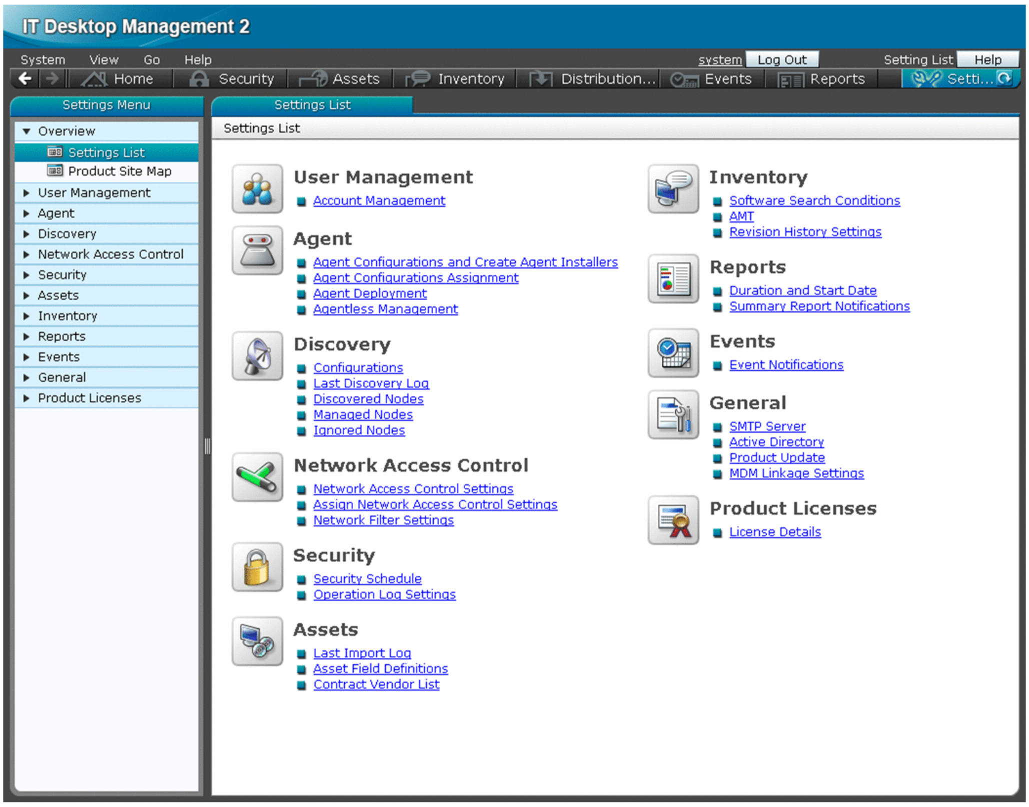
1.3.9 Working with the Settings module

In the Settings module, you can customize JP1/IT Desktop Management 2 settings such as user account settings and agent configurations. You can also search for devices and distribute agents from this module.

Each view of the Settings module is described next.

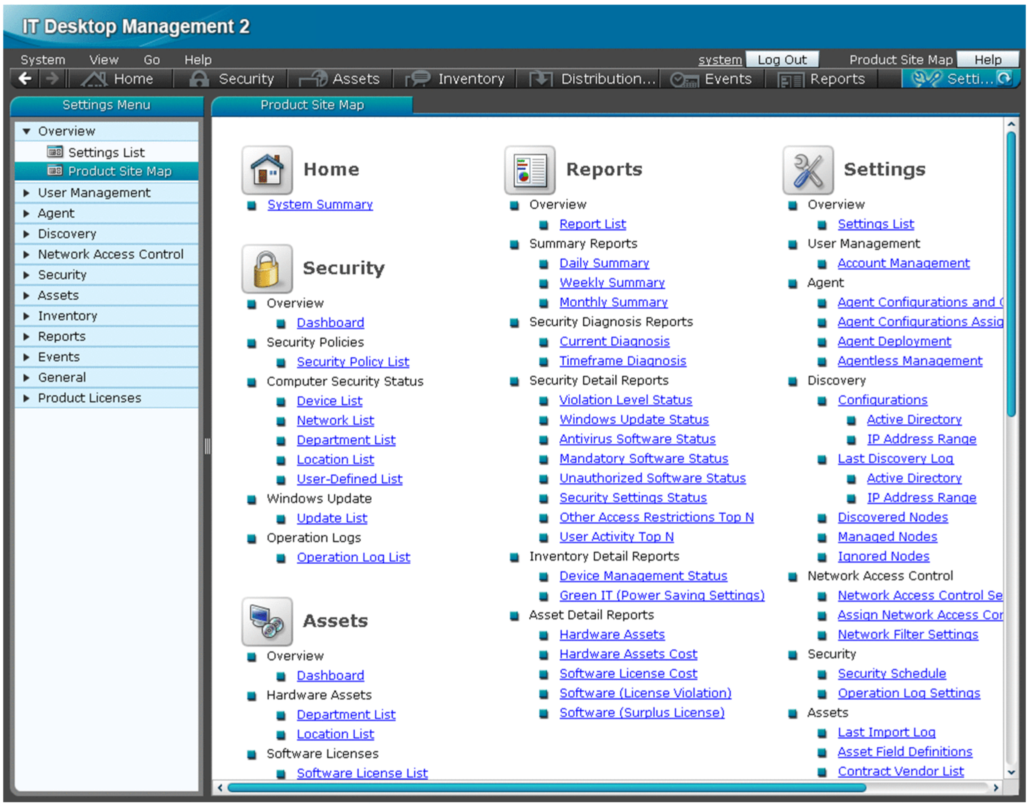
Settings List view

Lists the operations available in the Settings module. From this view, you can navigate to each view of the Settings module and customize the environment.



Product Site Map view

Lists the main components of the user interface provided by JP1/IT Desktop Management 2. You can go directly to a particular view by clicking the corresponding link. The **Product Site Map** view is useful if you need to access a particular view and are unsure of its location.



Views in the Settings module

User Management view

You can add, edit, and delete JP1/IT Desktop Management 2 user accounts.

Agent view

You can create and edit agent configurations and create installation sets. You can also distribute the agent software and assign agent configurations to agents.

Discovery view

Operations you can perform in this view include setting search conditions for devices, and manually initiating device discovery. You can also start managing a device in JP1/IT Desktop Management 2 by designating it as a management target.

Network Access Control view

You can specify, by network segment, whether to permit newly discovered devices to connect to the network. You can also set linkages with JP1/NETM/NM - Manager and specify the settings related to the network control list.

Security view

You can schedule security assessments of managed computers. You can also specify settings related to the automatic import and export of operation logs.

Assets view

You can set management items for asset information. You can also add, edit, and delete contract company information. If you import asset information from a CSV file, you can use this view to check the status and results of the import process.

Inventory view

You can add, edit, and delete conditions to be used when searching for software that does not appear in the **Programs and Features** list in Windows. You can also specify the settings for using AMT in JP1/IT Desktop Management 2 and for collecting revision histories.

Reports view

You can specify the retention period and start date for reports. You can also nominate a user as a recipient or a summary report.

Events view

You can select users to be notified when an event occurs, the type and severity of errors that generate a notification, and events for which no notification is issued.

General view

You can set up connections to the SMTP server, Active Directory, support services, and MDM systems.

Product Licenses view

You can view license information for JP1/IT Desktop Management 2 and register additional licenses.

2 Features of JP1/IT Desktop Management 2

This chapter explains the details of JP1/IT Desktop Management 2 features.

2.1 List of features

Feature	Description
System summary	You can use the home module and dashboards to view the status of the system from a variety of perspectives.
User account management	By setting permissions, task allocations, and administration scopes, you can create user accounts suited to the role and responsibilities of each administrator who manages JP1/IT Desktop Management 2.
Setup wizard	A wizard is provided that guides you through the process of setting up JP1/IT Desktop Management 2.
Agent installation	You can register a user's computer as a management target of JP1/IT Desktop Management 2 by installing the agent program on the computer. This allows you to use the features of JP1/IT Desktop Management 2 to manage that computer. There are several ways to install the agent. For example, an administrator can install the agent program manually, or you can distribute the program automatically from a management server.
Device management	When a device becomes a management target, you can use the features of JP1/IT Desktop Management 2 to manage the device. These include collecting and displaying device information, and monitoring and controlling whether devices are on or off. Managed devices can also be assessed against a security policy and contribute data to reports. You can use the search function and network monitoring function to discover the devices in your organization and automatically designate them as management targets.
Remote control	You can use the controller program to access the desktop of a user's computer and control it remotely. You can also use this program to send and receive files, record and play back screen activity, and chat with users.
Network connection management	JP1/IT Desktop Management 2 can monitor the network, preventing access by unauthorized devices and automatically isolating computers that are identified as a security risk.
Security management	You can determine the security status of the computers in your organization by creating a security policy to assess them against. You can also implement security measures automatically and remotely on computers that might pose a security risk, and send messages notifying users of potential issues.
Operation log management	You can acquire operation logs that record the history of tasks a user has performed, and view this information in the operation window. This feature allows you to scrutinize the log data closely when suspicious operations are detected that might lead to information being disclosed.
Asset management	You can manage the operating status of your system by keeping an inventory of the hardware assets and software licenses in your organization. There are two asset information management methods provided by JP1/IT Desktop Management 2. • Managing assets by using Asset Console You use Asset Console to manage assets. This is recommended if you want to manage asset information in more detail than when you use the JP1/IT Desktop Management 2 operation window: for example, if you want to customize an asset information search window, or manage asset information that uses Items. • Managing assets using the JP1/IT Desktop Management 2 operation window Use the JP1/IT Desktop Management 2 - Manager operation window (Assets module) to manage assets. This is recommended when you want to manage assets easily by using information collected by JP1/IT Desktop Management 2.
Software and file distribution	Administrators can distribute software and files on users' computers without needing to be on site. Distribution can be performed in the following two ways: • Distribution using Remote Installation Manager You use Remote Installation Manager for distribution. In this way, you can specify detailed conditions and operations on the distribution-destination computer. You can also use commands to distribute the software and files managed by Remote Installation Manager. The commands enable regular distribution using a batch file or automatic distribution in response to a specific event linking with JP1/AJS. This type of distribution is recommended if you want to specify detailed distribution conditions, or if you want to perform distribution every day. • Distribution using the operation window (ITDM-compatible distribution) You use Distribution (ITDM-compatible) modules of the operation window for distribution. Unlike distribution using Remote Installation Manager, you cannot specify detailed conditions or operations. Instead, you can let

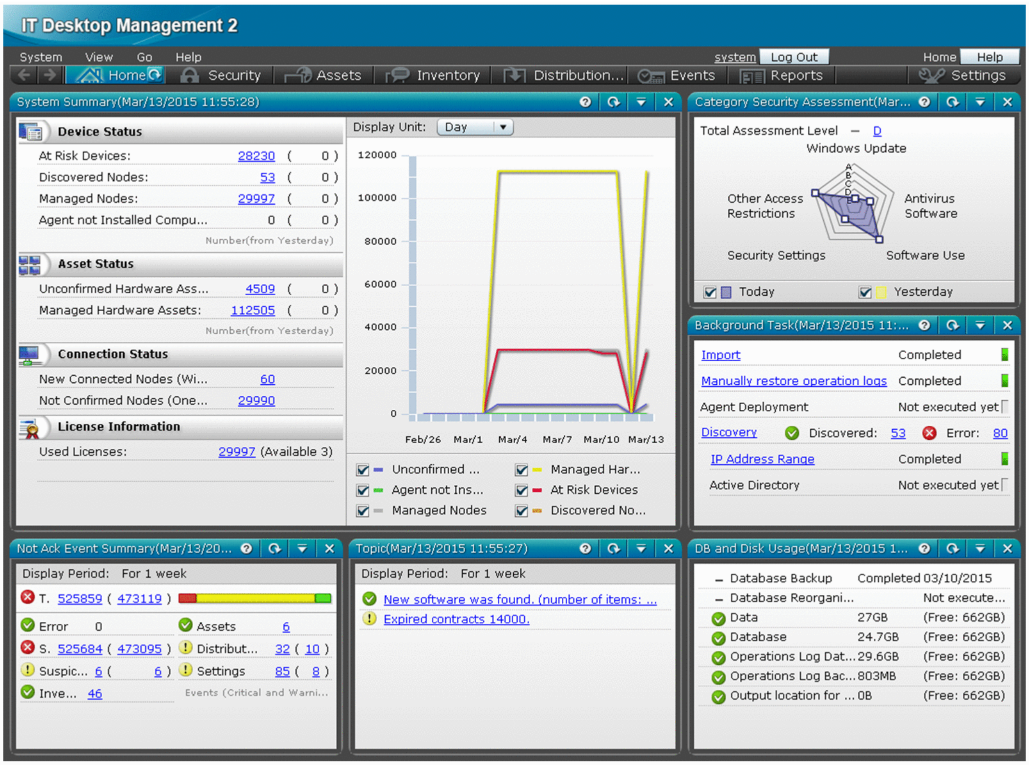
Feature	Description
Software and file distribution	the installer automatically install MSI-file-based software on the distribution-destination computer with simple steps using a wizard. You can also uninstall some of the software installed on a user's computer. This type of distribution is recommended when you want to distribute software with an MSI-file installer a few times in a week or month. Distribution using Remote Installation Manager and ITDM-compatible distribution are different functions. Therefore, the data for a function can only be used by that function. For example, software managed by Remote Installation Manager cannot be distributed using ITDM-compatible distribution.
File collection	You can collect files stored in users' computers. You can collect data (created by users) and error logs (output by software used by users) in a single operation.
Event viewer	You can view events that record the nature and results of actions performed by JP1/IT Desktop Management 2 features.
Report viewer	You can display all manner of reports describing aspects of your system such as the overall system status, the results of security diagnoses, power savings, and asset costs.
Filters	You can use filters to refine the information displayed in the modules. You can also save filter conditions for later use.
Use in cluster systems	You can use JP1/IT Desktop Management 2 in a cluster system.
Database management	You can use the database manager provided by JP1/IT Desktop Management 2 to back up and maintain the database.
Command line interface	You can use commands to perform a variety of tasks, such as importing and exporting management information and backing up and maintaining the database.
Operations on user computers	Users of managed computers will sometimes interact with JP1/IT Desktop Manager on their computers. This might entail viewing messages received from the management server, or entering user information.
Smart device control	By linking with an MDM system, JP1/IT Desktop Management 2 can lock, wipe, and otherwise control smart devices.

2.2 Displaying a system summary

JP1/IT Desktop Management 2 provides a Home module and dashboards that provide administrators with a concise overview of the system being managed. In addition to providing a system overview, these panels allow administrators to drill down through items of interest for a more in-depth view.

Home module

The Home module is the main window of JP1/IT Desktop Management 2 that appears when you log in. This module displays the information administrators need to know for the day-to-day running of the system, based on the most recent information available. This means that a quick visit to the Home module is all administrators need to gain an overview of the status of the system in general. Also, administrators can view more detailed information about an aspect of the system by clicking the items in the module.



System Summary(Mar/13/2015 11:55:28)

Device Status

At Risk Devices: 28230 (0)
Discovered Nodes: 53 (0)
Managed Nodes: 29997 (0)
Agent not Installed Compu... 0 (0)
Number(from Yesterday)

Asset Status

Unconfirmed Hardware Ass... 4509 (0)
Managed Hardware Assets: 112505 (0)
Number(from Yesterday)

Connection Status

New Connected Nodes (Wi... 60
Not Confirmed Nodes (One... 29990

License Information

Used Licenses: 29997 (Available 3)

Display Unit: Day

☑ Unconfirmed ... ☑ Managed Har...
☑ Agent not Ins... ☑ At Risk Devices
☑ Managed Nodes ☑ Discovered No...

Category Security Assessment(Mar...

Total Assessment Level – D

☑ Today ☑ Yesterday

Background Task(Mar/13/2015 11:...

Import Completed
Manually restore operation logs Completed
Agent Deployment Not executed yet
Discovery Discovered: 53 Error: 80
IP Address Range Completed
Active Directory Not executed yet

Not Ack Event Summary(Mar/13/20...

Display Period: For 1 week

T. 525859 (473119)
Error 0 Assets 6
S. 525684 (473095) Distribut... 32 (10)
Suspic... 6 (6) Settings 85 (8)
Inve... 46 Events (Critical and Warni...

Topic(Mar/13/2015 11:55:27)

Display Period: For 1 week

New software was found. (number of items: ...
Expired contracts 14000.

DB and Disk Usage(Mar/13/2015 1...

Database Backup	Completed 03/10/2015	
Database Reorgani...		Not execute...
Data	27GB	(Free: 662GB)
Database	24.7GB	(Free: 662GB)
Operations Log Dat...	29.6GB	(Free: 662GB)
Operations Log Bac...	803MB	(Free: 662GB)
Output location for ...	0B	(Free: 662GB)

- **System Summary** panel

  The **System Summary** panel presents an outline of the status of managed devices.

  - **Device Status**

    Displays the number of devices designated at-risk. The administrator can then check the security status of at-risk devices and take action where needed. This panel also displays the number of discovered nodes, the number of managed nodes, and the number of computers without the agent program installed.

  - **Asset Status**

    Shows the number of hardware assets whose status is *Unconfirmed*. The administrator can then check each asset to find out whether it is in use, in stock, or has been disposed of. This panel also shows the number of managed hardware assets.

  - **Connection Status**

    Shows the number of new devices that have connected to the network in the past week. This includes newly discovered devices and devices made management targets by installation of the agent program. This panel also shows the number of assets that have not been seen on the network in more than a month.

- **License Information**

  Shows the number of JP1/IT Desktop Management 2 licenses that are in use, and the number of licenses in surplus. Administrators can use this information to plan the purchase of additional licenses by monitoring trends in device and asset numbers.

- **Category Security Assessment** panel

  Shows a graph evaluating the security status of managed computers. By viewing the graph as a whole or focusing on individual categories, you can identify points of weakness and take action accordingly.

- **Background Task** panel

  Shows the status of tasks such as importing asset information, operation log manual retrieval, agent distribution, and device discovery. You can use this panel to view the results of completed tasks, or identify the cause of any errors and take actions accordingly.

- **Not Ack Event Summary** panel

  Shows the number of events that are yet to be acknowledged, and how many of those events have a severity level of *critical* or *warning*. This allows administrators to quickly identify and respond to critical events in particular. You can identify the presence of a critical event from the icon that appears to the left of the event type.

- **Topic** panel

  This panel shows important notices issued in the course of JP1/IT Desktop Management 2 operation. Always read the notices in this area, and respond quickly when made aware of a problem. Examples of the notifications in this area are as follows:

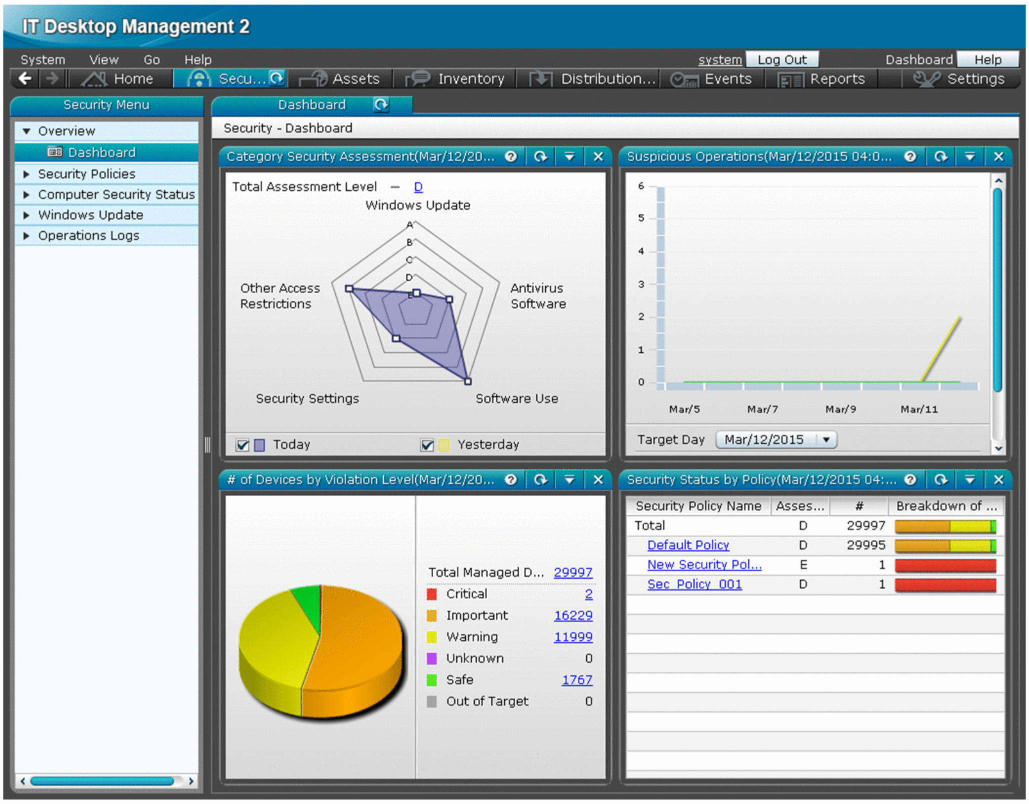
  - A data folder has insufficient free space
  - A software product has exceeded the number of available licenses
  - A contract has expired

- **DB and Disk Usage** panel

  Shows the status of database backup and reorganization tasks, and the amounts of used and available hard disk space. Based on this information, you can move the database backup folder from a nearly full disk to one with enough free space, or free up disk space by removing data that is no longer needed.

Dashboards

A dashboard is the first window that appears when you select an item in the menu at the top of the operation window. Like the home module, each dashboard displays panels in which you can monitor the status of various functions. As an example, the dashboard of the Security module is shown below.



Total Managed D...	29997
Critical	2
Important	16229
Warning	11999
Unknown	0
Safe	1767
Out of Target	0

Security Policy Name	Asses...	#	Breakdown of ...
Total	D	29997	
Default Policy	D	29995	
New Security Pol...	E	1	
Sec_Policy_001	D	1	

The Security module, Assets module, Device module, and Distribution (ITDM-compatible) module each have their own dashboard.

Tip

You can customize the panels displayed in the Home module and the various dashboards. To customize the layout, from the **View** menu at the top left of the window, select **Panel Layout**. In the dialog box, select a panel layout and select the panels you want to display.

2.2.1 List of Panels

The following table lists the panels displayed in the home module, and in the **Summary** view and **Dashboard** view of each module.

Category	Panel name	Description
Home	**System Summary**	Shows the status of managed devices, statuses of assets and connections, and license information. You can also view trends in the number of devices and assets in your system.
	Background Task	Shows the status of tasks such as asset information importation, operation log manual retrieval, agent distribution, and device discovery. If an error is reported, view the error details and take action accordingly.
	Not Ack Event Summary	Shows how many events that occurred within a specific time period have not been acknowledged. We recommend that you use this panel as the starting point for viewing and resolving critical events.

Category	Panel name	Description
Home	**Topic**	Shows the notifications that were issued within a specified time period. This panel lets you know when a contract has expired, when there are no more licenses available for a product, and other important information.
	DB and Disk Usage	Shows when the JP1/IT Desktop Management 2 database was last backed up and reorganized, and the amounts of used and available disk space.
Security	**Category Security Assessment**	Shows the overall security status of managed computers on a scale from A to E, and a chart showing security performance in individual categories. This panel also shows how the security status compares to the previous day. This allows you to monitor the effectiveness of security measures and make adjustments where necessary.
	No. of Devices by Violation Level	Shows the total number of managed devices, the number of devices at each violation level, and a graphical representation of violation levels across the system. Use this panel to quickly identify devices with a high violation level and take the appropriate action.
	Suspicious Operations	Shows the number of suspicious operations (related to data disclosure) detected by JP1/IT Desktop Management 2. You can access the operation log for the suspicious action by clicking a link. We recommend that you use this feature to find out whether any data might have been leaked.
	Security Status by Policy	This panel shows the overall security status of the system, and the security status in terms of individual security policies. If a security policy has a low rating, identify the computers that violate the policy and take remedial action.
Assets	**Hardware Assets Trend**	This panel shows trends in the number of hardware assets in each category. For example, you might notice an increase in hardware assets in *In Stock* status and decide to start disposing of older hardware.
	Customized HW Assets (Group/Filter)	This panel shows the number of hardware assets for each custom group and filter condition. For example, by defining a custom group or filter that displays hardware assets with an early purchase date, you can quickly identify hardware assets that might need replacing.
	Expired Contracts (next 3 months)	For each contract type, this panel shows the number of expired contracts and the number of contracts that are expiring soon. By clicking the links in this panel, you can identify contracts that are about to expire and plan a course of action.
	Software (License Violation)	This panel allows you to instantly see the pieces of managed software for which you have too few licenses, and those for which you have a surplus. If this panel shows that you have more instances of a product installed than you have licenses for the product, you can take action such as directing users to uninstall the software or purchasing additional licenses.
Inventory	**Managed Nodes Trend**	This panel shows trends in the number of devices in each agent installation status. For security reasons, we recommend that you install the agent program on computers managed by JP1/IT Desktop Management 2. Use this panel to identify computers that do not have the agent program installed, and install the program as needed.
	Customized Device Inventory (Group/Filter)	This panel shows the number of managed devices for each custom group and filter condition. For example, by defining a custom group or filter that displays devices that have not been used for a certain period of time, you can quickly identify hardware assets that can be declared idle.
	No. of Devices by OS	This panel shows the proportion of each OS on managed computers, and how many instances of each OS are in your system.
	New Software	This panel lists new software information collected from managed computers. Check this list regularly. If you discover non-business related software in the list, you can register it as prohibited software. You can also use this information when deciding whether to manage license information for a particular piece of software.
Distribution (ITDM-compatible)	**Task Status**	This panel shows the status of tasks executed by administrators, and those executed as part of the automatic enforcement of a security policy. We recommend that you view the **Error Task Status** panel if you only want to see tasks where errors have occurred.

Category	Panel name	Description
Distribution (ITDM-compatible)	**Error Task Status**	This panel shows the status of tasks where errors have occurred. Identify the cause of the error, take the appropriate action, and then re-execute the task. To view the status of tasks in general, we recommend that you use the **Task Status** panel.

2.3 Managing user accounts

If several administrators will be using JP1/IT Desktop Management 2, you can create a user account in JP1/IT Desktop Management 2 for each administrator.

You can set the following parameters for user accounts that define the range of operations the user can perform, and the scope of the information available to the user. By creating user accounts with the appropriate combinations of these parameters, you can ensure a proper division of responsibilities and effective internal controls among the administrators of a system.

Permission

> Set permissions appropriate to the range of operations the user performs. For example, you might have a manager who only needs read-only access to information, a system administrator who manages devices and assets, and a system administrator who manages user accounts.

Task allocation

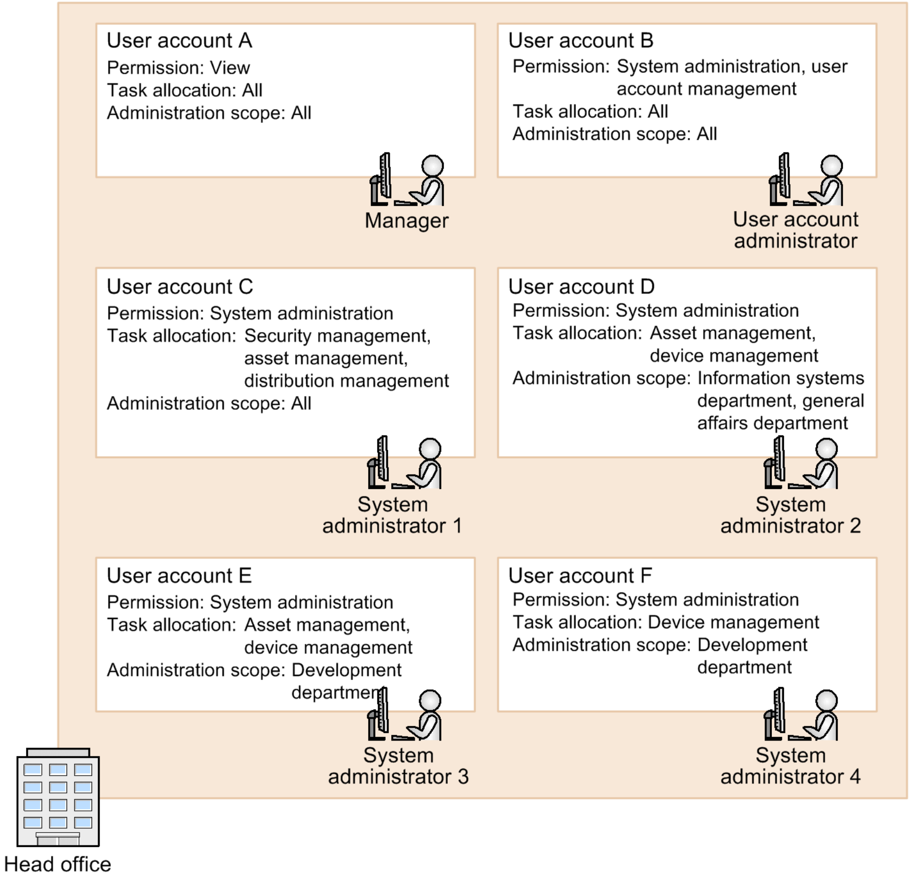
> You can restrict permissions further by limiting users to certain tasks such as security management, asset management, or device management.

Administration scope

> You can create user accounts in a manner that limits the information available to users at the department level. For example, users in the general affairs, sales, and research departments might have access to different information.

Manipulation of operation windows used for distribution using Remote Installation Manager, such as Remote Installation Manager and Packager, is allowed only for users who are given distribution management task allocation and system management authority in the user account settings.

The following figure shows an example of creating user accounts with separate parameters for each administrator.


User account A
Permission: View
Task allocation: All
Administration scope: All
Manager
User account B
Permission: System administration, user account management
Task allocation: All
Administration scope: All
User account administrator
User account C
Permission: System administration
Task allocation: Security management, asset management, distribution management
Administration scope: All
System administrator 1
User account D
Permission: System administration
Task allocation: Asset management, device management
Administration scope: Information systems department, general affairs department
System administrator 2
User account E
Permission: System administration
Task allocation: Asset management, device management
Administration scope: Development department
System administrator 3
User account F
Permission: System administration
Task allocation: Device management
Administration scope: Development department
System administrator 4
Head office

Users with user management permission are able to add, edit, and delete user accounts.

Add and delete user accounts when changes are made to the users who use JP1/IT Desktop Management 2 in your organization. Edit user accounts when changes to the management structure require changes to account passwords or permissions. User account passwords must be changed regularly. When a password approaches its expiration date, only the owner of the account or an administrator with user management permission can change the password.

Tip

A user with user management permission can unlock user accounts and reset passwords when a user is locked out or forgets his or her password.

2.3.1 Locking user accounts

You can specify that a user's account is to be locked when the user fails to log in to JP1/IT Desktop Management 2 a predetermined number of times. That user cannot log in again until the user account is unlocked.

You can specify the number of failed attempts before a user account is locked, in the **Other Settings** view in the setup window.

You can find out whether any accounts are locked by accessing the **Account Management** view in the Settings module from a user account with user management permission. You can then use the same view to unlock the account.

Disabled appears as the **Status** of locked user accounts in the **Account Management** view.

Tip

If there are no accounts with user management permission, unlock the account by restarting the management server.

2.3.2 User account permissions

There are three permissions you can assign to user accounts in JP1/IT Desktop Management 2:

- System administrator permission
  A user with this permission has full access to the features of JP1/IT Desktop Management 2, with the exception of user account management. He or she can perform any operation except adding, editing, or deleting a user account.
- User management permission
  A user with this permission is able to manage JP1/IT Desktop Management 2 user accounts. He or she can add, edit, or delete a user account.
- View permission
  A user with this permission is able to view the information managed by JP1/IT Desktop Management 2. Users are assigned view permission by default.

2.3.3 Available operations by user account permission

The permission assigned to a user account determines the modules the user can access and the tasks the user can perform. The following table shows the operation windows and ranges of operations available to user accounts for each permission when task allocations and administration scopes are not limited.

Operation window		Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard		Y	N	N
Home module		Y	Y*	Y*
Security module		Y	Y*	Y*
Assets module				
Device module				
Distribution (ITDM-compatible) module				
Events module				
Reports module				
Settings module	**User Management** view	N	Y	N
	Windows other than **User Management** view	Y	N	N

Operation window	Permission		
	System administrator permission	User management permission	View permission
Print reports and security policies	Y		
View help	Y		

Legend: Y: Can operate. Y*: Can view only. N: Cannot operate or view.

2.3.4 Task allocations for user accounts

In JP1/IT Desktop Management 2, you can assign task allocations to user accounts according to the role of the administrator who uses the account. By setting up user accounts with the appropriate combination of task allocations and permissions, you can limit the operations an administrator can perform to those suited to his or her role. This promotes stronger internal controls because administrators can only manage information related to their field of responsibility.

There are five task allocations:

Security management

Limits the user to tasks such as editing and applying security policies, applying security measures to devices according to their danger level, and managing and applying program updates. Because the application of security measures involves the distribution of software and program updates, a user assigned this task allocation is automatically allocated distribution management tasks.

Asset management

Limits users to tasks related to the management of asset information such as the equipment held by the organization, software licenses, and contracts.

Device management

Limits users to tasks such as the management of device information, remote control of devices, and managing installed software.

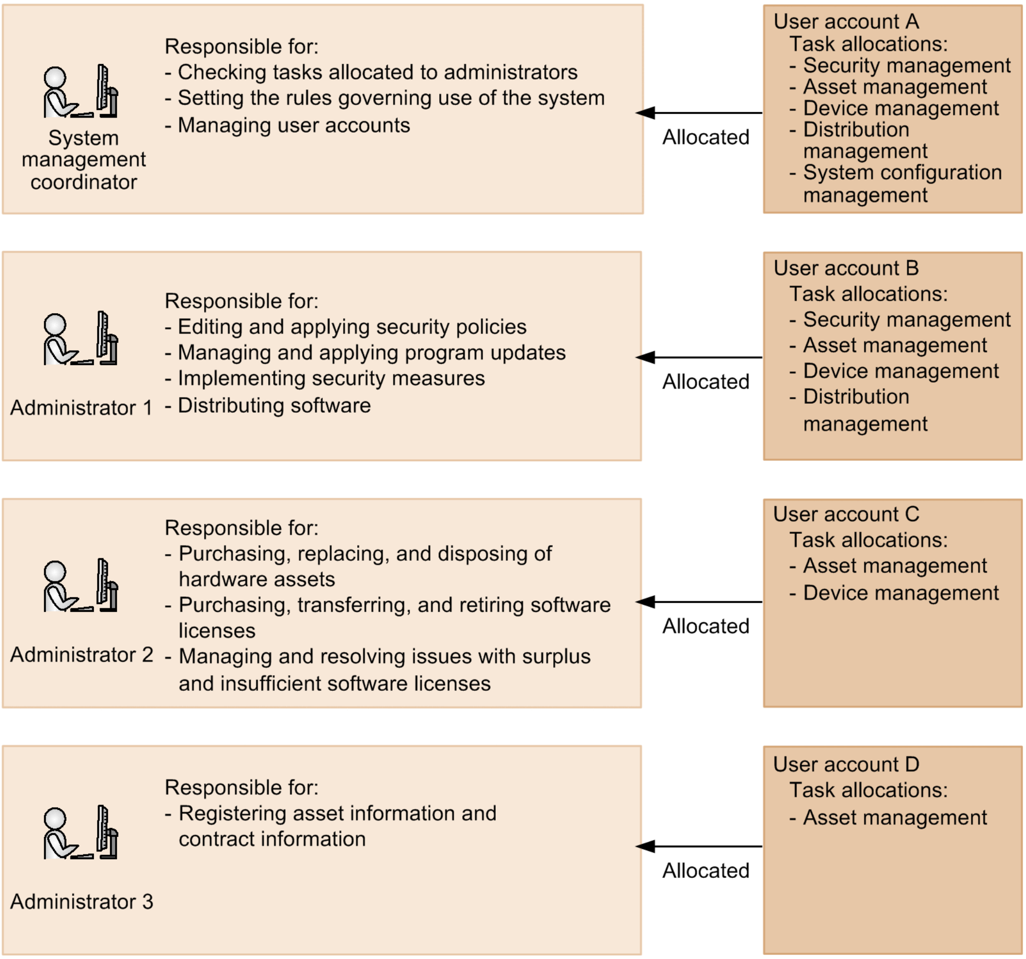
Distribution management

Limits users to tasks related to the distribution of software and files. A user who is allocated the distribution management and security management tasks can also distribute program updates.

System configuration management

Limits users to the management of configuration information for JP1/IT Desktop Management 2, such as configuring device search parameters, setting up agents, setting network control, and other tasks. Because these settings are essential to the running of JP1/IT Desktop Management 2, users with this task allocation must have system administrator permission. To add, edit, or delete user accounts, the user must also have user account management permission.

The following figure shows an example of assigning task allocations to user accounts according to the administrator's field of responsibility:


Responsible for:
- Checking tasks allocated to administrators
- Setting the rules governing use of the system
- Managing user accounts
System management coordinator
Allocated
User account A
Task allocations:
- Security management
- Asset management
- Device management
- Distribution management
- System configuration management
Responsible for:
- Editing and applying security policies
- Managing and applying program updates
- Implementing security measures
- Distributing software
Administrator 1
Allocated
User account B
Task allocations:
- Security management
- Asset management
- Device management
- Distribution management
Responsible for:
- Purchasing, replacing, and disposing of hardware assets
- Purchasing, transferring, and retiring software licenses
- Managing and resolving issues with surplus and insufficient software licenses
Administrator 2
Allocated
User account C
Task allocations:
- Asset management
- Device management
Responsible for:
- Registering asset information and contract information
Administrator 3
Allocated
User account D
Task allocations:
- Asset management

System management coordinator

A user responsible for coordinating overall system management. Because the system management coordinator is responsible not only for reviewing the task allocations of each management user, but also for managing all manner of JP1/IT Desktop Management 2 settings including operating procedures and user accounts, he or she must be assigned all task allocations.

Management user

A user responsible for day-to-day management of the system. Management users should only be assigned task allocations that are relevant to their fields of responsibility.

2.3.5 Available operations by task allocation

By assigning task allocations to a user account, you can limit the modules and menus available to the user and the tasks the user can perform. The range of available operations is determined from the user's permissions and task allocations.

Important note

In some cases, a module or menu accessible under a given task allocation contains items that are within the scope of a different task allocation. In this case, the user might be unable to display a particular module or perform a particular operation unless also assigned a task allocation that makes the item available. For example, the **Go to Device List** button does not appear on the **Asset Information** tab of the **Asset List area** in the Asset module for users who are only assigned the asset management task allocation. This is because operations in the

Device List view are within the scope of the device management task allocation. If an administrator needs to view the **Device List** view in the course of his or her work, the user account must be assigned the device management task allocation in addition to asset management.

Tip

If you assign an administration scope in addition to a task allocation, the information available within the scope of the task allocation is further restricted based on the department for which the administrator is responsible.

The following table shows the range of available user operations for each operation window, according to task allocation and permission.

The legend for the tables in this section is as follows:

Legend: Y: Can operate. Y*: Can view only. N: Cannot operate or view.

With security management set as task allocation

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard	None	N	N	N
Home module	None	Y	Y	Y
Security module	Overview	Y	Y	Y
	Security Policies	Y	Y*	Y*
	Computer Security Status	Y#1	Y*	Y*
	Windows Update	Y	Y*	Y*
	Operation Logs	Y	Y*	Y*
Assets module	All menus	N	N	N
Device module	All menus	N	N	N
Distribution (ITDM-compatible) module	Overview	Y	Y	Y
	Packages	Y	Y*	Y*
	Tasks	Y	Y*	Y*
Events module	Events	Y	Y*	Y*
Reports module	Overview	Y #2	Y #2	Y #2
	Summary Reports	Y	Y	Y
	Security Diagnosis Reports	Y	Y	Y
	Security Detail Reports	Y	Y	Y
	Inventory Detail Reports	N	N	N
	Asset Detail Reports	N	N	N
Settings module	Overview	Y #3	Y #3	N

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Settings module	User Management	N	Y	N
	Agent	N	N	N
	Device Discovery	N	N	N
	Network Access Control	N	N	N
	Security	Y	N	N
	Assets	N	N	N
	Inventory	N	N	N
	Reports	N	N	N
	Events	N	N	N
	General	N	N	N
	Product Licenses	N	N	N

#1: To edit the groups displayed in the device list, the following task allocations must be assigned.

- To edit device types, networks, and user definitions: Device management task allocation
- To edit departments and locations: Asset management task allocation

#2: Only an administrator with all task allocations can view or operate this item.

#3: The settings list is not displayed.

With asset management set as task allocation

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard	None	N	N	N
Home module	None	Y	Y	Y
Security module	All menus	N	N	N
Assets module	Overview	Y	Y	Y
	Hardware Assets	Y	Y*	Y*
	Software Licenses	Y	Y*	Y*
	Managed Software	Y	Y*	Y*
	Software License Status	Y	Y*	Y*
	Contracts	Y	Y*	Y*
Device module	All menus	N	N	N
Distribution (ITDM-compatible) module	All menus	N	N	N
Events module	Events	Y	Y*	Y*

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Reports module	Overview	Y [#1]	Y [#1]	Y [#1]
	Summary Reports	Y	Y	Y
	Security Diagnosis Reports	N	N	N
	Security Detail Reports	N	N	N
	Inventory Detail Reports	N	N	N
	Asset Detail Reports	Y	Y	Y
Settings module	Overview	Y [#2]	Y [#2]	N
	User Management	N	Y	N
	Agent	N	N	N
	Device Discovery	N	N	N
	Network Access Control	N	N	N
	Security	N	N	N
	Assets	Y	N	N
	Inventory	N	N	N
	Reports	N	N	N
	Events	N	N	N
	General	N	N	N
	Product Licenses	N	N	N

#1: Only an administrator with all task allocations can view or operate this item.

#2: The settings list is not displayed.

With device management set as task allocation

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard	None	Y	N	N
Home module	None	Y	Y	Y
Security module	All menus	N	N	N
Assets module	All menus	N	N	N
Device module	Overview	Y	Y	Y
	Device Inventory	Y[#1]	Y*	Y*
	Revision History	Y	Y*	Y*
	Software Inventory	Y	Y*	Y*

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Distribution (ITDM-compatible) module	All menus	N	N	N
Events module	Events	Y	Y*	Y*
Reports module	Overview	Y #2	Y #2	Y #2
	Summary Reports	Y	Y	Y
	Security Diagnosis Reports	N	N	N
	Security Detail Reports	N	N	N
	Inventory Detail Reports	Y	Y	Y
	Asset Detail Reports	N	N	N
Settings module	Overview	Y #3	Y #3	N
	User Management	N	Y	N
	Agent	Y	N	N
	Device Discovery	Y	N	N
	Network Access Control	N	N	N
	Security	N	N	N
	Assets	N	N	N
	Inventory	Y	N	N
	Reports	N	N	N
	Events	N	N	N
	General	N	N	N
	Product Licenses	N	N	N

#1: To edit departments and locations in the groups displayed in the device list, asset management task allocation must be assigned.

#2: Only an administrator with all task allocations can view or operate this item.

#3: The settings list is not displayed.

With distribution management set as task allocation

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard	None	N	N	N
Home module	None	Y	Y	Y
Security module	All menus	N	N	N
Assets module	All menus	N	N	N

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Device module	All menus	N	N	N
Distribution (ITDM-compatible) module	Overview	Y	Y	Y
	Packages	Y	Y*	Y*
	Tasks	Y	Y*	Y*
Events module	Events	Y	Y*	Y*
Reports module	Overview	Y #1	Y #1	Y #1
	Summary Reports	Y	Y	Y
	Security Diagnosis Reports	N	N	N
	Security Detail Reports	N	N	N
	Inventory Detail Reports	N	N	N
	Asset Detail Reports	N	N	N
Settings module	Overview	N	Y #2	N
	User Management	N	Y	N
	Agent	N	N	N
	Device Discovery	N	N	N
	Network Access Control	N	N	N
	Security	N	N	N
	Assets	N	N	N
	Inventory	N	N	N
	Reports	N	N	N
	Events	N	N	N
	General	N	N	N
	Product Licenses	N	N	N

#1: Only an administrator with all task allocations can view or operate this item.

#2: The settings list is not displayed.

With system configuration management set as task allocation

Operation window	Menu	Permission	
		System administrator permission	User management permission
Getting Started wizard	None	Y	N
Home module	None	Y	Y
Security module	All menus	N	N
Assets module	All menus	N	N

Operation window	Menu	Permission	
		System administrator permission	User management permission
Device module	All menus	N	N
Distribution (ITDM-compatible) module	All menus	N	N
Events module	Events	Y	Y*
Reports module	Overview	Y #1	Y #1
	Summary Reports	Y	Y
	Security Diagnosis Reports	N	N
	Security Detail Reports	N	N
	Inventory Detail Reports	N	N
	Asset Detail Reports	N	N
Settings module	Overview	Y	Y #2
	User Management	N	Y
	Agent	Y	N
	Device Discovery	Y	N
	Network Access Control	Y	N
	Security	Y	N
	Assets	Y	N
	Inventory	Y	N
	Reports	Y	N
	Events	Y	N
	General	Y	N
	Product Licenses	Y	N

#1: Only an administrator with all task allocations can view or operate this item.

#2: The Settings List is not displayed.

With no task allocations set

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard	None	N	N	N
Home module	None	Y	Y	Y
Security module	All menus	N	N	N
Assets module	All menus	N	N	N
Device module	All menus	N	N	N

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Distribution (ITDM-compatible) module	All menus	N	N	N
Events module	Events	Y	Y*	Y*
Reports module	Overview	N	N	N
	Summary Reports	Y	Y	Y
	Security Diagnosis Reports	N	N	N
	Security Detail Reports	N	N	N
	Inventory Detail Reports	N	N	N
	Asset Detail Reports	N	N	N
Settings module	Overview	N	Y #	N
	User Management	N	Y	N
	Agent	N	N	N
	Device Discovery	N	N	N
	Network Access Control	N	N	N
	Security	N	N	N
	Assets	N	N	N
	Inventory	N	N	N
	Reports	N	N	N
	Events	N	N	N
	General	N	N	N
	Product Licenses	N	N	N

#: The Settings List is not displayed.

With multiple task allocations set

When several task allocations are assigned to a user account, the available items are the items available to each task allocation combined. By way of example, the following table shows the scope of operations permitted for a user with the asset management and device management task allocations.

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Getting Started wizard	None	Y	N	N
Home module	None	Y	Y	Y
Security module	All menus	N	N	N
Assets module	Overview	Y	Y	Y
	Hardware Assets	Y	Y*	Y*

Operation window	Menu	Permission		
		System administrator permission	User management permission	View permission
Assets module	Software Licenses	Y	Y*	Y*
	Managed Software	Y	Y*	Y*
	Software License Status	Y	Y*	Y*
	Contracts	Y	Y*	Y*
Device module	Overview	Y	Y	Y
	Device Inventory	Y	Y*	Y*
	Revision History	Y	Y*	Y*
	Software Inventory	Y	Y*	Y*
Distribution (ITDM-compatible) module	All menus	N	N	N
Events module	Events	Y	Y*	Y*
Reports module	Overview	N	N	N
	Summary Reports	Y	Y	Y
	Security Diagnosis Reports	N	N	N
	Security Detail Reports	N	N	N
	Inventory Detail Reports	Y	Y	Y
	Asset Detail Reports	Y	Y	Y
Settings module	Overview	Y #	Y #	N
	User Management	N	Y	N
	Device Discovery	Y	N	N
	Agent	Y	N	N
	Network Access Control	N	N	N
	Security	N	N	N
	Assets	Y	N	N
	Inventory	Y	N	N
	Reports	N	N	N
	Events	N	N	N
	General	N	N	N
	Product Licenses	N	N	N

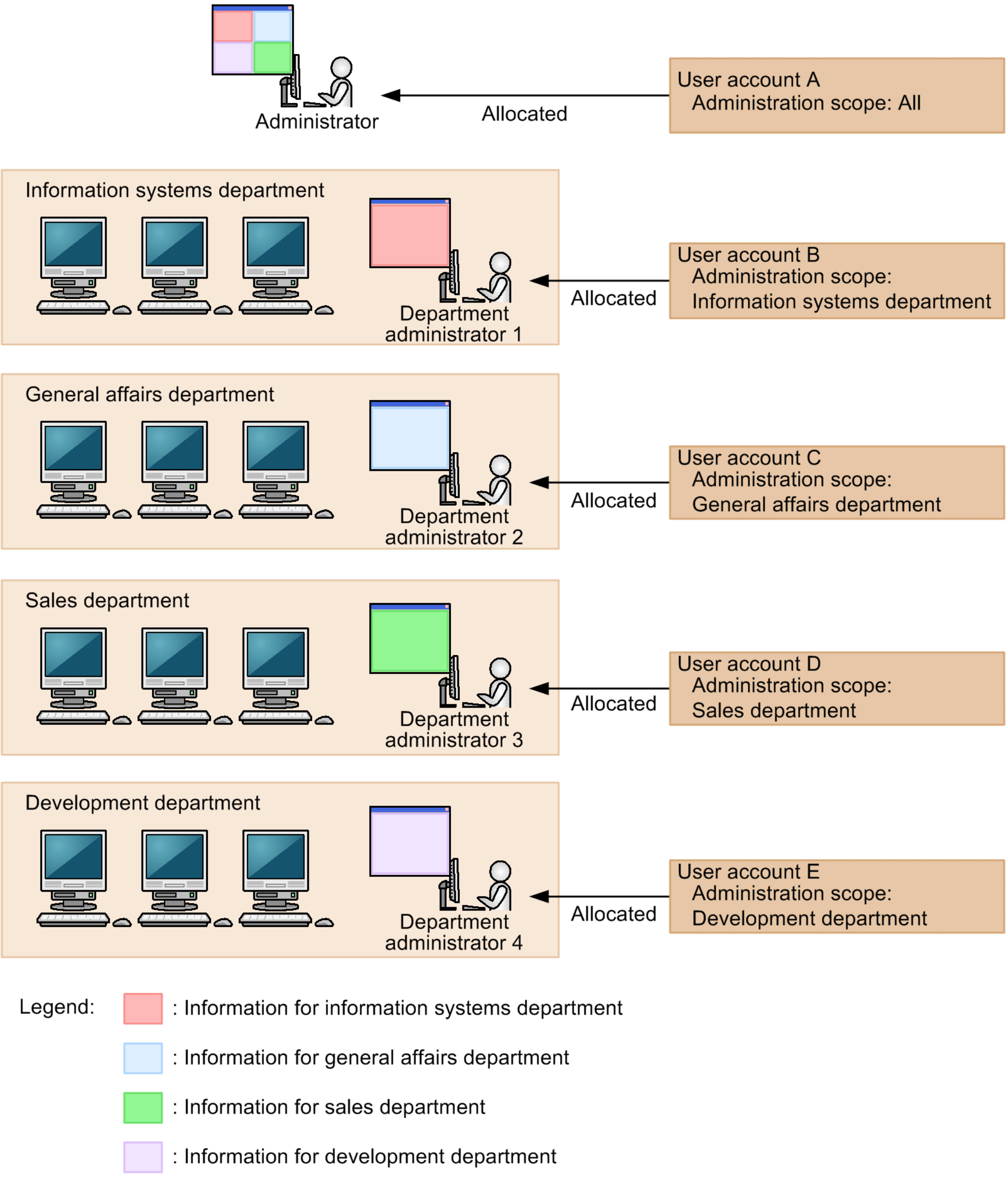
#: The Settings List is not displayed.

2.3.6 Administration scopes for user accounts

You can assign an *administration scope* to a user account in JP1/IT Desktop Management 2 according to the department for which the administrator is responsible. When a company has more devices than a single administrator can manage, you can assign administrators to individual departments. When designated as a department administrator, an administrator can view and manage devices and hardware assets associated with that department.

Note that administration scope settings are not applied to distribution that uses Remote Installation Manager.

The following figure shows an example of allocating administration scopes to user accounts for use by department administrators.


Administrator
Allocated
User account A
Administration scope: All
Information systems department
Department administrator 1
Allocated
User account B
Administration scope: Information systems department
General affairs department
Department administrator 2
Allocated
User account C
Administration scope: General affairs department
Sales department
Department administrator 3
Allocated
User account D
Administration scope: Sales department
Development department
Department administrator 4
Allocated
User account E
Administration scope: Development department
Legend:
🟥 : Information for information systems department
🟦 : Information for general affairs department
🟩 : Information for sales department
🟪 : Information for development department

Administrator

Manages the systems for the entire organization. By using an account with no administration scope, an administrator can view information for all departments.

Department administrator

Manages the systems for a particular department. By using an account with an administration scope, a department administrator only has access to information for the department for which he or she is responsible.

2.3.7 Differences in operation windows when administration scopes are assigned

When you use a user account that is limited to a particular administration scope, only the information applicable to that administration scope appears in the modules, and the operations you can perform are similarly restricted. The following table shows how the operation windows appear to users who are assigned a administration scope.

Operation module		Differences when administration scope is restricted
Home module	Home module	The following items do not appear: • welcome message • **Getting Started** button • **Getting Started Wizard** item in **Go** menu
	System Summary panel	**Used Licenses** are not clickable links.
	Not Ack Event Summary panel	Only information applicable to the administration scope appears.
	Topic panel	Some messages are not clickable links. In addition, some messages only contain information applicable to the administration scope.
	Background Task panel	The following items are not clickable links: • **Error** • **IP Address Range** • **Active Directory**
	DB and Disk Usage panel	--
	# of Devices by Violation Level panel	Only information applicable to the administration scope appears.
	Security Status by Policy panel	--
	Suspicious Operations panel	Only information applicable to the administration scope appears.
	Customized Device Inventory (Group/Filter) panel	Only information applicable to the administration scope appears.
	Customized HW Assets (Group/ Filter) panel	Only information applicable to the administration scope appears.
	Category Security Assessment panel	Only information applicable to the administration scope appears.
	Hardware Assets Trend panel	--
	Expired Contracts (next 3 months) panel	Only information applicable to the administration scope appears.
	Software (License Violation) panel	Only information applicable to the administration scope appears.
	# of Devices by OS panel	Only information applicable to the administration scope appears.

Operation module		Differences when administration scope is restricted
Home module	**Managed Nodes Trend** panel	--
	New Software panel	--
	Task Status panel	--
	Error Task Status panel	Only information applicable to the administration scope appears.
Security module	**Overview** view#	The range of information displayed depends on the panel.
	Security Policies view	The administrator can view but not edit the information. The tabs in the lower pane of the information area provide the same operations as when the administration scope is not restricted.
	Computer Security Status view	Only information applicable to the administration scope appears. The following items do not appear in the **Action** menu: • **Assign Policy** • **Cancel Policy** • **Enable Network Access Control** • **Disable Network Access Control** Messages about disabled network monitors do not appear in the message bar.
	Windows Update view	The administrator can view but not edit the information. **Update Information from Customer Support Offline** does not appear in the **Action** menu.
	Operation Logs view	Only information applicable to the administration scope appears.
Assets module	**Overview** view#	The range of information displayed depends on the panel.
	Hardware Assets view	Only information applicable to the administration scope appears. **Enable End User Form (Frequent Pop-up)** does not appear in the **Action** menu. In dialog boxes where hardware asset information can be added and edited, icons do not appear to the left of management items. You cannot add new items to the dialog boxes.
	Software License view	Only information applicable to the administration scope appears. The **Assigned Computers** tab also displays information not applicable to the administration scope. This information can be used for removing software licenses that are no longer required in departments after department information has changed. In dialog boxes where software license information can be added and edited, icons do not appear to the left of management items. You cannot add new items to the dialog boxes, with the exception of the **Managed Software Name** item.
	Managed Software view	**Update Information from Customer Support Offline** does not appear in the **Action** menu. The **Add as Unauthorized Software** button does not appear on the **Installed Software** tab.
	Software License Status view	Only information applicable to the administration scope appears.

Operation module		Differences when administration scope is restricted
Assets module	**Contracts** view	Only information applicable to the administration scope appears. In dialog boxes where contract information can be added and edited, icons do not appear to the left of management items. You cannot add new items to the dialog boxes.
Devices module	**Overview** view#	The range of information displayed depends on the panel.
	Device Inventory view	Only information applicable to the administration scope appears. The following items do not appear in the **Action** menu: • **Enable End User Form (Frequent Pop-up)** • **Enable Network Access Control** • **Disable Network Access Control** • **Set Credentials** Messages about disabled network monitors do not appear in the message bar. In dialog boxes where device information can be edited, icons do not appear to the left of management items. You cannot add new items to the dialog boxes.
	Revision History view	Only information applicable to the administration scope appears.
	Software Inventory view	**Remove Software** and **Update Information from Customer Support Offline** do not appear in the **Action** menu. The **Add as Unauthorized Software** button does not appear on the **Installed Software** tab.
Distribution (ITDM-compatible) module	**Overview** view#	The range of information displayed depends on the panel.
	Packages view	--
	Tasks view	--
Events module		For events whose source is device information or asset information, only information applicable to the administration scope appears. Some messages do not appear as links.
Reports module	**Overview** view	--
	Summary Reports	--
	Security Diagnosis Reports	Reports are limited to information gathered within the administration scope of the user.
	Security Detail Reports	The following reports are limited to information gathered within the administration scope of the user: • **Violation Level Status** report • **Windows Update Status** report • **Antivirus Software Status** report • **Mandatory Software Status** report • **Unauthorized Software Status** report • **Security Settings Status** report
	Inventory Detail Reports	Reports are limited to information gathered within the administration scope of the user.
	Asset Detail Reports	Reports are limited to information gathered within the administration scope of the user.

Operation module		Differences when administration scope is restricted
Settings module	**Overview** view	Only the **Product Site Map** window appears.
	User Management view	--
	Agent view	In the **Agent Configuration and Installation Set Creation** view, the user can only refer to the information. In the **Agent Configurations** view, the user can view but not edit information. In the **Agent Configurations Assignment** view, only information applicable to the administration scope appears. The **Change Target Group Type** button, **Assign** button, and **Cancel** button at the top of the information area are unavailable. In the **Agent Distribution** view, only the information in the administration scope appears. The **Agentless Management** view does not appear.
	Device Discovery view	Only the following views can be displayed, and only information applicable to the administration scope appears in these views: • **Discovered Nodes** view • **Managed Nodes** view • **Ignored Nodes** view Note that in the **Discovered Nodes** and **Managed Nodes** views, **Set Credentials** and **Start Discovery** do not appear in the **Operation Menu**.
	Network Access Control view	Not displayed.
	Security view	Not displayed.
	Assets view	Only the **Last Import Log** view can be displayed.
	Inventory view	Not displayed.
	Reports view	Not displayed.
	Events view	Not displayed.
	General view	Not displayed.
	Product Licenses view	Not displayed.

Legend: --: Restricting the administration scope has no effect.

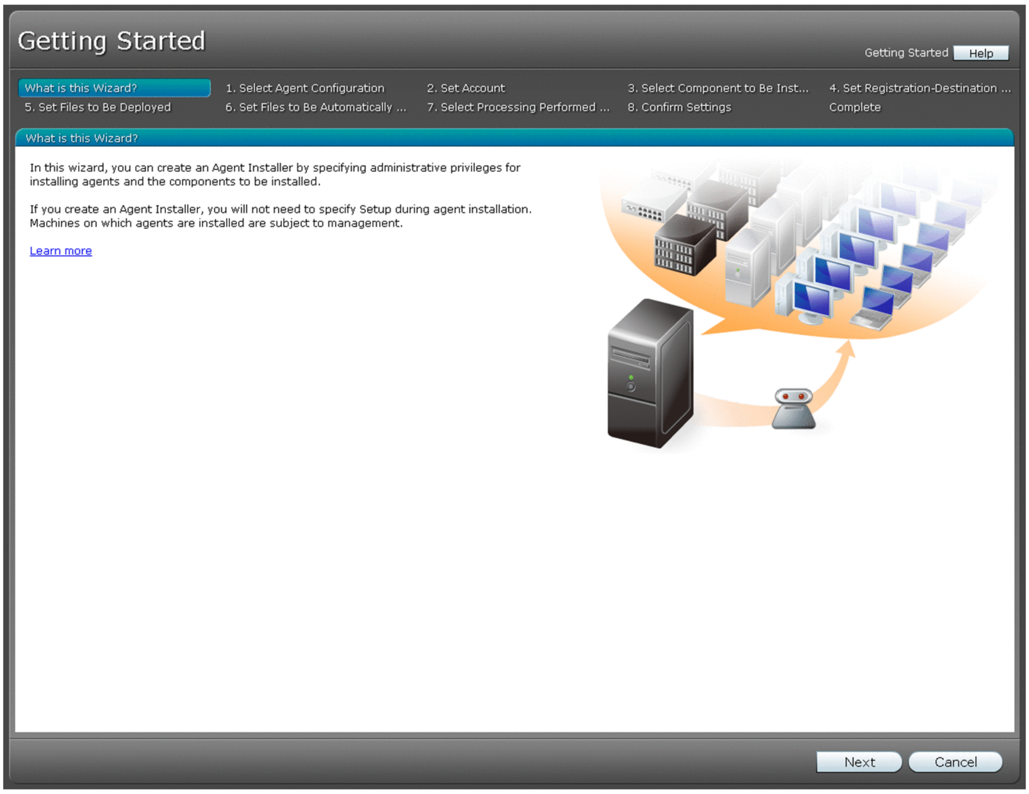
#: The panels in the **Overview** view are the same as those in the Home module.

Tip

If you log in using an account with a administration scope, you cannot edit the department information (the **Department** management item) that appears in the menu and other areas of each module.

2.4 Using the Getting Started wizard

When you log in to JP1/IT Desktop Management 2, you can access the **Getting Started** wizard by clicking the **Getting Started** button in the Home module. This wizard guides you through the initial stages of JP1/IT Desktop Management 2 operation.


Getting Started
Getting Started
Help
What is this Wizard?
1. Select Agent Configuration
2. Set Account
3. Select Component to Be Inst...
4. Set Registration-Destination ...
5. Set Files to Be Deployed
6. Set Files to Be Automatically ...
7. Select Processing Performed ...
8. Confirm Settings
Complete
What is this Wizard?
Learn more
Next
Cancel

In this wizard, you can create an Agent Installer by specifying administrative privileges for installing agents and the components to be installed.

If you create an Agent Installer, you will not need to specify Setup during agent installation. Machines on which agents are installed are subject to management.

By following the prompts in the wizard, you can create an installer file (installation set) for installing an agent on the computer. Executing this file on each computer installs the agent on each computer. For details, see the description on manually installing an agent in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Configuration Guide*.

You can also install an agent on a computer by Active Directory discovery and network discovery.

2.4.1 Discovering devices

You can search for devices connected to the network or registered in Active Directory, and register discovered devices as management targets.

Searching the network

You can search the network within a specified IP address range. You can also set authentication information, enabling JP1/IT Desktop Management 2 to gather information from devices as part of the search process.

If you do not have a clear picture of the devices deployed throughout your organization, you can gather the information you need by conducting a search. You can then plan agent deployment based on the results of the search process.

Searching Active Directory

If your organization uses Active Directory, you can search for computers registered in Active Directory. You can search multiple Active Directory servers if needed. The discovery process acquires information registered in Active Directory.

By registering the information obtained from Active Directory in JP1/IT Desktop Management 2, you can use the information in reports and to manage devices.

As part of the search process, you can automatically designate discovered devices as management targets, and automatically distribute the agent program to discovered computers. You can also configure the system to notify the administrator by email when a new device is discovered.

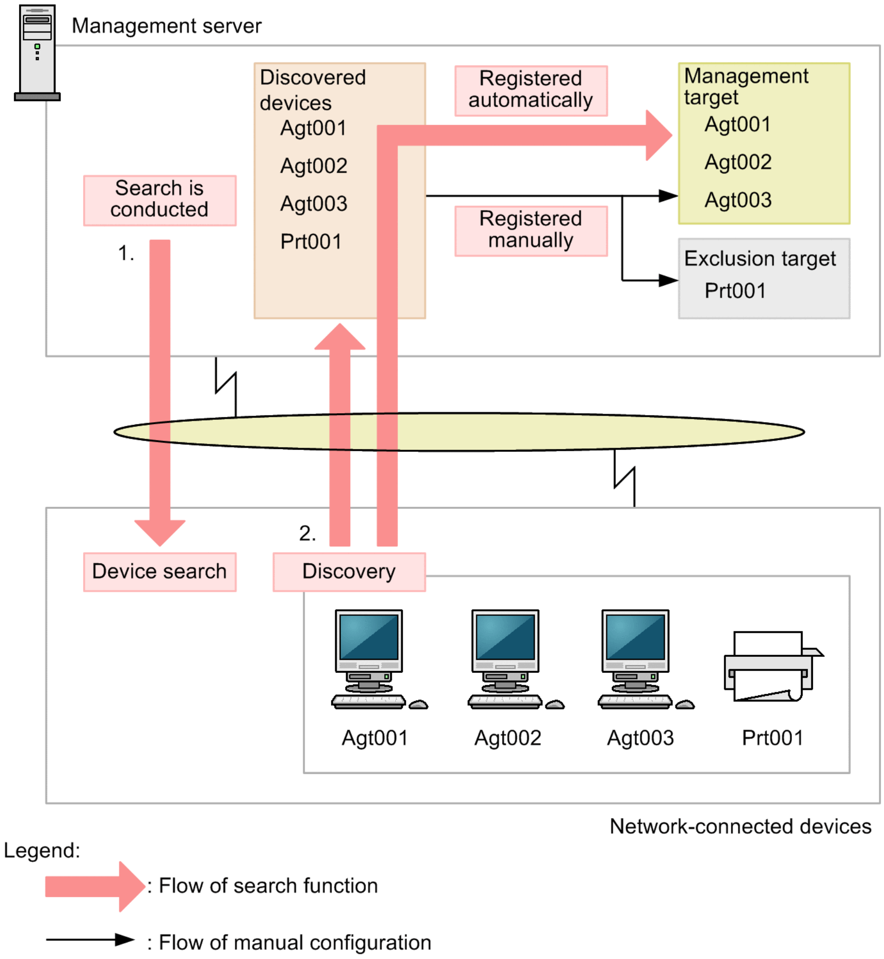
2.4.2 Discovering networked devices

You can search for devices connected to a network, and register discovered devices as management targets of JP1/IT Desktop Management 2.

You can search a specific range of network addresses for devices. You can register discovered devices such as computers that require security management as management targets, and devices such as routers that do not require security management as exclusion targets.

As part of the search process, you can automatically register discovered devices as management targets, and automatically distribute the agent program to discovered computers. You can also configure the system to notify the administrator by email when a new device is discovered.

The following figure shows an overview of searching for devices and registering discovered devices as management targets.



1. On the management server, search for devices on a routine basis by specifying a network range to search, a discovery schedule, and other parameters.

   Important note

   To conduct an intensive search for devices in the network by specifying a discovery period, specify 50,000 or less IP addresses in the discovery range. If more than 50,000 IP addresses are contained, the search might stop.

   Tip

   Management servers can connect to a maximum of 10 devices at once during a search.

2. Discovered devices can be registered as management targets automatically, or set aside to be manually registered as a management target or exclusion target at a later time.

Related Topics:

- (1) Devices supported as management targets
- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information

(1) Discovery conditions

Several conditions must be met before you can discover devices. Each discovery method has different conditions.

Discovering devices in Active Directory

The correct settings must be specified for the connection-target Active Directory server in the **Active Directory** view under **General** in the Settings module.

Discovering networked devices

The following conditions must be satisfied:

- If a device to be discovered is in the same segment as the management server, the device must respond to ARP requests from the management server.
- If a device to be discovered is in a different segment from the management server, the device must respond to ICMP ECHO (`ping`) from the management server.
- Devices must have IP addresses assigned
- The discovery range must be set correctly
- Authentication information must be set correctly

You can set the discovery range and authentication information in the **IP Address Range** view accessed by clicking **Configurations** under **Discovery** in the Settings module.

The prerequisites for a network environment in which devices can be discovered are as follows:

- The network supports TCP/IP communication and the firewall settings and other parameters permit communication through chosen ports.
- The management server and managed devices are able to communicate with each other via ICMP.

Important note

Virtual machines are treated as separate computers for discovery purposes. The guest OS of a virtual machine must be assigned its own IP address and MAC address separate from those assigned to the host OS.

Important note

You cannot manage agentless devices in a NAT environment.

Important note

By default, computers running Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003 (Service Pack 2 or later), or Windows XP (Service Pack 2 or later) cannot use ICMP due to Windows firewall settings. To use ICMP in the discovery process, ICMP must be enabled in the configuration of the computer being discovered.

Important note

Do not specify a discovery range that includes a loop-back address or broadcast address. Searches whose discovery range contains such an address might discover devices wrongly.

Tip

You can discover devices that use a wireless LAN, WAN, or VPN, provided that the network environment meets the above prerequisites.

You can automatically distribute the agent program to discovered computers that are running Windows. For details about the conditions that must be met for this to occur, see 2.5.2 Criteria for agent distribution to online-managed computers.

(2) Estimating data traffic during network searches

The following shows general guidelines for estimating how much traffic is generated by a network search.

When using SNMP authentication

If SNMP authentication is successful, approximately 2 KB of data is sent per device.

When using Windows administrative shares

If login to the Windows administrative share is successful, approximately 2.5 MB of data is sent per device. Agent distribution uses approximately 80 MB of data traffic. The data traffic varies depending on the agent configuration.

2.4.3 Linking with Active Directory

By linking with Active Directory, you can retrieve information about devices registered on an Active Directory server, and register those devices with JP1/IT Desktop Management 2. You can also obtain information like user names, telephone numbers, and email addresses that JP1/IT Desktop Management 2 cannot collect automatically.

By acquiring department and location information from Active Directory, you can also synchronize the group relationships of managed devices and asset information with the organizational units (OU) managed by Active Directory.

Device information available from Active Directory

The following table describes some of the features that become available when you link with Active Directory.

Feature	Description
Device registration	This feature lets you discover the computers managed by Active Directory and register them as management targets in JP1/IT Desktop Management 2. You can also update system information based on information provided by Active Directory.
Information retrieval	From the information managed by Active Directory, you can retrieve shared management items relating to device information and hardware asset information, and added management items relating to hardware asset information. Note that **Active Directory** must be set as the data source for the item.
Retrieval of organizational hierarchy	You can import the hierarchy of organizational units (OU) managed by Active Directory and use it to define the group configuration in JP1/IT Desktop Management 2.

The following table shows the device information you can acquire from Active Directory.

Type of device information		Linkage with Active Directory	
		Device registration	Information retrieval
Device type	PC (Windows)	Y	Y
	Server (Windows)	Y	Y
System information	Computer information	Y	N
	OS information	Y	N
	Network information	Y	N
Shared management items		Y	Y
Added management items		Y	Y

Legend: Y: Can be acquired. N: Cannot be acquired.

For details about the device information you can acquire from Active Directory, see (3) Device information that can be acquired from Active Directory.

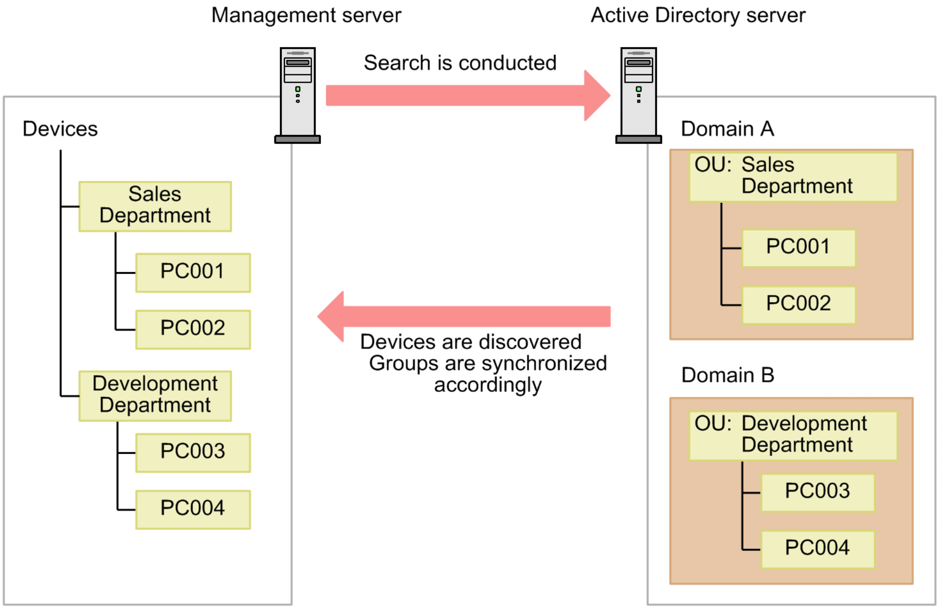
Timing of device information acquisition

If JP1/IT Desktop Management 2 is configured to link with Active Directory, it searches the Active Directory database daily at 23:00 and acquires the relevant device information. You can change the time and frequency of this search by setting a discovery schedule in the **Active Directory** view under **Configurations** in the **Discovery** area of the Settings module.

(1) Searching for devices in Active Directory

You can search for computers managed in Active Directory domains and root OUs and register them as management targets. We recommend that you use this method if your organization already uses Active Directory to manage computers.

The following figure shows an overview of searching Active Directory for devices.



Options for device discovery

You can use the following methods to search for devices registered in Active Directory.

Immediate

JP1/IT Desktop Management 2 connects to Active Directory and searches for devices, acquiring device information for the devices it discovers. Use this option when you first install JP1/IT Desktop Management 2 or when you want changes to Active Directory information to be immediately reflected in the JP1/IT Desktop Management 2 database. You can begin a search from the **Active Directory** link under **Discovery Condition Configuration** in the **Device Discovery** view in the Setting module.

> **Tip**
>
> If you cancel the search before it finishes, any computer information and group information that has been acquired to that point is incorporated into the database.

Scheduled

Regular searches take place according to the discovery settings specified for Active Directory. During this process, device information is acquired for discovered devices. The discovery schedule is determined by the values in **Start At**, **Repeat Interval** (daily, weekly, or monthly), and **Repeat** in the Settings module. By default, discovery takes place daily at 23:00.

> **Tip**
>
> If the search is interrupted or cannot take place at the scheduled time because the service is stopped, the system is shut down, or for some other reason, it will take place at the next scheduled start time.
>
> If the search is interrupted, the process begins again for all computers the next time the service starts. Even if several search attempts have failed, this process takes place only once.

You can check the status of the search in the Last Discovery Log window accessed from the **Discovery** view in the Settings module. To notify the administrator by email when the process is finished, set a **Notice of Discovery Completion** in the **Discovery** view.

Removing managed devices

When you delete a computer from Active Directory, the corresponding information is not deleted from JP1/IT Desktop Management 2. To remove a computer that was discovered from Active Directory, remove it manually from the JP1/IT Desktop Management 2 database.

Discovery conflicts

The discovery of devices registered in Active Directory can sometimes conflict with other forms of discovery.

Conflicts with other Active Directory searches

If Active Directory is already being searched when a search is scheduled to start, the latter process is canceled until the next scheduled start time.

Conflicts with network searches

If a network search is already in progress, the Active Directory search takes place as normal. If both processes discover the same device, the results of network discovery using administrative shares and SNMP take priority over the results of Active Directory discovery, and the results of Active Directory discovery take priority over the results of network discovery using ARP and ICMP.

Related Topics:

- (4) Importing departmental group configurations from Active Directory

(2) Setting connection destinations for Active Directory searches

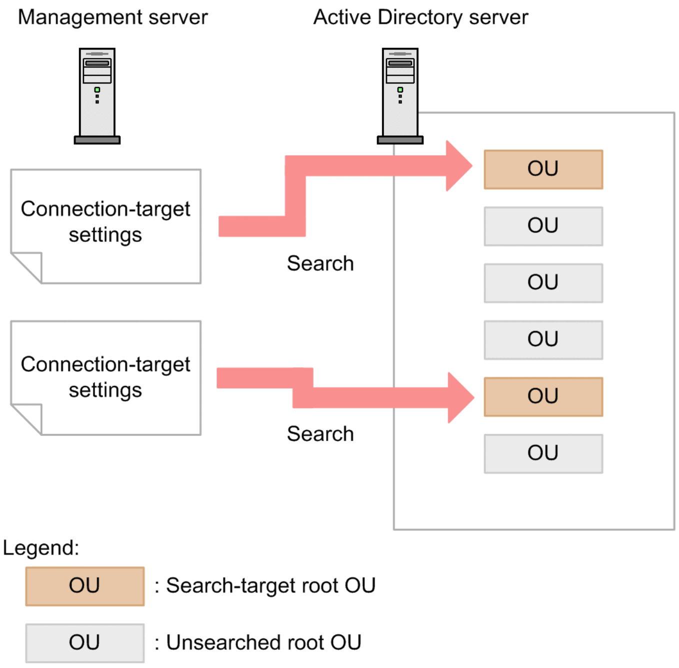
Before you can use Active Directory to search for and discover devices, you need to specify the connection-target Active Directory server and the root OU of the domains you want to search.

You can specify multiple connection targets, each consisting of an Active Directory address and a root OU. Set a number of connection targets equivalent to the number of Active Directory servers and root OUs where you want to discover devices.

The following are examples of setting connection targets for Active Directory searches.

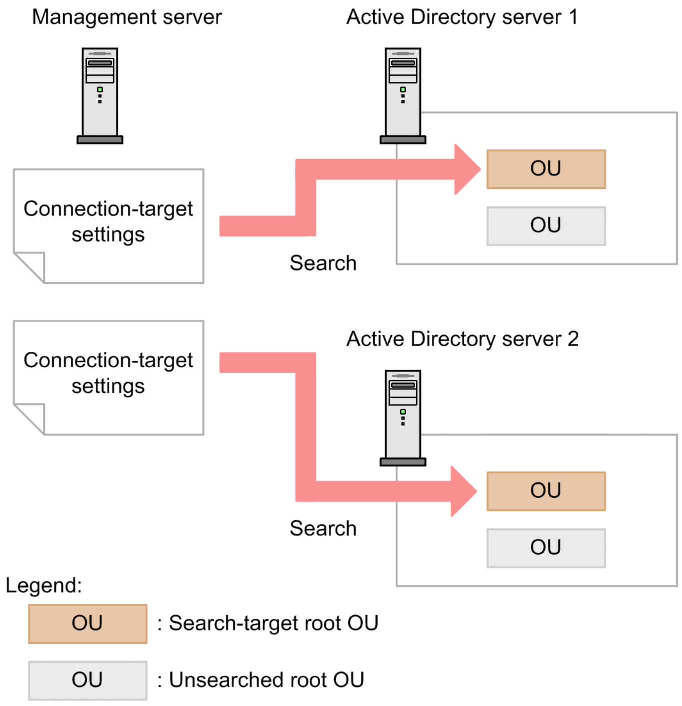
When connecting to one Active Directory server and discovering devices in multiple root OUs

Although the management server only connects to one Active Directory server, it searches for devices in multiple root OUs. This means that you need to create a number of connection destination settings equivalent to the number of root OUs.



When connecting to several Active Directory servers

When searching for devices on several Active Directory servers, you need to create a connection destination setting for each Active Directory server.


Management server
Active Directory server 1
Connection-target settings
Search
OU
OU
Connection-target settings
Active Directory server 2
Search
OU
OU
Legend:
OU : Search-target root OU
OU : Unsearched root OU

(3) Device information that can be acquired from Active Directory

The following table lists the device information you can obtain from an Active Directory server.

System information

Device information item		Source		Contents
		Object name (LDAP)	Attribute name (LDAP)	
Device type		computer	operatingSystem	`PC` is set for client-type OSs. For server-type OSs, `server` is set.
Computer information	Computer name	computer	sAMAccountName	Acquires the computer name of the computer.
	Host name	computer	dNSHostName	Acquires the DNS name of the computer if one is assigned.
		computer	sAMAccountName	Acquires the computer name of the computer if no DNS name is assigned.
OS information	OS	computer	operatingSystem	Acquires the name of the OS.
	OS service pack	computer	operatingSystemServicePack	Acquires information about the OS service pack.
Network information	IP address	--	--	Uses DNS to resolve an IP address from the host name.
	MAC address	--	--	Uses ARP to acquire a MAC address from the IP address.

Legend: --: Although this device information can be acquired from Active Directory, it does not appear on the source Active Directory server.

You can also acquire the information in the following table:

Device information item	Description
Registered Date/Time	For a newly discovered device, the date and time when the device was discovered is acquired. When updating device information, the existing date and time is left unchanged.
Last Modified Date/Time	If the device has been modified, the date and time when the device was modified is acquired. No date and time is acquired if the device information has not been modified.
Mode	If the **Auto-Manage Discovered Nodes** option is selected and the device has a product license, `Managed` is set. If the **Auto-Manage Discovered Nodes** option is selected and the device does not have a product license, `Discovered` is set. If the **Auto-Manage Discovered Nodes** option is not selected, `Discovered` is set.
Management Type	Agentless Management (Authentication Successful) is set.
Connection settings	`Unknown` is set.
Device Status	`Unknown` is set.
Management Status	`Agent not Installed` is set.
Last Alive Confirmation Date/Time	The date and time when the server last connected to the Active Directory and found the device.

Common management items

Shared management items	Source		Contents
	Object name (LDAP)	Attribute name (LDAP)	
Department	computer	distinguishedName#1	Acquires the department with which the device is associated.
Location	computer	location	Acquires the location of the device.
User Name	User or InetOrgPerson#2	displayname	Acquires the user name of the device.
Account	User or InetOrgPerson#2	userPrincipalName	Acquires the account name of the device.
E-mail	User or InetOrgPerson#2	mail	Acquires the e-mail address of the user of the device.
Phone	User or InetOrgPerson#2	telephoneNumber	Acquires the telephone number of the user of the device.

#1: Organization unit (OU) values in attributes are subjected to conversion before being registered in the common management item. For example, if the attribute value is `CN=PC001,OU=2U,OU=Design1G,OU=DesignDivision,DC=domain,DC=local`, then `DesignDivision/Design1G/2U` is registered as the department.

#2: The User or InetOrgPerson object associated with the managedBy attribute of the computer object.

Added management items

You can use the following methods to relate information retrieved from Active Directory to added management items.

Legend: Y: Template provided. N: No template provided.

Item specification

A method that uses supplied templates to specify objects in the Active Directory database.

For example: `Name (Computer)`

Customized

A process whereby the administrator specifies the object names managed by Active Directory and the LDAP attribute names.

Added management items are acquired as character string data.

The following table shows the objects you can acquire for each entity specified when acquiring information from Active Directory.

Specifiable entity	Associated object	Description
Computer	Computer	Used to manage computer information.
Organizational unit (OU)	Organization Unit (OU)	Contains `Computer`, `User`, and other values of `Organization Unit`. This information is used to record the department and location of a device, and to acquire information about the organizational unit (OU) to which a computer belongs.
User	User	Used to acquire information about the administrator of a computer.
	InetOrgPerson#	A type of user. This object is used to acquire information about the administrator of a computer.

#: In Windows 2000, you must apply the InetOrgPerson Kit to use this object.

The following table lists the information that can be acquired from the `Computer` object.

Item name	LDAP attribute name	Template provided
Name (Computer)	sAMAccountName	Y
DNS Host Name	dNSHostName	Y
Description	description	Y
Name	operatingSystem	N
Version	operatingSystemVersion	N
Service Pack	operatingSystemServicePack	N
Location	location	Y
Name (User)	managedBy	Y
Office Location	--#	N
Country	--#	N
State	--#	N
City	--#	N
Address	--#	N
Phone	--#	N
FAX	--#	N
Canonical name of object	distinguishedName	N

#: Shows the corresponding attribute value for the User or inetOrgPerson object whose value is the same as `Name (User)`. For details on the LDAP attribute names used to acquire this information, see the tables later in this section that show the information that can be acquired from the User and InetOrgPerson objects.

The following table lists the information that can be acquired from an Organization Unit (OU) object.

Property name	LDAP attribute name	Template provided
Country	co	Y
Zip code	postalCode	N
State	st	N
City	l	N
Address	street	N
Description	description	N
Name	managedBy	Y
Link to group policy object	gPLink	N

The following table lists the information that can be acquired from a User object.

Item name	LDAP attribute name	Template provided
Last Name	sn	Y
First Name	givenName	Y
Initials	initials	Y
Display Name	displayName	Y
Description	description	Y
Office Location	physicalDeliveryOfficeName	Y
Phone	telephoneNumber	Y
E-Mail	mail	Y
Web Page	wWWHomePage	Y
Country	co	Y
Zip code	postalCode	Y
State	st	Y
City	l	Y
P. O. Box	postOfficeBox	Y
Address	streetAddress	Y
Logon name	userPrincipalName	Y
Logon name (Windows 2000 or earlier)	sAMAccountName	N
Log on to	userWorkstations	N
User profile profile path	profilePath	N
User profile logon script	scriptPath	N

Item name	LDAP attribute name	Template provided
Home folder Local path	homeDirectory	N
Home folder Connect	homeDrive	N
Home phone	homePhone	Y
Pager	pager	Y
Mobile	mobile	Y
FAX	facsimileTelephoneNumber	Y
IP Phone	ipPhone	Y
Notes	info	Y
Company	company	Y
Department	department	Y
Job title	title	Y
Manager Name	manager	Y
Report Direct	directReports	Y

The following table lists the information that can be acquired from an InetOrgPerson object.

Item name	LDAP attribute name	Template provided
Last Name	sn	Y
First Name	givenName	Y
Initials	initials	Y
Display Name	displayName	Y
Description	description	Y
Office Location	physicalDeliveryOfficeName	Y
Phone	telephoneNumber	Y
Email	mail	Y
Web Page	wWWHomePage	Y
Country	co	Y
Zip code	postalCode	Y
State	st	Y
City	l	Y
P. O. Box	postOfficeBox	Y
Address	streetAddress	Y
Logon name	userPrincipalName	Y
Logon name (Windows 2000 or earlier)	sAMAccountName	N
Log on to	userWorkstations	N
User profile profile path	profilePath	N

Item name	LDAP attribute name	Template provided
User profile logon script	scriptPath	N
Home folder Local path	homeDirectory	N
Home folder Connect	homeDrive	N
Home Phone	homePhone	Y
Pager	pager	Y
Mobile	mobile	Y
FAX	facsimileTelephoneNumber	Y
IP Phone	ipPhone	Y
Notes	info	Y
Company	company	Y
Department	department	Y
Job Title	title	Y
Manager Name	manager	Y
Report Direct	directReports	Y

Important note

Although you can specify attributes that acquire information from items not mentioned in these tables, operation is not guaranteed in these circumstances.

For a detailed description of device information, see the following sections:

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

(4) Importing departmental group configurations from Active Directory

By importing information about the structure of organizational units (OU) from Active Directory, you can synchronize the department hierarchy maintained by JP1/IT Desktop Management 2 with the Active Directory OUs. By actively maintaining the department group configuration managed by Active Directory, you can centrally manage the configuration of managed devices.

JP1/IT Desktop Management 2 imports information about organizational units as part of the search process.

When you specify an organizational unit (root OU) that you want to import from Active Directory, the group configuration for its subordinate OUs is automatically created in the corresponding department group. To import information about department group hierarchies from Active Directory, select **Get Department Hierarchy**

Information in the **Active Directory** view accessed from the **General** menu. When this check box is selected, the manager collects department group information when it accesses Active Directory to search for devices. For details on searching Active Directory for devices, see (1) Searching for devices in Active Directory.

The following table shows the effect that importing organizational units (OUs) from Active Directory has on the JP1/IT Desktop Management 2 group configuration.

Active Directory organizational unit (OU)	JP1/IT Desktop Management 2 department group configuration	
	Present	Not present
Present	If the name is different, the group name is updated accordingly.	The group is added.
Not present	The group is removed.	No action taken.

Note that changing the department group configuration in JP1/IT Desktop Management 2 does not affect the organizational units (OU) registered on the Active Directory server.

Important note

After the import process, do not manually add, change, or remove any part of a department group configuration that is synchronized with Active Directory. Any such changes will be overwritten when organizational unit (OU) information is next imported.

If a managed device belongs to a group that is synchronized with an Active Directory OU, the group affiliation of the device changes in line with the Active Directory OU. If the group to which the device belongs is removed, the device is reassigned to the `Unknown` group.

Tip

If you specify an upper-level domain and its lower-level domain simultaneously in a domain name attribute, the manager imports information for the organizational unit (OU) of the upper-level domain, which includes the information for lower-level domains.

(5) Cautionary notes for Active Directory linkage

Note the following when linking with Active Directory:

- You cannot acquire information from an organizational unit (OU) that does not contain at least one computer.
- Even if a computer is registered in Active Directory, you cannot acquire device information if the computer is not a JP1/IT Desktop Management 2 management target.
- Only character string data can be acquired from Active Directory.
- You cannot use certain single-byte symbols and tab characters in the name of an OU in Active Directory.#

#: Do not use the following symbols: !, ", %, ', *, /, : (colon), <, >, ?, @, \, ｜, +, =, , (comma), or ; (semicolon). The linkage function might not operate correctly if an OU name contains any of these characters.

2.4.4 Detecting devices by using the network monitoring function

You can detect a new device attempting to access the network by enabling the network monitor for the network segment groups displayed in the Network List view. To display the Network List view, in the Device module, select **Device Inventory** and then **Network List**. A network search is automatically performed for the detected device. If the device is discovered, its access to the network is controlled according to the network monitor settings.

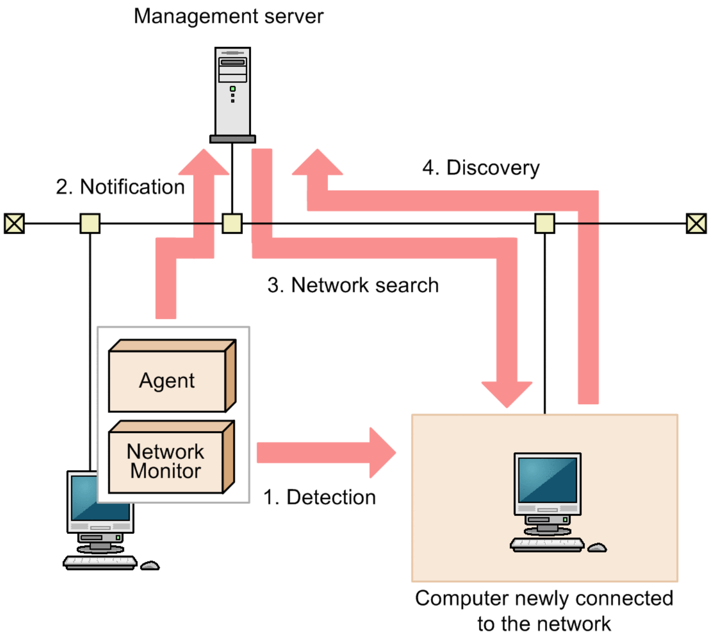
Important note

Before using the network monitoring function, make sure that you are fully aware of the devices to which network access is granted and those to which network access is denied. If network access control is applied incorrectly, network access control can cause unexpected business interruptions, for example, by disabling network access for devices used for business operations.

Tip

To detect devices, enable the network monitor for a single computer on which an agent is installed per network segment. By installing an agent on and enabling the network monitor for a computer capable of accessing multiple networks using multiple network cards, you can monitor multiple network segments using just one computer. Set an appropriate IP address range for the network segment and assign the corresponding authentication information. If a detected device has a network address that is outside the IP address range, a search is performed without using the authentication information. In this case, only the MAC address and IP address information is acquired from that device.

The following figure shows how a device connected to the network is detected and registered inJP1/IT Desktop Management 2:



Legend:

Agent: A computer with the agent installed

Network Monitor: A network monitor agent

1. The computer on which an agent is installed and for which the network monitor is enabled detects a device attempting to access the network.

2. The computer on which an agent is installed and for which the network monitor is enabled notifies the management server that a device has been detected.

3. Based on the received information, the management server searches the network for the detected device.

   Tip

   If you want to perform agentless authentication when the device is discovered, you need to set the IP address range that includes the IP addresses monitored by the network monitor as well as the corresponding authentication information in advance.

4. If the device is discovered during the search, it is automatically included as the management target or an agent is automatically deployed to it, depending on the search conditions.

Important note

The network monitoring function cannot detect devices in the network segments that cannot be accessed directly from the management server, such as networks through NAT.

Important note

If you have enabled the setting for automatically deploying an agent to a device discovered during network search, an agent is deployed to a discovered computer even when that computer is denied network access.

Under this circumstance, an agent is installed on a computer that is denied network access. Depending on the network control setting specified in the security policy and the result of a security check performed for that computer, the computer might be able to access the network.

Important note

If you remove a device that has been discovered by the network monitoring function, that device cannot be rediscovered until you disconnect from the network and then reconnect to it. If the time interval between network disconnection and reconnection is too short, the device might not be rediscovered.

Tip

Regardless of whether **Permit** or **Not Permit** is specified in the network monitor settings, devices accessing the network can be discovered. If the network monitor discovers a device, a network search is automatically performed for that device. If you have enabled the **Auto-Manage Discovered Nodes** or **Auto-Install Agent** setting for the network search, the device discovered by the network monitor is automatically included as a management target or an agent is automatically deployed to the device. The device then becomes a management target, and a product license is used for that device.

If you do not want to automatically include a discovered device as a management target, clear the **Auto-Manage Discovered Nodes** and **Auto-Install Agent** check boxes in **Configurations** so that you can manually select management targets.

The network monitoring function monitors the following networks:

- IPv4 networks. The IPv6 networks are not supported.
- The network monitoring function monitors computers running the OSs listed below. Computers running other OSs can be included as management targets only if such computers use standard TCP/IP network protocols.
    - Windows 95
    - Windows 98
    - Windows Me
    - Windows XP
    - Windows NT 3.51 and 4.0
    - Windows 2000
    - Windows Server 2003
    - Windows Vista
    - Windows Server 2008
    - Windows 7
    - Windows Server 2012
    - Windows 8
    - Windows 8.1
- The network monitoring function monitors TCP/IP network protocols. Protocols such as NetBEUI and IPX are not supported.
- To control devices accessing a wireless LAN, make sure that the access point relays MAC address information. If the access point does not relay MAC address information, network control cannot be performed.

2.5 Installing the agent

We recommend that you install the agent on computers managed by JP1/IT Desktop Management 2. Installing the agent program allows you to manage a computer efficiently using all the features of JP1/IT Desktop Management 2, which include analyzing the computer's status from the operation window and controlling its operation.

There are two approaches to managing a computer with the agent installed: *offline management* and *online management*.

Tip

You can also manage agentless computers. However, some JP1/IT Desktop Management 2 features including automatic application of security measures, message notification, and software and file distribution are unavailable to agentless computers. Agentless management is always used for devices other than computers.

You can use the following methods to install the agent on a computer:

Online management

- Installation by an administrator

  You can use either of the following methods:

  - Install the agent automatically on the user's computer by distributing the program from the management server
  - Have an administrator create an installation set (an installer file that includes the agent program and setup information) and register a logon script on the domain controller

    When the user logs on to Windows, the agent is installed automatically on the user's computer.
- Installation by a user

  The administrator creates an installation set and provides it to the user. The user then installs the agent by executing the installation set.

Offline management

- The administrator creates an installation set and uses it to install the agent on the computer
- The administrator creates an installation set and registers a logon script on the domain controller

  When the user logs on to Windows, the agent is installed automatically on the user's computer.
- The administrator uses the supplied media to install and set up the agent on the computer

Tip

Because computers with the agent installed are automatically designated management targets, you must have one product license for each computer.

2.5.1 Distributing the agent to online-managed computers

You can install the agent on a computer by distributing the agent program from the management server.

There are two ways to distribute the agent:

- Automatic distribution to discovered computers

You can automatically distribute the agent program to discovered computers that are running Windows. As each computer is discovered, the agent is distributed to it. Use this approach if you want to install the agent on every computer in your organization.

- Manual distribution to agentless computers

  You can manually distribute the agent to a management-target computer or discovered computer. Because this approach allows you to select the computers on which to install the agent, it can be used when there are computers in your organization that you want to leave agentless.

For details about the conditions that must be met to distribute the agent, see 2.5.2 Criteria for agent distribution to online-managed computers.

2.5.2 Criteria for agent distribution to online-managed computers

The OS configuration of a distribution-target computer is subject to the same criteria as for when sharing Windows management data in agentless management. For details on these criteria, see 4.2.7 Prerequisites for agentless management.

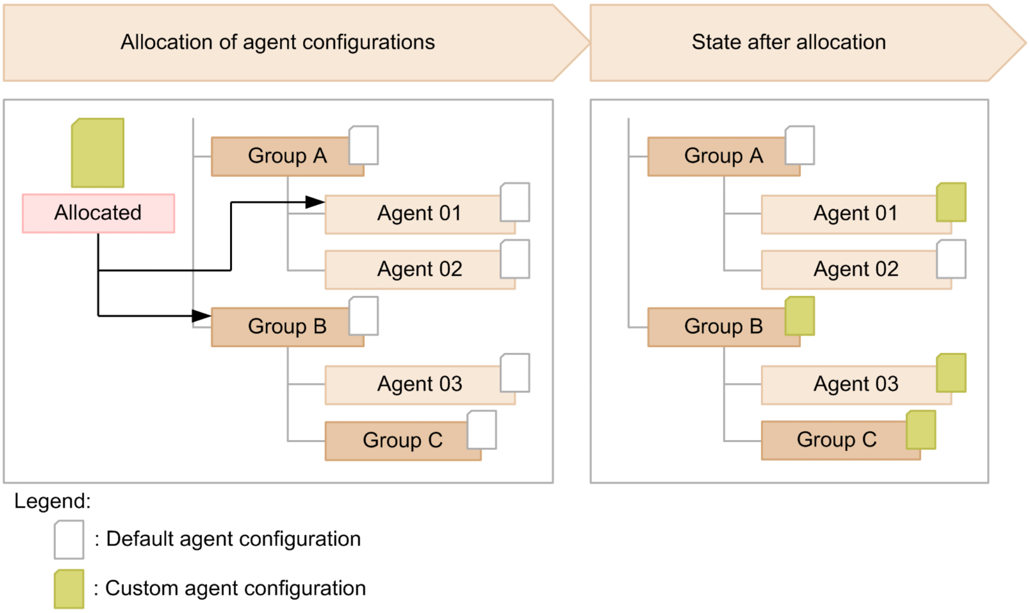
2.5.3 Assigning agent configurations to online-managed computers

You can control how agents are configured by handling agent configurations on the management server. When you change agent configurations on the management server, the new settings take effect on every online-managed computer assigned those particular agent configurations. This allows you to efficiently change how agents are set up across the system.

By default, each computer is assigned the default agent configuration. However, if an online-managed computer is automatically registered in a group with its own agent configurations, the computer is assigned the default agent configuration for that group. For example, if you assign the XP settings to the Windows XP Professional OS group, a computer running Windows XP that becomes a management target is automatically assigned the XP settings.

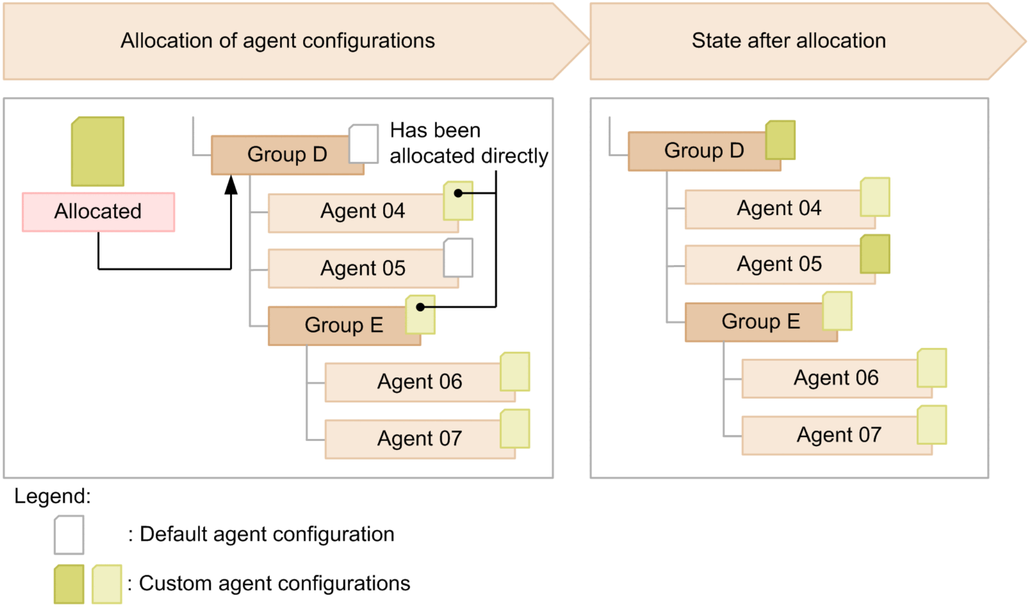
You can apply agent configurations at the computer or group level by creating the settings and assigning them to a specific computer or group. You cannot assign agent configurations to a user-defined group.

When you assign agent configurations to an individual computer, the settings take effect on that computer. If you assign agent configurations to a group, the settings take effect on every online-managed computer in that group. The following figure shows how agent configurations are assigned.



Note: "Agent" indicates an online-managed computer.

If agent configurations are assigned to an individual computer and the group to which it belongs, the agent configurations applied to the computer itself take effect. A group that is not directly assigned agent configurations does not inherit the agent configurations of the upper-level group. The following figure shows which agent configurations apply when a computer is assigned more than one set.



Note: "Agent" indicates an online-managed computer.

If you cancel agent configurations, the settings assigned to the upper-level group take effect.

In some circumstances, such as when a computer has several network cards, a computer might be registered in more than one group intended for a certain range of IP addresses. If a computer belongs to several groups each with different agent configurations, the default agent configuration apply to that computer.

2.6 Managing devices

All manner of devices including computers, servers, printers, and networking equipment connect to corporate networks. The first step towards gaining a picture of the devices in your organization and managing them from the perspectives of security and asset management is to designate the devices as management targets of JP1/IT Desktop Management 2.

When the devices in your organization are managed by JP1/IT Desktop Management 2, you can use features like the following to efficiently assess the nature of the devices.

- Manage devices in lists like a ledger
- Automatically collect the latest device information
- Keep track of the status of devices using a graphical interface incorporating panels and reports

A maximum of 30,000 devices can be managed.

You can make a device a management target by:

Installing the agent on a computer

A computer with the agent installed automatically becomes a management target with it connects to the management server. If you use JP1/IT Desktop Management 2 to manage the devices in your organization, we recommend that you install the agent on all computers.

Designating a discovered device as a management target

You can use the search feature to discover devices that are connected to the network or managed by Active Directory. You can configure the system to automatically designate discovered devices as management targets, or define management targets manually by selecting the devices you want to manage from a list. Use this method to manage devices other than computers.

> **Tip**
>
> The discovery process helps you gain a clear picture of the devices in your organization.

Acquiring information about smart devices by linking with an MDM system

By using the MDM linkage feature, you can acquire smart device information from an MDM system and use it to discover smart devices. You can configure the system to automatically designate discovered devices as management targets, or define management targets manually by selecting the smart devices you want to manage from a list.

You need one license for each device you designate as a management target. Make sure that you have enough licenses for the number of devices you will be managing.

Related Topics:

- 2.6.1 Designating discovered devices as management targets
- 3.1 Overview of product licenses

2.6.1 Designating discovered devices as management targets

While computers with the agent installed are automatically designated as management targets, other devices must be made management targets by a manual process.

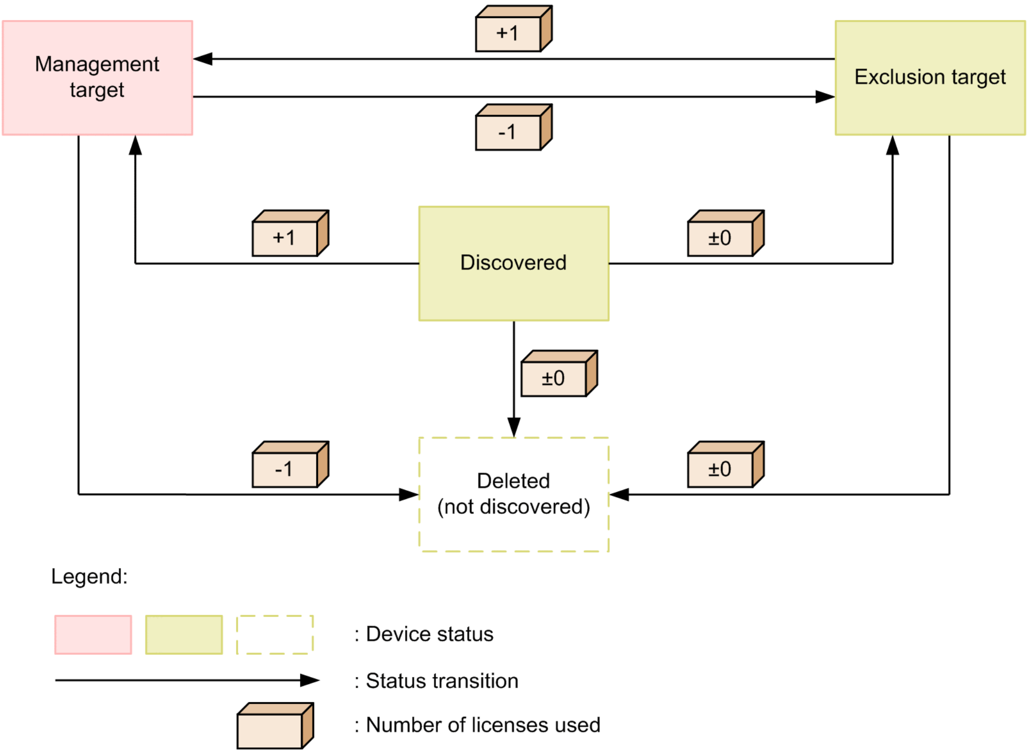
Tip

In the discovery settings, you can choose to configure the system to automatically designate discovered computers as management targets.

You can designate a discovered device as a management target or exclusion target. To manage a device in JP1/IT Desktop Management 2, designate it as a management target. Devices that you do not need to manage in JP1/IT Desktop Management 2 can be designated as exclusion targets.

You need one license for each device you designate as a management target. Making a managed device an exclusion target decreases the number of used licenses by one.

The following figure shows how transitions in device statuses affect the number of used licenses.



Discovered

The device has been discovered by a discovery process. A device in this state does not use a license. You can choose whether to manage a discovered device in JP1/IT Desktop Management 2 by designating it as a management target or exclusion target.

If the system is configured to automatically designate discovered devices as management targets, a device enters this status when there are no more licenses available.

Management target

The device is to be managed by JP1/IT Desktop Management 2. Each management target device uses one license. When you have registered a device as a management target, you can use the features of JP1/IT Desktop Management 2 to manage the device.

You can designate a managed device as an exclusion target or remove the device as a management target if needed.

Exclusion target

The device is excluded as a management target of JP1/IT Desktop Management 2. A device in this state does not use a license. For example, if you only want to manage computers in JP1/IT Desktop Management 2, you can designate other devices like printers and networking equipment as exclusion targets.

> **Tip**
>
> If a device does not require management, you can designate it as an exclusion target. The agent program is no longer distributed to the exclusion target device. This prevents it from appearing in the results of future discovery processes, limiting the results to new devices.

You can designate an excluded device as a management target or remove the device as a management target if needed.

Deleted

Device information has been removed from JP1/IT Desktop Management 2. When you delete a device, information about the device is removed from the database.

Deleted devices can be discovered again. When this occurs, the device is treated as a new device and previous settings are not retained.

Related Topics:

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

(1) Devices supported as management targets

JP1/IT Desktop Management 2 can manage any device that is connected to a network and has an IP address. The following table lists the types of devices that can be management targets.

Device types		Management method			
		Agent	Agentless	Active Directory linkage	MDM system linkage
PC or server (including virtualized environments)	Windows	Y	Y	Y	N
	UNIX	N	Y	N	N
	Linux	N	Y	N	N
	Mac OS	N	Y	N	N
Smart device		N	N	N	Y
Other device		N	Y	N	N

Legend: Y: Can be managed. N: Cannot be managed.

A device that has an IPv4 and an IPv6 address can be managed using its IPv4 address.

You can manage a device with only an IPv6 address by discovering the device in Active Directory. In this case, you can keep track of the device presence but not any other information.

Related Topics:

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information
- 2.4.2 Discovering networked devices

(2) Managing virtual computers

You can manage the virtual computers in your system as separate devices, provided they have an operating system installed. This allows you to collect device information for virtual computers and manage their security status.

To be recognized as a computer independently from its host virtualization server, a virtual computer must meet one of the following criteria:

- The virtual computer has a different MAC address from the virtualization server
- If the virtual computer shares its MAC address with the virtualization server, an agent is installed on the virtualization server and on the virtual computer

Installing the agent on a virtual computer allows it to be recognized as a separate entity from its host, even when they share a MAC address.

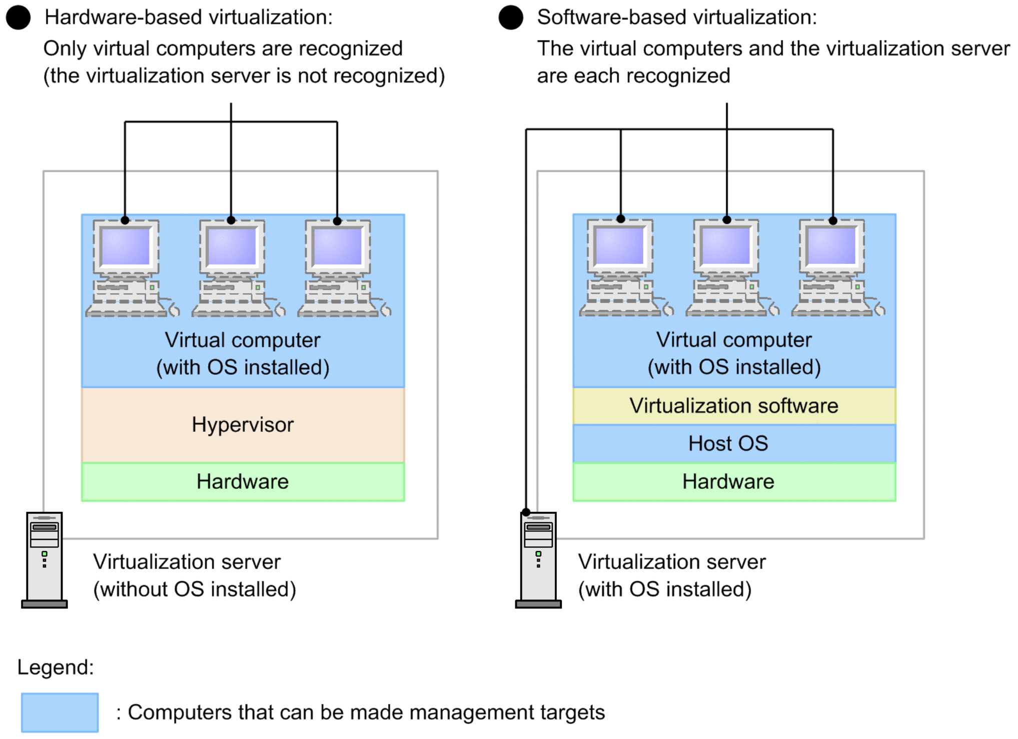
When using hardware-based virtualization

When a virtualization server manages virtual computers using a hypervisor that works directly on the hardware, you can manage each virtual computer as a separate computer. However, because there is no OS on the virtualization server, the server itself is not recognized as a standalone computer and cannot be managed.

When using software-based virtualization

When a virtualization server manages virtual computers using virtualization software running on an operating system, because the virtual computers and the virtualization server each have operating systems installed, they can be managed as separate computers.

The following figure shows how JP1/IT Desktop Management 2 handles virtualization servers and virtual computers.


● Hardware-based virtualization:
Only virtual computers are recognized
(the virtualization server is not recognized)
Virtual computer
(with OS installed)
Hypervisor
Hardware
Virtualization server
(without OS installed)
● Software-based virtualization:
The virtual computers and the virtualization server
are each recognized
Virtual computer
(with OS installed)
Virtualization software
Host OS
Hardware
Virtualization server
(with OS installed)
Legend:
: Computers that can be made management targets

Use of Citrix XenApp or the Windows Terminal Service is not supported. Installing the agent on a server with Citrix XenApp or the Windows Terminal Service installed does not allow you to manage the server.

2.6.2 Collecting device information

JP1/IT Desktop Management 2 collects device information from the devices it manages. It can also collect device information from Active Directory, or information can be entered directly by an administrator. You can view device information in the Device module.

For details about the types of device information JP1/IT Desktop Management 2 can collect, see (1) Types of device information you can collect.

Note that the range of information you can collect depends on the type of device, as described next.

Computers with the agent installed

The manager collects every piece of device information managed by JP1/IT Desktop Management 2. It can also collect the information managed by Active Directory. Administrators can also enter certain information directly.

You can also display a form to users and collect the information they enter. For details about how to collect information entered by users, see (12) Collecting user information.

You can also search for and collect information about software that does not appear in the **Programs and Features** list of the Windows Control Panel. For details, see (11) Defining search conditions for software information.

Agentless computers

Device information is collected during the discovery process, to the extent permitted by the authentication settings. Authentication can use Windows administrative shares or SNMP. If authentication fails, the manager acquires device information within the scope available to the ICMP or ARP protocol.

You can also collect the information managed by Active Directory, and administrators can enter certain information directly.

Devices other than computers

The manager acquires the range of device available via SNMP authentication or the ICMP or ARP protocol. Administrators can also enter certain information directly.

Timing of device information collection

The following describes how the timing with which information is collected depends on the device type.

Computers with the agent installed

Online-managed computers

JP1/IT Desktop Management 2 automatically collects device information when a computer becomes a management target, and updates the database when changes are detected in the information associated with a computer.

Offline-managed computers

Device information is updated each time you use external media to provide the computer's information to the management server.

Agentless computers and devices other than computers

Device information is updated regularly according to a set schedule.

You can collect the latest device information from devices with the agent installed at any time you wish.

When collecting device information in this way, the management server collects the most recent information entered by the user.

Related Topics:

- (11) Defining search conditions for software information

(1) Types of device information you can collect

JP1/IT Desktop Management 2 collects device information from the devices it manages. There are two categories of device information: Basic device information, and common fields (assets and device inventory).

Basic device information

Device information that is collected by default. There are four categories of basic device information: **System Details**, **Hardware Details**, **Installed Software Details**, and **Security Details**.

Common fields (Assets and device inventory)

Information that relates to the user of a device. You can have users enter this information directly.

The range of device information you can collect depends on whether the device is a computer with the agent installed. For agentless devices, the information you can collect depends on the authentication method used. The explanation below refers to the following types of authentication used with agentless devices:

- Administrative share: You can use the authentication provided by a Windows administrative share.
- SNMP: You can use the authentication implemented by SNMP.
- ARP: You can use the authentication implemented by ARP.
- ICMP: You can use the authentication implemented by ICMP.
- Active Directory: JP1/IT Desktop Management 2 links with Active Directory.
- MDM: JP1/IT Desktop Management 2 links with an MDM system.

If a device cannot undergo authentication using Windows administrative shares or SNMP, you can use ICMP or APR to verify the device presence but not to collect information from the device. When linking with Active Directory, some items can be collected from Active Directory while others cannot.

When linking with an MDM system to manage smart devices, you can collect the information managed by the MDM system as device information.

You can view collected device information in the **Device Inventory** and **Software Inventory** views of the Device module. Reasons why the system might be unable to collect device information include the device being turned off or not connected to the network, or failing to establish a connection with the management server. Items for which --, N/A, or Unknown is displayed could not be collected. Reasons why a particular item cannot be collected include the device's authentication status, device type, operating system, and software.**SNMP: NG(No credential)** might appear if not enough information was collected to identify a device.

The tables in the next section show the items of device information you can collect, and whether each item can be collected from a computer with the agent installed, an agentless device, Active Directory, or an MDM system.

(2) Device status information that can be collected

The following table lists the information JP1/IT Desktop Management 2can collect about the status of a device.

Management Type

Icon	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
	Agent Management Indicates a device with the agent installed.	Y	--	--	--	--	--
	Agentless Management (Authentication Successful) Indicates a device that has undergone successful authentication via a Windows administrative share or via SNMP.	--	Y	Y	--	Y	--
	Agentless Management (Authentication Failed) Indicates a device that has not undergone authentication.	--	--	--	Y	--	--
	Agent Management (Network Access Control) Indicates a device with the agent installed and with network access control enabled.	Y	--	--	--	--	--
	Agent Management (Network Access Control)(Starting management) Indicates a device with the agent installed and network access control in the process of starting.	Y	--	--	--	--	--

Icon	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
	Agent Management (Network Access Control)(Failed to start management) Indicates a device with the agent installed, where an attempt to start network access control has failed.	Y	--	--	--	--	--
	Agent Management (Network Access Control)(Stopped management) A device with the agent installed and network access control disabled.	Y	--	--	--	--	--
	Agent Management (Network Access Control)(Failed to stop management) A device with the agent installed where an attempt to stop network access control has failed.	Y	--	--	--	--	--
	Agent Management (Relay system) Indicates a device with a relay system installed.	Y	--	--	--	--	--
	Agent Management (Relay system)(Network Access Control) Indicates a device with a relay system installed and with network access control enabled.	Y	--	--	--	--	--
	Agent Management (Relay system)(Network Access Control)(Starting management) Indicates a device with a relay system installed and network access control in the process of starting.	Y	--	--	--	--	--
	Agent Management (Relay system)(Network Access Control)(Failed to start management) Indicates a device with a relay system installed, where an attempt to start network access control has failed.	Y	--	--	--	--	--
	Agent Management (Relay system)(Network Access Control)(Stopped management) Indicates a device with a relay system installed and network access control in the process of stopping.	Y	--	--	--	--	--

Icon	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
	Agent Management (Relay system)(Network Access Control)(Failed to stop management) Indicates a device with a relay system installed, where an attempt to stop network access control has failed.	Y	--	--	--	--	--
	MDM Linkage Management Indicates a device for which information has been acquired from an MDM system.	--	--	--	--	--	Y

Legend: Y: Can be collected. --: Not applicable.

Connection settings

Connection settings indicate the network connection settings status in JP1/IT Desktop Management 2.

Icon	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
	Allowed The device is able to connect to the network.	Y	Y	Y	Y	Y	Y
	Blocked The device is unable to connect to the network. This status also applies to devices whose network connection was automatically blocked by a security policy or the network monitoring function.	Y	Y	Y	Y	Y	Y
	Forced Block A device whose network connection has been blocked by an administrator.	Y	Y	Y	Y	Y	Y
	Not use period A device that is not allowed to connect to the network because it is outside the allowed time period defined in the network control list.	Y	Y	Y	Y	Y	Y
	Unknown JP1/IT Desktop Management 2is determining whether the device is permitted to connect to the network. The device will transition to	Y	Y	Y	Y	Y	Y

Icon	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
❓	another status when the judgment is made.	Y	Y	Y	Y	Y	Y

Legend: Y: Can be collected.

Device Status

Icon	Description	Agent installed#1	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
⏻	Running Indicates that the computer is on.	Y	Y	Y	Y	N	N
⏻	Stop Indicates that the computer is off.#2	Y #3	Y	Y	Y	N	N
❗	Warning There is a problem with the device. You can use the **System Information** and **Events** tabs of the Device module to investigate further.	Y #3, #4	N	Y#5	N	N	N
✖	Critical There is a serious problem with the device. You can use the **System Information** and **Events** tabs of the Device module to investigate further.	N	N	Y#6	N	N	N
❓	Unknown The status of the device is unknown.	N	N	Y	Y	Y	Y

Legend: Y: Can be collected. N: Cannot be collected.

Note:

For details about the conditions under which each device status is displayed, see (8) Criteria for device statuses.

#1

Stop appears as the device status when you first acquire the status of an offline-managed computer. Each time thereafter, the device retains its previous status.

#2

If a device cannot be communicated with, the device status becomes Stop.

#3

The following devices' statuses become Warning when they are turned off and being managed offline. The status for such devices never appears as Stop.

- Relay system
- Computer with the agent installed and network access control enabled

#4

The device status for an agent-installed computer on which network monitoring is enabled becomes Warning when JP1_ITDM2_Network Monitor service is stopped.

#5

The device status for a printer whose toner or paper level is low becomes Warning.

#6

The device status for a printer that has no remaining toner or paper becomes Critical.

Management Status

Icon	Description	Agent installed	Agentless				MDM
			Administrative share	SNMP	ARP/ ICMP	Active Directory	
	Online management The device is being managed online.	Y	--	--	--	--	--
	Offline management The device is being managed offline.	Y	--	--	--	--	--
—	Agent not Installed The agent is not installed on the device.	--	Y	Y	Y	Y	Y

Legend: Y: Can be collected --: Not applicable

Host ID

Item	Description	Agent installed	Agentless				MDM
			Administrative share	SNMP	ARP/ ICMP	Active Directory	
Host ID	Displays the host ID.	Y	Y	Y	Y	Y	Y

Legend: Y: Can be collected

(3) System information that can be collected

This section describes the information that JP1/IT Desktop Management 2 can collect as system information. System information consists of the following:

- Device type
- Computer information
- User information
- OS information
- Network information
- Printer information

Device type

Device type	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
PC	Set when the OS type is one of the following: • Windows 8.1 • Windows 8 • Windows 7 • Windows Vista • Windows XP • Windows 2000 • Windows OS (unknown edition) • Windows OS (unknown type) • Mac OS • Unknown OS	Y	Y	Y	N	Y	N
Server	Set when the OS type is one of the following: • Windows 2000 Server • Windows 2000 Advanced Server • Windows Server 2003 • Windows Server 2008 • Windows Server 2012 • UNIX • Linux	Y	Y	Y	N	Y	N
Storage	Must be assigned to a device by an administrator.	N	N	N	N	N	N
Network Device	Collected automatically for a network device other than a network printer.	N	N	Y	N	N	N
Printer	Collected automatically for a network printer.	N	N	Y	N	N	N
Smart Device	Set when the information was acquired from an MDM system.	N	N	N	N	N	Y
Peripheral Device	Must be assigned to a device by an administrator.	N	N	N	N	N	N
USB Device	Set in the following cases:	N	N	N	N	N	N

Device type	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
USB Device	- When input by an administrator - When registered from the **Register USB Device** dialog box	N	N	N	N	N	N
Display	Must be assigned to a device by an administrator.	N	N	N	N	N	N
Other	Must be assigned to a device by an administrator.	N	N	N	N	N	N
Custom device type	Must be assigned to a device by an administrator.	N	N	N	N	N	N
Unknown	Set when the device type could not be acquired.	N	N	N	Y	N	N

Legend: Y: Can be collected automatically. N: Cannot be collected automatically.

Computer information

Item		Description	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Computer information	Computer Name (Description)	Name (Computer) The computer name set in the **Computer Name Changes** dialog box displayed by clicking **Change** on the **Computer Name** panel of the System Properties. For SNMP authentication, the acquired host name is displayed. For a smart device, the user name, contract phone number, and model name displayed to identify the smart device in the MDM system are displayed. Description (Computer) The value in the **Computer description** field on the **Computer Name** panel of the System Properties. For SNMP authentication, the description about the device and the object ID unique to the device developer are displayed. For smart devices, this information cannot be acquired.	Y	Y	Y	N	Y	Y
	Host Name	The fully qualified domain name of the physical host.	Y	Y	Y	N	Y	Y

Item		Description	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Computer information	Host Name	In the following circumstances, the NetBIOS name or the host name without a domain name are collected. • The host is not part of a domain or its domain membership cannot be confirmed • The host name was acquired by an SNMP search For a smart device, the user name, contract phone number, and model name displayed to identify the smart device in the MDM system are collected.	Y	Y	Y	N	Y	Y
	Model (Manufacturer)	The model and manufacturer of the computer, assigned by the vendor.	Y	Y	N	N	N	Y
	UUID	The universally unique identifier (UUID) of the computer.	Y	Y	N	N	N	N
	Serial #	The serial number (BIOS information) of the computer.	Y	Y	N	N	N	Y
	CPU	The model name of the CPU.	Y	Y	Y	N	N	N
	Total Memory	The total amount of physical memory installed in the computer.	Y	Y	Y	N	N	Y
	Total Free Space	The amount of free space on the hard disk (the type of logical drive is Local Disk). If the total amount of free space on the local disk exceeds 9,223,372,036,854,775,807 bytes, 9,223,372,036,854,775,807 (bytes) is displayed.	Y	Y	N	N	N	N
System Drive	System Drive	The total number of logical drives.	Y	Y	N	N	N	N
	System Drives (Type/ Free/Total/ File System)	If there are several system drives, the following information can be collected for each drive: Type The type of drive, such as hard disk, CD/DVD drive, or removable disk. Free space#1 The free space available on the drive. Capacity#1 The total capacity of the drive. File system#1 The name of the file system, such as FAT32 or NTFS.	Y	Y	N	N	N	N
	Disk Name (Capacity/ Interface)#2	Disk Name The model of the hard disk drive. Total Capacity The total capacity of the hard disk drive.	Y	Y	Y#3	N	N	Y#4

Item		Description	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
System Drive	Disk Name (Capacity/ Interface)[#2]	Interface The interface such as IDE or SCSI used with the hard drive.	Y	Y	Y[#3]	N	N	Y[#4]
BIOS Information	BIOS Information	The name of the BIOS.	Y	Y	N	N	N	N
	Manufacturer	The manufacturer of the BIOS.	Y	Y	N	N	N	N
	Serial Number	The serial number of the BIOS.	Y	Y	N	N	N	N
	Version (BIOS/ SMBIOS)	BIOS The version of the BIOS. SMBIOS The version of the SMBIOS.	Y	Y	N	N	N	N
	Release Date	The release date of the BIOS.	Y	Y	N	N	N	N
AMT Firmware Version		The version of the AMT firmware.	Y	N	N	N	N	N
Power Control	Turn off monitor (AC/DC)[#5, #6]	The length of time until the monitored power supply shuts off. AC Indicates an AC power supply. DC Indicates a DC (battery) power supply.	Y	Y	N	N	N	N
	System standby (AC/DC)[#5]	The length of time until the system enters standby. AC Indicates an AC power supply. DC Indicates a DC (battery) power supply.	Y	Y	N	N	N	N
	System hibernates (AC/DC)[#5]	The length of time until the system goes into hibernation. AC Indicates an AC power supply. DC Indicates a DC (battery) power supply.	Y	Y	N	N	N	N
	Turn off hard disks (AC/DC)[#4, #5]	The length of time before the hard disk is turned off. AC Indicates an AC power supply. DC Indicates a DC (battery) power supply.	Y	Y	N	N	N	N
	Processor Throttle (AC/DC)[#5, #6]	The power setting of the processor. AC Indicates an AC power supply. DC Indicates a DC (battery) power supply.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

#1: In Windows 8.1, Windows 8, Windows Server 2012, Windows 7, and Windows Server 2008 R2, information cannot be collected if BitLocker drive encryption is locked.

#2: In Windows Server 2012, if a virtual disk is configured with the storage service, the virtual disk information is collected as a physical disk.

#3: Only Disk Name and Capacity can be collected.

#4: Only Capacity can be collected.

#5: If a user without Administrator permission is logged on to a computer running Windows Server 2003 or Windows XP, the system collects the power control settings for the last user who logged on with Administrator permission.

#6: If these features cannot be used, correct information might not have been collectable.

User Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Last Logged On User Name (User Name)	The user name or account name and domain name (or computer name) of the last user to log on.	Y#	Y#	N	N	N	N
Last Logged On User Description	A description of the last user to log on.	Y#	Y#	N	N	N	N
Locale/Current Time Zone	Locale The locale of the last user to log on. Current Time Zone The time zone of the last user to log on.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

#: If the last user to log in is a domain user, you cannot collect the full name and description of the user.

OS Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
OS and Service Pack (Language)	The language of the OS and the service packs applied to the OS. This information indicates which language version of Windows (such as English or Japanese) is installed, not the locale setting.	Y	Y	N	N	Y#	N
Serial #	The serial number of the OS. The serial number is different from the license key needed to install the OS.	Y	Y	N	N	N	N

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Owner (Company)	Owner The owner name entered by the user when installing the OS. Company The company name entered by the user when installing the OS.	Y	Y	N	N	N	N
OS last startup date/ time	The last startup date and time of the OS.	Y	Y	N	N	N	N
Windows directory	The directory in which the OS is installed.	Y	Y	N	N	N	N
Windows Installer Version	The version number of Windows Installer.	Y	Y	N	N	N	N
Windows Update (Agent Version)	The version number of the Windows Update agent.	Y	Y	N	N	N	N
IE Version (Service Pack)	IE Version The Internet Explorer version. IE Service Pack The service pack version of Internet Explorer.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

#: Only the service pack information can be collected.

Network Details

Item	Description	Agent installed#1	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
IP Address/Subnet Mask	The IP address and subnet mask of the device.	Y	Y	Y	Y#2, #3	Y	N
Network Adapter	The name of the network adapter.	Y	Y	Y	N	N	N
MAC Address	The MAC address of the device.	Y	Y	Y	Y#3, #4	Y	Y
Default Gateway	The default gateway.	Y	Y	Y	N	N	N
WINS Server Address (Primary/ Secondary)	Primary The address of the primary WINS server. Secondary The address of the secondary WINS server.	Y	Y	N	N	N	N

Item	Description	Agent installed[#1]	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
DNS Server Address	The address of the DNS server.	Y	Y	N	N	N	N
DHCP	Whether or not DHCP is enabled.	Y	Y	N	N	N	N
DHCP Server Address	The address of the DHCP server.	Y	Y	N	N	N	N
Lease Acquisition/ Expiration Date/ Time	The date and time when the DHCP lease was acquired, and then date and time when the lease expires.	Y	Y	N	N	N	N
Domain (Workgroup)/Role	Domain The name of the domain or workgroup to which the computer belongs. Domain Role The role of the device in the OS domain, such as primary domain controller or member workstation.	Y	Y	Y[#5]	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

#1: Cannot be collected from an offline-managed computer lacking a NIC.

#2: Only the IP address can be collected.

#3: The collected information does not appear on the **System Details** tab of the **Device Information** view of the Device module. You can review the collected information by exporting the device list.

#4: Only collected in environments that use ARP.

#5: Only the Domain is collected.

Printer Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Printing Method (Method /Colors)	The printing method used by the printer.	N	N	Y	N	N	N
Consumables (Type/ Description/ Condition)	The type of consumable (such as ink) used by the printer, and the amount remaining.	N	N	Y	N	N	N

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Paper Feed Tray (Type/Name/Condition)	The type of paper feed tray used in the printer, and the amount of paper remaining.	N	N	Y	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Smart Device Information

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
IMEI	The ID number assigned to the mobile device.	N	N	N	N	N	Y
UDID	An identifier assigned to smart devices made by Apple.	N	N	N	N	N	Y
ICCID	A number assigned to the SIM card in smart devices manufactured by Apple.	N	N	N	N	N	Y
IMSI	An ID number that identifies a subscriber of a mobile communication device. An IMSI is assigned to the SIM card of a smart device.	N	N	N	N	N	Y
Contract phone number	The telephone number assigned to the subscriber.	N	N	N	N	N	Y
E-mail	The E-mail address of the smart device.	N	N	N	N	N	Y
Carrier	The company that provides the communication service used by the smart device.	N	N	N	N	N	Y
Passcode setting	Whether a passcode is set on the device.	N	N	N	N	N	Y
Internal storage (Free)	Internal storage The internal storage capacity of the smart device. Free The free space available on the internal storage of the smart device.	N	N	N	N	N	Y
External storage (Free)	External storage The capacity of media (such as SD cards) installed in the smart device. Free The free space available on media (such as SD cards) installed in the smart device.	N	N	N	N	N	Y
RAM (Free)	RAM The memory capacity of the smart device. Free The amount of free memory available on the smart device.	N	N	N	N	N	Y

Legend: Y: Can be collected. N: Cannot be collected.

(4) Hardware information

This section describes the hardware information you can collect. Hardware information consists of the following:

- Processor Details
- Memory Details
- Hard Disk Details
- CD-ROM Drive Details
- Removable Drive Details
- Printer Details
- Video Controller Details
- Sound Card Details
- Network Adapter Details
- Monitor Details
- Keyboard Details
- Mouse Details

Processor Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Processor Details	The number of processors.	Y	Y	N	N	N	N
Processor Name	The name of the processor.	Y	Y	Y	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Memory Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Memory Details	The total amount of physical memory installed in the computer.	Y	Y	N	N	N	N
Total Capacity	The amount of physical memory installed in the computer.	Y	Y	N	N	N	Y
Slots	The total amount of physical memory installed in a memory slot. If the computer has several memory slots, the amount of memory in each slot can be collected.	Y	Y	N	N	N	N

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Virtual Memory Capacity#	The total amount of virtual memory.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

#: The virtual memory capacity is the sum of the available physical memory and the total size of the page files. If the computer is running Windows Server 2003 (no service pack) or Windows XP, the virtual memory capacity in the system information is the total size of the page files.

Hard Disk Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Hard Disk Details	The number of hard disk drives.	Y	Y	Y	N	N	N
Disk names (Total Volume/ Interface)#3	When there is more than one hard disk, the following information is collected for each disk: Hard Disk Model The model name of the hard disk drive. Total Volume The capacity of the hard disk. This item shows the total capacity regardless of how the drive is partitioned. Interface The interface of the hard disk drive, such as IDE or SCSI.	Y	Y	Y#1	N	N	Y#2
Drive (Free/ Total/File System)	When there is more than one hard disk, the following information is collected for each disk: Free The amount of free space on the drive. Total The total capacity of the drive. File System The name of the file system.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Note: Drive information cannot be collected for network drives.

#1: The Interface item cannot be collected.

#2: Only the Total item can be collected.

#3: In Windows Server 2012, if the storage service has been used to create a virtual disk, the information for the virtual disk is collected as if it is a physical disk.

CD-ROM Drive Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
CD-ROM Drive Details	The number of CD/DVD drives.	Y	Y	N	N	N	N
CD-ROM Drive	The model name of the CD/DVD drive. If there are several CD/DVD drives, this information is collected for each drive.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Removable Drive Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Removable Drive Details	The number of removable drives.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Printer Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Printer Details	The number of printers set up on the computer.	Y	Y	N	N	N	N
Printer Name (Type)	If there are several printers, the following information is collected for each printer: Printer Name The name of the printer. Type The printer type.	Y	Y	N	N	N	N
Driver	The printer driver. If there are several printers, this item is collected for each printer.	Y	Y	N	N	N	N
Shared Name	The shared name of the printer. If there are several printers, this item is collected for each printer.	Y	Y	N	N	N	N
Server Name (Port)	If there are several printers, the following items are collected for each printer:	Y	Y	N	N	N	N

Item	Description	Agent installed	Agentless				
			Admini strative share	SNM P	ARP/ ICMP	Active Directory	MDM
Server Name (Port)	Server Name The name of the printer server. Port The printer port.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Video Controller Details

Item	Description	Agent installed	Agentless				
			Admin istrativ e share	SNM P	ARP/ ICM P	Active Director y	MDM
Video Controller Details	The number of video drivers.	Y	Y	N	N	N	N
Video Chip	The name of the video chipset.	Y	Y	N	N	N	N
VRAM Capacity	The amount of VRAM on the video card.	Y	Y	N	N	N	N
Video Driver	The name of the video driver.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Sound Card Details

Item	Description	Agent installed	Agentless				
			Admini strative share	SNM P	ARP/ ICMP	Active Director y	MDM
Sound Card Details	The number of sound card drivers.	Y	Y	N	N	N	N
Product Name (Manufacturer)	The name and manufacturer of the sound card.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Network Adapter Details

Item	Description	Agent installed	Agentless				
			Admin istrativ e share	SNMP	ARP/ ICMP	Active Directo ry	MDM
Network Adapter Details	The number of network adapters.	Y	Y	Y	N	N	N
Network Adapter	The name of the network adapter.	Y	Y	Y	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Monitor Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Monitor Details	The number of monitors.	Y	Y	N	N	N	N
Monitor	The name of the monitor.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Keyboard Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Keyboard Details	The number of keyboards.	Y	Y	Y	N	N	N
Keyboard	The name of the keyboard.	Y	Y	Y	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Mouse Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Mouse Details	The number of mouse.	Y	Y	Y	N	N	N
Mouse	The name of the mouse.	Y	Y	Y	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

(5) Installed software information

This section describes the information you can collect about installed software. Installed software information consists of the following:

Software listed in **Programs and Features**

Information about the software registered in the **Programs and Features** section of the Windows Control Panel.

Important note

If both of the following conditions exist, uninstall the software, and then delete the user account. If you delete the user account before the software is uninstalled, the relevant software information will remain as installed software information for JP1/IT Desktop Management 2.

- Software that appears only in the **Programs and Features** section of the Windows Control Panel is installed on the user's computer.

- You want to delete the user account used to install the software that meets the above condition.

Software registered in **Software Search Conditions**

Information about software that is not registered in the **Programs and Features** section of the Windows Control Panel. By setting search conditions in the **Software Search Conditions** view of the Settings module, you can search for and collect information about executable files (with the extention `exe`, for example) on the computer.

Installed OS

Information about the OS installed on the computer.

For details about software search conditions, see (11) Defining search conditions for software information.

Important note

Modern UI applications cannot be managed as software information.

Software listed in Programs and Features

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Software Name	The name of the installed software. If Windows Updates are registered in groups, the name of the group is displayed.	Y	Y	N	N	N	N
Version	The version of the installed software.	Y	Y	N	N	N	N
Software Vendor	The vendor of the installed software.	Y	Y	N	N	N	N
Support URL	The URL of the support page for the installed software.	Y	Y	N	N	N	N
Purchasing Status	The manner in which the software is licensed. Volume license version or Full-product version appears as the purchasing status.	Y*	Y*	N	N	N	N
Product ID	The product ID of Microsoft Office installed on the computer. This item appears in the **Software List** view of the Device module if the purchasing status is *Volume license version*. The last five digits are replaced with asterisks in the **Software List**.	Y*	Y*	N	N	N	N

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
GUID	The globally unique identifier (GUID) of the installed software.	Y*	Y*	N	N	N	N
Installation Date	The date on which the software was installed.	Y	Y	N	N	N	N
Installation Folder	The installation path of the software.	Y	Y	N	N	N	N

Legend: Y: Can be collected. Y*: Only collected for some software. N: Cannot be collected.

Items labeled Y* can be collected only for the following Microsoft Office products:

Japanese versions of Microsoft Office products

Software Name	Edition
Microsoft Office	Microsoft Office Enterprise 2007#1
	Microsoft Office Home and Business 2010#2
	Microsoft Office Personal Edition 2003#2
	Microsoft Office Professional Edition 2003#2
	Microsoft Office Professional Enterprise Edition 2003#1
	Microsoft Office Professional 2007
	Microsoft Office Professional 2010#2
	Microsoft Office Professional Plus 2007#1
	Microsoft Office Professional Plus 2010#1
	Microsoft Office Professional Plus 2013#1, #3
	Microsoft Office Standard Edition 2003
	Microsoft Office Standard 2007
	Microsoft Office Standard 2010#1
	Microsoft Office Standard 2013#1, #3
	Microsoft Office Ultimate 2007#2
Microsoft Lync	Microsoft Lync 2010#1
	Microsoft Lync 2013#1, #3
Microsoft Office Access	Microsoft Office Access 2003#4
	Microsoft Office Access 2007
	Microsoft Access 2010
	Microsoft Access 2013#1, #3

Software Name	Edition
Microsoft Office Excel	Microsoft Office Excel 2003#4
	Microsoft Office Excel 2007
	Microsoft Excel 2010
	Microsoft Excel 2013#1, #3
Microsoft Office FrontPage	Microsoft Office FrontPage 2003
Microsoft Office Groove	Microsoft Office Groove 2007
Microsoft Office InfoPath	Microsoft Office InfoPath 2007
	Microsoft InfoPath 2010
	Microsoft InfoPath 2013#1, #3
Microsoft Office InterConnect	Microsoft Office InterConnect 2007
Microsoft Office OneNote	Microsoft Office OneNote 2007
	Microsoft OneNote 2010
	Microsoft OneNote 2013#1, #3
Microsoft Office Outlook	Microsoft Office Outlook 2003#4
	Microsoft Office Outlook 2007
	Microsoft Outlook 2010
	Microsoft Outlook 2013#1, #3
Microsoft Office PowerPoint	Microsoft Office PowerPoint 2003#4
	Microsoft Office PowerPoint 2007
	Microsoft PowerPoint 2010
	Microsoft PowerPoint 2013#1, #3
Microsoft Office Project	Microsoft Office Project Professional 2003
	Microsoft Office Project Professional 2007
	Microsoft Project Professional 2010
	Microsoft Project Professional 2013#1, #3
	Microsoft Office Project Standard 2003
	Microsoft Office Project Standard 2007
	Microsoft Project Standard 2010
	Microsoft Project Standard 2013#1, #3
Microsoft Office Publisher	Microsoft Office Publisher 2003
	Microsoft Office Publisher 2007
	Microsoft Publisher 2010
	Microsoft Publisher 2013#1, #3
Microsoft Office SharePoint Workspace	Microsoft SharePoint Workspace 2010

Software Name	Edition
Microsoft Office Visio	Microsoft Office Visio 2003 Professional
	Microsoft Office Visio 2003 Standard
	Microsoft Office Visio 2007 Professional
	Microsoft Office Visio 2007 Standard
	Microsoft Visio 2010 Premium
	Microsoft Visio 2010 Professional
	Microsoft Visio 2010 Standard
	Microsoft Visio Professional 2013#1, #3
	Microsoft Visio Standard 2013#1, #3
Microsoft Office Word	Microsoft Office Word 2003#2, #4
	Microsoft Office Word 2007
	Microsoft Word 2010
	Microsoft Word 2013#1, #3

#1: Collected only when the purchasing status is `Volume license version`.

#2: Collected only when the purchasing status is `Full-product version`.

#3: The product ID cannot be collected.

#4: The purchasing status cannot be collected.

English versions or Chinese versions of Microsoft Office products

Software Name	Edition
Microsoft Office	Microsoft Office Enterprise 2007
	Microsoft Office Professional 2007
	Microsoft Office Professional Plus 2007
	Microsoft Office Professional Plus 2010
	Microsoft Office Professional Plus 2013#1, #2
	Microsoft Office Standard 2007
	Microsoft Office Standard 2010
	Microsoft Office Standard 2013#1, #2
Microsoft Lync	Microsoft Lync 2010
	Microsoft Lync 2013#1, #2
Microsoft Office Access	Microsoft Office Access 2007
	Microsoft Access 2010
	Microsoft Access 2013#1, #2
Microsoft Office Excel	Microsoft Office Excel 2007

Software Name	Edition
Microsoft Office Excel	Microsoft Excel 2010
	Microsoft Excel 2013#1, #2
Microsoft Office Groove	Microsoft Office Groove 2007
Microsoft Office InfoPath	Microsoft Office InfoPath 2007
	Microsoft InfoPath 2010
	Microsoft InfoPath 2013#1, #2
Microsoft Office OneNote	Microsoft Office OneNote 2007
	Microsoft OneNote 2010
	Microsoft OneNote 2013#1, #2
Microsoft Office Outlook	Microsoft Office Outlook 2007
	Microsoft Outlook 2010
	Microsoft Outlook 2013#1, #2
Microsoft Office PowerPoint	Microsoft Office PowerPoint 2007
	Microsoft PowerPoint 2010
	Microsoft PowerPoint 2013#1, #2
Microsoft Office Project	Microsoft Office Project Professional 2007
	Microsoft Project Professional 2010
	Microsoft Project Professional 2013#1, #2
	Microsoft Office Project Standard 2007
	Microsoft Project Standard 2010
	Microsoft Project Standard 2013#1, #2
Microsoft Office Publisher	Microsoft Office Publisher 2007
	Microsoft Publisher 2010
	Microsoft Publisher 2013#1, #2
Microsoft Office SharePoint Workspace	Microsoft SharePoint Workspace 2010
Microsoft Office Visio	Microsoft Office Visio 2007 Professional
	Microsoft Office Visio 2007 Standard
	Microsoft Visio 2010 Standard
	Microsoft Visio 2010 Professional
	Microsoft Visio 2010 Premium
	Microsoft Visio Professional 2013#1, #2
	Microsoft Visio Standard 2013#1, #2
Microsoft Office Word	Microsoft Office Word 2007
	Microsoft Word 2010

Software Name	Edition
Microsoft Office Word	Microsoft Word 2013#1, #2

#1: Collected only when the purchasing status is `Volume license version`.

#2: The product ID cannot be collected.

Software registered in the Software Search Conditions view

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Software Name	The name of the installed software. If Windows Updates have been registered in groups, the name of the group is displayed.	Y	N	N	N	N	N
Version	The version of the installed software.	Y	N	N	N	N	N
Software Vendor	The vendor of the installed software.	Y	N	N	N	N	N
Software Installation Date	The date on which the software was installed.	Y	N	N	N	N	N
Installation Folder	The installation path of the software.	Y	N	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Installed OS

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Software Name	The name of the installed software.	Y	Y	N	N	N	N
Version	The version of the installed software.	Y	Y	N	N	N	N
Software Vendor	The vendor of the installed software.	Y	Y	N	N	N	N
Installation Date	The date on which the software was installed.	Y	Y	N	N	N	N
Installation Folder	The installation path of the software.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

(6) Security information

This section describes the information you can collect about a device's security. Security information consists of the following:

- Windows Update Details
- Antivirus Software Details
- Windows Service Details
- OS Security Details
- Hibun Details

Windows Update Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Automatic Windows Update[#1]	Information indicating whether the Windows Update feature is enabled.	Y	Y	N	N	N	N
Installed Updates	The number of installed updates.	Y	Y	N	N	N	N
Article ID (Installation Date)[#2]	The name of the Windows update and the date when the update was installed.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

#1: Collected when the Workstation service of the OS is running.

#2: A hyphen (−) is displayed if information about the installation date could not be acquired.

Antivirus Software Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Software Name	The name of the antivirus product.	Y	Y	N	N	N	N
Version	The version of the antivirus product.	Y	Y	N	N	N	N
Installation Date	The date on which the antivirus product was installed.	Y*	Y*	N	N	N	N
Scan Engine Version	The scan engine version of the antivirus software.	Y*	Y*	N	N	N	N
Virus Definition File Version	The version (date) of the definition file used by the antivirus product.	Y*	Y*	N	N	N	N
Auto Protect	The auto-protect setting (resident or non-resident) of the antivirus product.	Y*	Y*	N	N	N	N

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Last Scanned Date/Time	The date and time when the computer was last scanned for viruses.	Y*	Y*	N	N	N	N

Legend: Y: Can be collected. Y*: Can be collected for some products. N: Cannot be collected.

For details about the antivirus software information you can collect, see (14) Supported anti-virus products.

Windows Service Details

Item	Description	Agent installed#	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Windows Service Details	The display name of an active Windows service that is prohibited by a security policy.	Y	N	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Note: This information is collected when the Workstation service is running on the OS.

#: Only collected from online-managed computers.

OS Security Details

Item		Description	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Account Details	Account Name	The name of a Windows local account. Account details are collected for each account name.	Y	Y	N	N	N	N
	Days Since Last Password Change	The number of days since the account password was last changed. This information is not collected for disabled or expired accounts.	Y	Y	N	N	N	N
	Password Strength#1	The strength of the password.	Y	Y	N	N	N	N
	Password Never Expires	Whether the password is configured to never expire.	Y	Y	N	N	N	N
Power On Password		Whether the computer has a power-on password.	Y	Y	N	N	N	N
Guest Account		Whether or not a Guest account is configured on the computer.	Y	Y	N	N	N	N

Item		Description	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ICMP	Active Directory	MDM
Auto Logon		Whether automatic logon is enabled in Windows.	Y	Y	N	N	N	N
Shared Folder		Whether a shared folder is set up on the computer.	Y	Y	N	N	N	N
Administrative share		Whether administrative shares are enabled.	Y	Y	N	N	N	N
DCOM		Whether DCOM is enabled on the computer.	Y	Y	N	N	N	N
Anonymous Access		Whether information can be collected by anonymous access.	Y	Y	N	N	N	N
Screen Saver Details	Account Name	The name of the Windows local account. Screen Saver Details are collected for each account name.	Y	Y[#2]	N	N	N	N
	Screen Saver Settings	Whether a screen saver is enabled.	Y	Y[#2]	N	N	N	N
	Password	Whether the screen saver is password-protected.	Y	Y[#2]	N	N	N	N
	Startup Time	The length of time before the screen saver activates.	Y	Y[#2]	N	N	N	N
Windows Firewall		Whether the Windows firewall is enabled.	Y	Y	N	N	N	N
Remote Desktop		Whether the remote desktop feature is enabled.	Y	Y	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Note: This information is collected when the Workstation service of the OS is running.

#1: The following passwords are considered to have low strength:

- Blank passwords
- Passwords that match the account name exactly
- A password that is the same character string as the account name, and consists of only upper case letters, only lower case letters, or has only the first letter capitalized.
- A password that is the same character string as the computer name, and consists of only upper case letters, only lower case letters, or has only the first letter capitalized.
- `password`, `PASSWORD`, or `Password`
- `admin`, `ADMIN`, or `Admin`
- `administrator`, `ADMINISTRATOR`, or `Administrator`

JP1/IT Desktop Management 2 does not judge the strength of passwords associated with disabled, expired, or locked user accounts. When an account has a weak password, the last modified date/time of the password changes when its security is assessed. However, the password itself is left unchanged.

#2: When using an administrative share to collect device information, the system only collects information for the user who is logged on to Windows at the time of collection.

Hibun Details

Item	Description	Agent installed	Agentless				
			Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Product Name	The full name of the installed product.	Y	N	N	N	N	N
Version	The version of the installed software.	Y	N	N	N	N	N
Patch Version	Information about the patches applied to the installed software.	Y	N	N	N	N	N
Login User ID	The user ID of the last user who logged in to the Hibun product.	Y	N	N	N	N	N
Last Login Date/Time	The time when a user last logged in to the Hibun product.	Y	N	N	N	N	N
Last Logout Date/Time	The time when a user last logged out from the Hibun product.	Y	N	N	N	N	N
Drive	The local drive.	Y	N	N	N	N	N
Encryption Status	The encryption status of the drive.	Y	N	N	N	N	N

Legend: Y: Can be collected. N: Cannot be collected.

Note: The information in this table can be collected when the managed computer is running version 09-00 or later of the Hibun product.

(7) Shared management items for asset information and device information

Item	Description	Input method/data type (default)	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Department	The department where the user of the computer works.	Entry by adminstrator/ Hierarchy	Y	N	N	N	Y	N
Location	The physical location of the computer.	Entry by adminstrator/ Hierarchy	Y	N	Y#	N	Y	N
User Name	The name of the computer user.	Entry by administrator/ Text	Y	N	N	N	Y	N

Item	Description	Input method/data type (default)	Agent installed	Agentless				
				Administrative share	SNMP	ARP/ ICMP	Active Directory	MDM
Account	The account of the computer user.	Entry by administrator/ Text	Y	N	N	N	Y	N
E-mail	The E-mail address of the computer user.	Entry by administrator/ Text	Y	N	N	N	Y	N
Phone	The telephone number of the computer user.	Entry by administrator/ Text	Y	N	N	N	Y	N

Legend: Y: Can be collected. N: Cannot be collected.

#: Collected when location information is set in the SNMP agent.

(8) Criteria for device statuses

Device status	Criteria
Running	The current time is within 10 minutes of the last confirmation time plus the polling interval.
Stop	This status appears in situations like the following: • The current time is more than 10 minutes after the last confirmation time plus the polling interval. • Device information was collected for anoffline-managed computer for the first time.#
Warning	This status appears in situations like the following: • The current time is more than 10 minutes after the last confirmation time plus the polling interval, and network monitor is enabled on the agent. • Device information was collected for the first time for an offline-managed computer with the network monitor enabled.# • The system fails to negotiate authentication with an agentless computer. • SNMP reports that a printer device is in Warning status (for example, toner is low).
Critical	SNMP reports that a printer device is unusable (for example, the printer is out of paper).
Unknown	Information about the device status could not be collected.

Note:

A computer with the network monitor agent installed might report several device statuses. In this case, the device status displayed in the modules is determined as follows:

1. The most severe status is displayed. In order of severity, the statuses are Critical, Warning, Stop, Running, and Unknown.
2. If the reported statuses have the same severity level, the device status reported for the most important system component is shown. The agent is the most important, followed by the network monitor agent.

#

Thereafter, the device retains its previous status.

(9) Timing of device information collection

Device information is collected from online management agents according to a regular schedule determined by the monitoring interval in the agent configurations. When an online management agent detects that device information has changed, it reports the device information to the management server. No information is reported if the device information is unchanged.

The following table lists the device information reported to the management server.

Detected item		Reported information	Monitoring interval
Host ID		All device information[#1]	Monitoring Interval (Others) (min)
Connection-target management server		All device information[#2]	Monitoring Interval (Others) (min)
System information		All information for detected items	Monitoring Interval (Others) (min)[#3]
Hardware information		All information for detected items	Monitoring Interval (Others) (min)
Installed software information		Information about additions, deletions, and changes among detected items	Monitoring Interval (Security) (min)[#4]
Security information	Windows Update	All information for detected items	Monitoring Interval (Security) (min)
	Anti-virus product information	All information for detected items	Monitoring Interval (Security) (min)
	Service security settings	All information for detected items	Monitoring Interval (Security) (min)
	OS security settings	All information for detected items	Monitoring Interval (Security) (min)
Hibun information		All information for detected items	Monitoring Interval (Others) (min)
Common management items	Entered by user	All device information for detected items	When the user finishes entering
Added management items			

#1: If a host ID is changed, the agent determines that the device on which it is installed has changed, and reports a full set of device information.

#2: When the connection-target management server changes, the agent reports a full set of information to the new connection-target management server. Any instructions received from the previous connection target are retained.

#3: The Free Space attribute of the System Drive item in the computer information is collected once every 24 hours.

#4: Changes to the software information discovered in a software search are detected once every 24 hours.

(10) Collecting software information

JP1/IT Desktop Management 2 also collects software information when it collects device information from the computers it manages. You can view software information arranged by product name and version in the **Software Inventory** view of the Device module.

Tip

An event is generated whenever software is added to a managed computer. By configuring email notification, you can have the administrator notified by email when software is added.

When software that is not registered in JP1/IT Desktop Management 2 is found on a managed computer, its discovery is reported in the **Topic** panel of the Home module. You can view a list of newly discovered software in the **New Software** panel of the **Dashboard** view in the **Overview** view of the Device module. You can also display the **New Software** panel in the Home module by selecting **Panel Layout** in the **View** menu at the top of the module.

There are three types of software information. For details about the items collected for each type, see (5) Installed software information.

Software registered in **Programs and Features**

Information about the software registered in the **Programs and Features** section of the Windows Control Panel. This information is collected from computers with the agent installed, and from agentless computers using authentication to administrative shares.

Software registered in **Software Search Conditions**

Information about software not listed in the **Programs and Features** section of the Windows Control Panel. You can specify these conditions in the **Software Search Conditions** view of the Settings module. JP1/IT Desktop Management 2 uses these conditions to find and collect information about executable files (such as `exe` files) on computers that have the agent program installed.

A search for software is conducted when the computer starts, and every 24 hours thereafter. The agent searches every local drive on the computer for software, and collects information about software that matches the software search conditions.

Operating system information

Information about the operating system installed on a computer. This information can be collected from computers with the agent program installed, and from agentless computers using authentication to administrative shares.

Setting software search conditions

As software search conditions, specify the executable file names you want to find.

If software that matches the search conditions is also present in the **Programs and Features** section of the Windows Control Panel, software information found by the search is not registered for that item.

If the search finds software with the same file name in different folders, information is collected for each piece of software, and several sets of software information are registered for software with the same name. You can distinguish between each piece of software by its installation path.

You can define software search conditions directly from the Settings module, or you can import conditions as a list. The search conditions you define apply to all computers with the agent installed. You cannot define separate sets of software search conditions for individual computers. For details about how to set software search conditions, see (11) Defining search conditions for software information.

Displaying computers with software installed

After collecting software information from managed computers, you can view a list of computers with a particular piece of software installed. This list appears on the **Installed Computers** tab of the **Software Inventory** view.

The following table lists the items shown on the **Installed Computers** tab.

Item	Description
Host Name	The host name of the managed computer with the software installed.
Manufacturer	The manufacturer of the computer with the software installed.
IP Address	The IP address of the computer with the software installed.
OS	The OS on the computer with the software installed.
User Name	The name of the user of the computer with the software installed.
Registered Date/Time	The date and time when the computer with the software installed was registered.
Installation Date	The date and time when the software was installed on the managed computer.

(11) Defining search conditions for software information

By collecting software information from managed computers, you can see how software licenses are being used, monitor whether prohibited software and mandatory software are installed in keeping with a security policy, and gain a clear understanding of what software is installed on the computers in your organization.

The process for collecting software information depends on the type of software, as follows:

Software registered in the **Programs and Features** section of the Windows Control Panel

Software information is collected automatically from computers with the agent installed, and from agentless computers that support authentication by administrative shares.

Software not registered in the **Programs and Features** section of the Windows Control Panel

You can collect software information from computers with the agent installed by defining software search conditions.

By defining software search conditions, you can search computers for software that matches the conditions, and collect software information for discovered software. A search is conducted when the computer starts, and every 24 hours thereafter.

You can edit software search conditions when software is renamed or upgraded and its parameters change.

You can update several software search conditions at once by exporting, editing, and then importing the conditions.

You can delete the software search conditions associated with software that no longer needs managing.

(12) Collecting user information

You can collect user information from computers with the agent installed by displaying an input window in which the user can enter the required information. This allows you to collect information like department names and asset numbers that JP1/IT Desktop Management 2 cannot collect automatically, which reduces the administrator's workload in data entry.

There are two types of user information you can collect:

Shared management items for asset information and device information

Information common to device information and hardware asset information.

Added management items for hardware asset information

Custom asset management items added to hardware asset information by an administrator.

You can use the Settings module to specify the date and time to allow users to start entering user information. If you specify the date and time, user information cannot be entered until the specified date and time is reached. When the local time of a user's computer reaches the specified date and time, a balloon tip appears and user information can be entered. Whether to display balloon tips can be selected in the **User notification settings** view for the agent configuration.

You can also set a schedule to collect user information on a regular basis from online-managed computers with the agent installed.

(13) Collecting registry information

You can collect registry information for computers as shared management items for hardware asset and device information, and as added management items for hardware asset information. By collecting registry information, you can use JP1/IT Desktop Management 2 to manage information specific to users and proprietary information defined by applications. Registry information can only be acquired from computers with the agent installed.

To collect registry information, you need to change the data source for the relevant items in the **Asset Field Definitions** view of the Settings module.

You must specify the root key and path of the registry entries that you want to collect. You can specify the following root keys:

- HKEY_CURRENT_USER#
- HKEY_LOCAL_MACHINE
- HKEY_CLASSES_ROOT
- HKEY_USERS
- HKEY_CURRENT_CONFIG

#: When you specify a registry value under the HKEY_CURRENT_USER root key, the value is for the user who initiated the console session.

The formats of registry values are converted according to their data type. The following table shows how registry values of each data type are collected.

Data type	Collection method
REG_SZ, REG_EXPAND_SZ	The character string is not converted.
REG_MULTI_SZ	Information is collected in the form of several character strings connected by commas (,). For example: xxx,yyy,zzz
REG_DWORD#1	The numerical value is collected as a decimal character string.
REG_BINARY, REG_QWORD#2	Each byte of the binary value is converted to a hexadecimal character string, and the resulting strings are connected by spaces. For example: xx yy zz

#1: Not collected when the data type is REG_DWORD_BIG_ENDIAN.

#2: Not collected when the computer is running Windows Server 2003 or Windows XP.

(14) Updating device information

The device information on the management server is updated based on the information collected from managed computers.

The relative priority of device information depends on how the information is collected. For example, because device information for a computer with the agent installed is updated with information supplied by the agent, device information is not updated using information supplied by SNMP. The order of priority when updating device information is as follows:

1. Device information collected by the agent[#1]
2. Device information collected via a Windows administrative share
3. Device information collected by SNMP
4. Device information collected from Active Directory
5. Device information collected by MDM linkage
6. Device information collected by ARP
7. Device information collected by ICMP (limited to confirming device presence)
8. Device information entered by an administrator[#2]

#1: Includes device information for offline-managed computers supplied via an online-managed computer.

#2: Information entered by an administrator always takes priority for the **Device Type** item.

The factors that determine whether device information is updated are how the new information was collected, and how the information already in the database was collected. The following table shows whether device information is updated for each combination of these factors.

Method of device information collection		Existing information		
		Entered by administrator	Collected from device	Not collected
Entered by administrator		Y[#1]	Y	Y
Collected from device	Data collected	Y[#2]	Y	Y
	Collected with empty value	N	Y[#3]	Y[#3]
	Not collected or value unchanged	N	N	N

Legend: Y: Device information is updated. N: Device information is not updated.

#1: An administrator can enter the **Host Name**, **IP Address**, **Subnet Mask**, **Operating System**, and **Device Type** items.

#2: Values of **Device Type** entered by an administrator always take priority, and are not replaced with information collected from a device.

#3: If the **Host Name** field is collected with an empty value, the device information is updated with the host ID.

Tip

When you collect device information from a device with more than one set of network information, the device information sometimes appears to relate to more than one device. In this case, to ensure that the number of devices is accurately tracked, only the device that matches the first set of network information is updated. Devices that match the other sets of network information are deleted. When this occurs, the date and time of agent deployment is aggregated in the remaining device information.

(15) Information collected when updating device information

The following device information is collected when you update device information manually or as part of a regular search for devices:

- Device type
- System information
- Hardware information
- Installed software information
- Windows Update information
- Anti-virus product information
- Service security settings
- OS security information
- Hibun information
- Shared management items for device and hardware asset information
- Added management items

(16) Events generated when updating device information

When an update to device information results in particular items being changed, added, or deleted, an event is generated and appears in the Events module.

The following table describes what actions cause events to be generated.

Item of device information		Event	Event trigger
Hardware information	Memory capacity	Changed	The new data differs from the existing data.
Hard disk	The following items of hard disk information: • Disk name • Capacity • Interface	Added	No part of the existing data exactly matches the new data.
		Deleted	No part of the new data exactly matches the existing data.
Installed software information	Software name	Added	No part of the existing data exactly matches the new data, with the exception of Windows Update information.
		Deleted	No part of the new data exactly matches the existing data, with the exception of Windows Update information.
	Version	Changed	When data for a given Software Name differs in the new and existing data, with the exception of Windows Update information.
Security information	Windows Update	Changed	The new data differs from the existing data.
	Service security settings	Added	The new data is not found in the existing data.
		Deleted	The existing data is not found in the new data.
	Account name in OS security settings	Added	The new data is not found in the existing data.
		Deleted	The existing data is not found in the new data.

Item of device information		Event	Event trigger
Security information	The following items for an account name in OS security settings: • Days since last password change • Password strength • Password never expires	Changed	The value of any of these items for a given account name differs in the existing and new data.
	Power on password in OS security settings	Changed	The new data differs from the existing data.
	Guest account in OS security settings	Changed	The new data differs from the existing data.
	Auto logon in OS security settings	Changed	The new data differs from the existing data.
	Shared folder in OS security settings	Changed	The new data differs from the existing data.
	Administrative share in OS security settings	Changed	The new data differs from the existing data.
	DCOM in OS security settings	Changed	The new data differs from the existing data.
	Anonymous access in OS security settings	Changed	The new data differs from the existing data.
	The following items of screen saver information in the OS security settings • Screen saver • Password • Startup time	Changed	The value of any of these items differs in the existing and new data.
	Windows Firewall in OS security settings	Changed	The new data differs from the existing data.
	Remote desktop in OS security settings	Changed	The new data differs from the existing data.

(17) Collecting the device revision history

Users in an organization might change the computer configuration by, for example, inserting and removing a memory card, or installing or uninstalling software. It is not easy for the system administrator to find problems that are caused by changes, such as the theft of a memory card, or installation of software not permitted in the organization.

If information for devices managed by JP1/IT Desktop Management 2 changes, information before and after the change can be collected in the revision history. The revision history allows you to check only the device information that has changed, helping you find problematic changes easily. Check the revision history on a regular basis to confirm that no suspicious changes have been made.

To collect the revision history, you must specify the collection of revision history in the Settings module.

Process for collecting the revision history

If device information changed, the new device information is saved in the database. The new device information is compared with the old one at 0:00 everyday, and any differences are collected as the revision history for the day.

How to check the revision history

You can use the following two methods to check the collected revision history.

Checking the revision history displayed in the operation window

The **Revision History** view of the Device module allows you to check the latest revision history. This view displays a maximum of 600,000 entries in the revision history. If the number of entries exceeds 600,000, the oldest information is overwritten by the latest information.

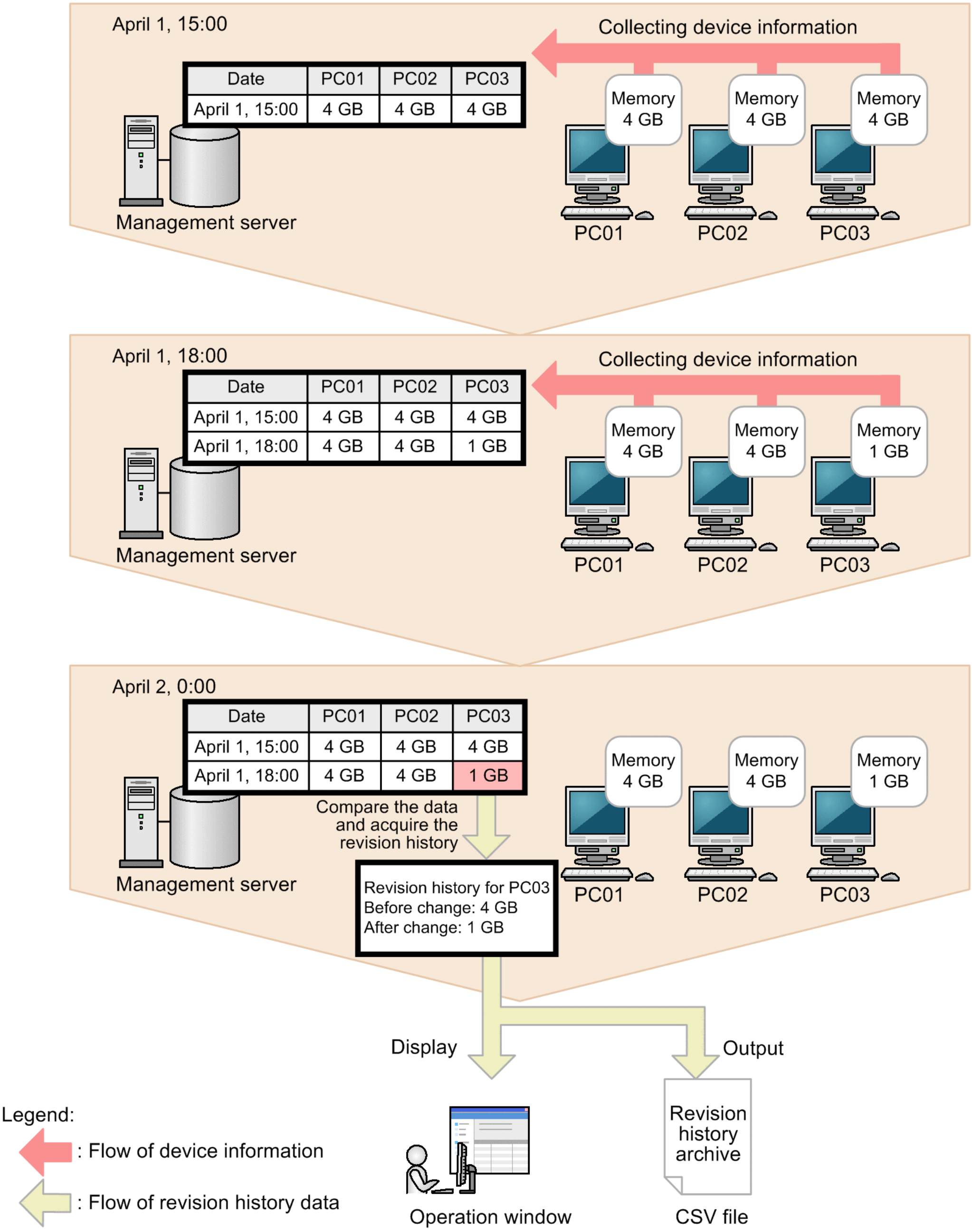
Checking the revision history archive output to a CSV file

You can output the revision history archive to a CSV file. The output revision history archive allows you to retain information about the changes even if the revision history contains more than 600,000 entries. To output the revision history archive, you must specify the output settings during the setup.

Important note

If you delete device information, the host name of the deleted device is not displayed in the **Revision History** view of the Device module. If you need to check the host name of the deleted device, check the revision history archive output to a CSV file.

The following figure shows an overview of collecting and checking the revision history.



Date	PC01	PC02	PC03
April 1, 15:00	4 GB	4 GB	4 GB

Date	PC01	PC02	PC03
April 1, 15:00	4 GB	4 GB	4 GB
April 1, 18:00	4 GB	4 GB	1 GB

Date	PC01	PC02	PC03
April 1, 15:00	4 GB	4 GB	4 GB
April 1, 18:00	4 GB	4 GB	1 GB

Revision history for PC03
Before change: 4 GB
After change: 1 GB

(18) Device information which can be collected in revision history and the conditions to detect changes

The following table describes the device information items whose changes can be collected in the revision history, and when JP1/IT Desktop Management 2 detects changes in device information.

Device information item	Changes collected in revision history	Conditions to detect changes
Mode	Changes to the management mode (**Discovered**, **Managed**, or **Ignored**) are collected.	The management mode is changed as follows: • **Discovered** is changed to **Managed**. • **Managed** is changed to **Ignored**. • **Ignored** is changed to **Managed**. • Device information indicated as **Managed** is deleted.
Management Type	Changes to the following management types are collected: • Agent Management • Agentless Management (Authentication Successful) • Agentless Management (Authentication Failed) • MDM Linkage Management	The device information has changed since the last time it was collected.
Host Name[#1]	Changes to the host name collected as computer information in the system information are collected.	• The device information has changed since the last time it was collected. • The host was changed in the operation window.
UUID (Computer Details)	Changes to the UUID collected as computer information in the system information are collected.	The device information has changed since the last time it was collected. Note, however, that changes to only the case of hexadecimal alphabetic letters (A to F or a to f) are ignored.
Total Memory (Computer Details)	Changes to the amount of memory collected as computer information in the system information are collected.	The device information has changed since the last time it was collected.
External Storage Capacity (Smart Device Information)	Changes to the external storage capacity collected as smart device information in the system information are collected.	The device information has changed since the last time it was collected.
IMSI (Smart Device Information)	Changes to the IMSI collected as smart device information in the system information are collected.	The device information has changed since the last time it was collected.
IP Address (Network Details)[#1, #2, #3]	Changes to an IP address collected in Network Details in the system information are collected.	• The device information has changed since the last time it was collected. • An IP address has changed in the operation window.
MAC Address (Network Details)[#2]	Changes to the MAC address collected in Network Details in the system information are collected.	The device information has changed since the last time it was collected. Note, however, that changes to only the case of hexadecimal alphabetic letters (A to F or a to f) are ignored.
Processor Name (Processor Details)[#2]	Changes to the processor collected in Processor Details in the hardware information are collected.	The device information has changed since the last time it was collected.

Device information item	Changes collected in revision history	Conditions to detect changes
Disk Name (Hard Disk Details)#2	Changes to the disk name collected in Hard Disk Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Hard Disk Capacity (Hard Disk Details)#2	Changes to the hard disk capacity collected in Hard Disk Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Drive Name (CD-ROM Drive Details) #2	Changes to the drive name collected in Drive Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Video Chip (Video Controller Details)#2	Changes to the video chip collected in Video Controller Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Video Chip VRAM Capacity (Video Controller Details)#2	Changes to the video chip VRAM capacity collected in Video Controller Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Video Driver (Video Controller Details)#2	Changes to the video driver collected in Video Controller Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Sound Card Product Name (Sound Card Details) #2	Changes to the sound card product name collected in Sound Card Details in the hardware information are collected.	The device information has changed since the last time it was collected.
Installed Software Details	Changes to the following items in Installed Software Details are collected: • Software Name • Version • Product ID	The device information has changed since the last time it was collected.
Department (Common Fields)	Changes to Department, which is a shared management item for asset information and device information, are collected.	• The device information has changed since the last time it was collected. • The department has changed in the operation window. • The information is changed by importing a CSV file.
Location (Common Fields)	Changes to Location, which is a shared management item for asset information and device information, are collected.	• The device information has changed since the last time it was collected. • The location has changed in the operation window. • The information is changed by importing a CSV file.
User Name (Common Fields)	Changes to User Name, which is a shared management item for asset information and device information, are collected.	• The device information has changed since the last time it was collected. • The user name has changed in the operation window. • The information is changed by importing a CSV file.

#1: For a device that has one or more IP addresses with DHCP enabled, if the host name or an IP address is changed as follows, the changes in step 2 cannot be collected in the revision history.

1. The system administrator uses the operation window to change the device's host name or IP address for which DHCP is disabled.

2. After the above change, only the IP addresses for which DHCP is enabled are changed automatically.

In this case, the values of the device information and revision history displayed in the operation window are temporarily inconsistent. When the device information is collected the next day, the revision history is also collected and the values become consistent.

#2: If a device information item has multiple values, changes are collected if at least one value has been added, changed, or deleted. However, changes to only the order of values are not collected. The following table uses an example of Disk Name (Hard Disk Details) that has multiple values to show whether the revision history is collected.

Device information value		Revision history collected?
Before the change	After the change	
HDDModel1, HDDModel2	HDDModel2, HDDModel3	Y
HDDModel1, HDDModel2	HDDModel1	Y
HDDModel1, HDDModel2	HDDModel1, HDDModel2, HDDModel3	Y
HDDModel1, HDDModel2	HDDModel2, HDDModel1	N

Legend: Y: Collected. N: Not collected.

#3: If DHCP is enabled for both the new and old IP addresses, the revision history is not collected. If DHCP is disabled for either the new or old IP address, the revision history is collected. The DHCP setting cannot be acquired if device information is collected by using SNMP or ICMP. If the DHCP setting cannot be acquired, the IP addresses are compared while DHCP is assumed to be disabled.

(19) Behavior after managed computers are disconnected from the network

If a managed computer loses network connectivity, the system attempts to connect to the computer at the interval specified in the agent configurations as if the computer were still connected to the network.

In this scenario, the management server cannot determine whether the managed computer has disconnected from the network or was switched off. Therefore, an online-managed computer that has disconnected from the network is assumed to have been turned off if a length of time equivalent to the server connection interval plus 10 minutes has elapsed since the last alive confirmation date/time. An agentless device is assumed to be turned off as soon as the management server is unable to collect information from the device.

During search for devices connected to the network, a managed device is not assumed to be turned off even if the management server is unable to collect information from the device. To check the status of an agentless device, select **Update Device Details** in the Device list or check the status after the information is updated regularly.

The device information for a computer remains unchanged until the computer reconnects to the network and JP1/IT Desktop Management 2 is able to collect up-to-date information for the computer.

Behavior of online-managed computers when disconnected from the network

Computers that are disconnected from the network are still subject to security policies. As a result, the following occurs:

- The user is prevented from starting restricted software.
  Blocked attempts to start restricted software are recorded as events on computers with the agent installed.
- The user is prevented from using devices if the security policy prohibits their use.
- Operation log entries are recorded.

Operation logs are stored locally in the agent-installed computer.

> **Tip**
>
> These do not occur on agentless computers. This is because the security status of an agentless computer is judged by assessing its device information against the security policy on the management server, not as a result of sending a security policy to the computer itself.

Behavior when computers reconnect to the network

When a computer reconnects to the network after a period of isolation, it uploads security-related items and the latest device information according to the monitoring interval specified in the agent configurations, not immediately upon reconnection. Events that were saved locally while the computer was isolated from the network are uploaded when the computer next communicates with the management server.

A user's computer uploads operation logs to the management server. When the computer reconnects to the network, all the operation logs stored on the computer are uploaded at the next scheduled upload time.

Assessment of security status

While a computer is isolated from the network, its security status continues to be assessed based on the information in the database that was collected by the management server before the computer became isolated from the network.

(20) Creating groups

Groups are classified into system-sorted groups (Device type, Network, Department, and Location) that are automatically created by the system and user-defined groups created by the system administrator. Devices are automatically sorted into groups according to the device information and hardware asset information. The created groups are displayed in the menu area.

The following describes how each type of group is created.

Device type

Groups are created according to the device types (such as PC, server, or printer) collected from devices. When device information is collected from a computer with the device type `PC` or `Server`, subgroups are created for each OS.

Network

Groups are created for each network address based on the IP addresses and subnet masks of devices.

Department

Groups are created based on the department information collected from devices. If an administrator has registered a department hierarchy in the **Asset Field Definitions** view of the Settings module, it is automatically reflected in the group hierarchy.

When linking with Active Directory, the OU hierarchy is reflected in the group hierarchy.

Location

Groups are created based on the location information collected from devices. If an administrator has registered a location hierarchy in the **Asset Field Definitions** view of the Settings module, it is automatically reflected in the group hierarchy. If you use SNMP to collect device information, the location values collected by SNMP are reflected in the created groups.

When linking with Active Directory, the location values collected for each computer are reflected in the created groups.

User-Defined

The system administrator adds groups in the **Edit User-Defined List** dialog box that opens from the menu area. The managed computers are automatically sorted into the corresponding groups according to the conditions specified for each group in the user definitions.

Related Topics:

- 2.4.3 Linking with Active Directory

(21) Process for definitions and groups for departments and locations

In the Settings module, you can edit definitions of departments and locations in device information collected from users. The definitions you added in the Settings module are automatically added as groups in the menu area of the Assets module and the Device module. You can also view a list of definitions that are deleted due to office reorganization or personnel changes and delete all these definitions at one time. To do this, use the **Delete Hierarchies Used in Old Organization** dialog box that opens from the menu area of the Assets module and the Device module.

Department and location groups can be edited in the menu area.

The following describes the available operations and results when editing definitions in the Settings module and when editing groups in the menu area.

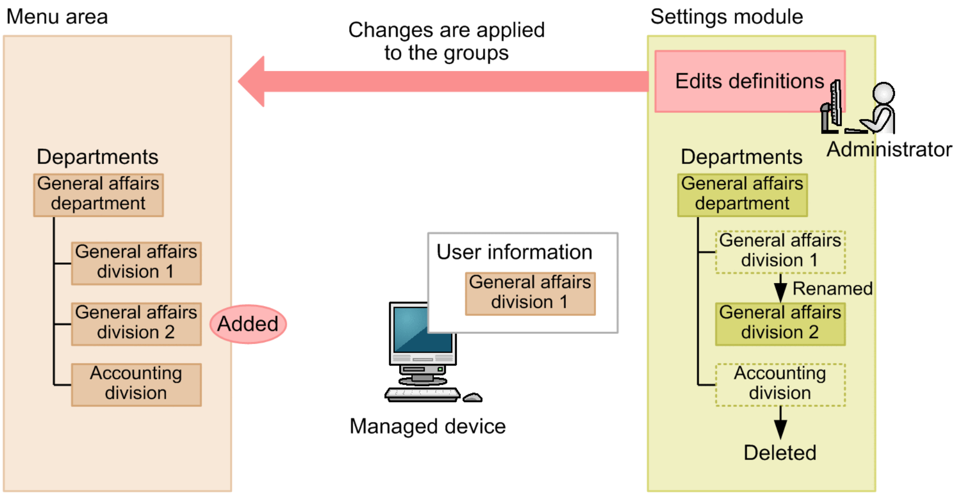
When editing definitions in the Settings module

In the Settings module, you can do the following to edit information:

- Add definitions
- Delete definitions
- Rename definitions
- Change the position of a definition in the hierarchy

If you edit information in the Settings module, the changes are applied to the definitions, and not to the user information on the devices. If you add, rename, or rearrange a definition, a new group corresponding to the edited definition is added while the group for the definition before the change remains in the menu area. If you delete a definition, the group corresponding to the definition you deleted also remains in the menu area.

The following figure shows the results that are applied to the menu area and user information on the device when a definition is renamed and another definition is deleted in the Settings module.


Menu area
Changes are applied to the groups
Settings module
Edits definitions
Administrator
Departments
General affairs department
General affairs division 1
General affairs division 2
Added
Accounting division
User information
General affairs division 1
Managed device
Departments
General affairs department
General affairs division 1
Renamed
General affairs division 2
Accounting division
Deleted

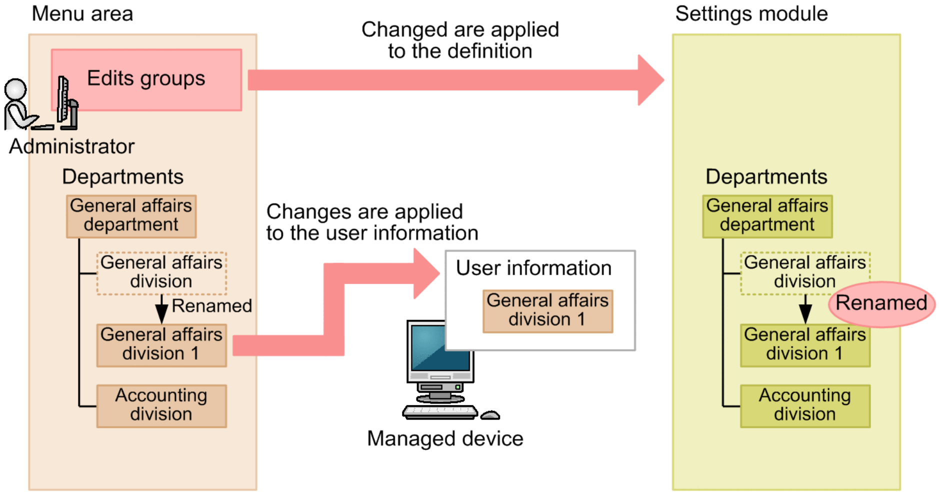
When editing groups in the menu area

In the menu area, you can do the following to edit information:

- Rename groups
- Delete groups

If you edit groups in the menu area, the changes are also applied to the user information on the device registered in the group, in addition to the group definition.

The following figure shows the results that are applied to the definition and user information on the device when a group is renamed in the menu area.



Menu area
Edits groups
Administrator
Departments
General affairs department
General affairs division
Renamed
General affairs division 1
Accounting division
Changed are applied to the definition
Changes are applied to the user information
User information
General affairs division 1
Managed device
Settings module
Departments
General affairs department
General affairs division
Renamed
General affairs division 1
Accounting division

Tip

Create department and location definitions that reflect how you intend to manage devices. If the definitions disagree with the user information, edit the user information so that devices are registered in the groups you defined, as intended. By doing so, an administrator can manage devices in groups aligned with his or her intentions.

Settings required after definitions and groups are edited

If definitions and groups are edited due to office reorganization or personnel changes, you must do the following.

If department definitions are added

Do the following for the added departments:

- Assign security policies
- Assign agent configurations
- Add the department administrator to the administration scope

If department definitions are changed

Do the following for the changed departments, except for the case where you changed the definitions by using the `ioassetsfieldutil import` command:

- Assign security policies
- Assign agent configurations
- Add the department administrator to the administration scope

In addition, delete the following asset information items associated with the department of the old organization, or associate them with another department:

- Hardware asset information

- Software asset information
- Contract information

If a department definition is deleted

Delete the following asset information items associated with the deleted department, or associate them with another department:

- Hardware asset information
- Software asset information
- Contract information

If a department group is deleted

Delete the following asset information items associated with the deleted department, or associate them with another department:

- Hardware asset information
- Software asset information
- Contract information

(22) Overview of user-defined groups

User-defined groups, into which devices are sorted based on a given condition, can be edited in the menu area of the Security module and Device module.

You can assign security policies to user-defined groups. Unlike other groups, user-defined groups cannot be used for assigning agent configurations or reports.

Only one level of a user-defined group can be created. The name of a user-defined group can be a string with 256 or fewer ASCII characters other than control characters.

Devices are sorted according to the type of device information, target items, judgment condition, and judgment value specified in the user-defined group conditions. Therefore, you cannot directly sort devices into groups. A device that matches multiple user-defined groups is sorted into all the groups it matches. No devices are sorted into user-defined groups for which no conditions are set.

Type of device information

The type of device information of the target item. You can select **Device list (sorted by system)** (**Device type**, **Network**, **Department**, or **Location**) or **Custom Field** whose information is added by the system administrator.

Target items

The target item for the user-defined group conditions. If multiple target items are set, only the devices that meet the conditions for all the target items are sorted into groups.

Judgment conditions

The conditions used to compare the target item value with the judgment value. Devices are sorted into groups based on the result of the comparison.

Judgment value

The value that is compared with the target item according to the judgment condition.

The **Devices for Which Conditions Do Not Apply** group appears in the menu area by default. Devices that are not sorted into the user-defined groups created by the system administrator will be sorted into this group.

Judgment conditions and judgment values that can be specified for user-defined groups

Judgment conditions and judgment values that can be specified for a user-defined group vary depending on the type of device information. The following tables list the judgment conditions and judgment values that can be specified for each type of device information.

If Type of device information is Device list (sorted by system)

Judgment condition	Judgment value
Equals the judgment value	Hierarchy values displayed in the pull-down menu
Does not equal the judgment value	
Equals the judgment value (including lower-hierarchy values)#	
Does not equal the judgment value (including lower-hierarchy values)#	

#: Cannot be specified if the target item is **Network**.

If Type of device information is Custom Field

Data type of judgement item	Judgment condition	Judgment value
Text	Equals the judgment value	Character string with 1 to 256 characters The specified value is case sensitive. Single-byte characters are distinguished from double-byte characters during judgment.
	Does not equal the judgment value	
	Begins with the judgment value	
	Ends with the judgment value	
	Contains the judgment value	
Number	Equals the judgment value	-2,147,483,647 to 2,147,483,647
	Does not equal the judgment value	
	Equal to or greater than the judgment value	
	Less than or equal to the judgment value	
	Greater than the judgment value	
	Less than the judgment value	
Enumeration	Equals the judgment value	Value displayed in the pull-down menu The specified value is case sensitive. Single-byte characters are distinguished from double-byte characters during judgment.
	Does not equal the judgment value	

When devices are sorted into user-defined groups

Devices are sorted into groups according to the specified user-defined group conditions when one of the following occurs:

- The name of a user-defined group is changed.
- A user-defined group is deleted.
- User-defined group conditions are edited.
- A device that belongs to the system-sorted group specified for the target item by the user-defined group conditions moves to another group.
- The **Custom Field** information specified for the target item by the user-defined group conditions is updated.

- The **Custom Field** information specified for the target item by the user-defined group conditions is deleted.

(23) Deleting duplicate device information

If an action such as reinstalling the operating system causes the agent program to be removed from a computer, a situation might arise in which the same device is registered more than once in the database. To delete duplicate device information:

- In the **Device Inventory** view of the Device module, delete the device whose Last Modified Date/Time is farther in the past.
- In the **Device Inventory** view of the Device module, sort the list of devices by MAC address. If two devices have the same MAC address, remove one of the devices.

2.6.3 Controlling devices

You can control the devices managed by JP1/IT Desktop Management 2. This section describes how to control devices in the following ways:

Send messages to users

You can send a message to a user of a computer. You can also send the same message to several computers at once.

Control a computer's access to the network

You can permit or deny a computer network access.

Collect user information

You can collect information from users by displaying an input window on the user's computer.

Turn a computer on or off

You can restart computers remotely and turn computers on and off. This function can be used for device management, remote control, ITDM-compatible distribution, and distribution using Remote Installation Manager.

Collect the latest device information

You can collect the latest device information any time you wish.

Define prohibited software

You can view a list of software installed on a computer, and designate certain software as prohibited software. This allows you to view the violation level of the computer in terms of installed software in the Security module. You can also prevent users from using certain software, or uninstall it remotely.

Uninstall software

You can uninstall software by selecting it from a list of software installed on a computer.

Remotely control a computer

You can access the desktop of a computer and control it remotely.

Control smart devices

You can lock, wipe, and reset passcodes on smart devices managed by JP1/IT Desktop Management 2.

(1) Conditions for power control

This section describes the conditions that must be met to control the power status of a computer.

Conditions for turning on a computer

If there is a value for AMT Firmware Version in the device information, the system uses AMT to turn on the computer. If not, the system uses Wake on LAN. The following conditions must be met to turn on a computer:

Important note

You cannot turn on a computer if any of the following apply:

- The computer is in a wireless LAN environment
- A LAN and wireless LAN are connected to the same subnet
- The computer is suspended in battery mode

Conditions on the management server

When using AMT

- The AMT user ID and password must be registered in the **AMT** view under **Inventory** in Settings module.
- Port 16992 used by AMT must be available.
- The name of the device to be turned on must be resolved from a host name.

When using Wake on LAN

- None.

Conditions on the computer

When using AMT

- The computer is connected to the management server.
- The agent is installed on the computer.
- The computer supports AMT.
  A computer supports AMT if a value appears for AMT Firmware Version in the device information.
- The user name and password for AMT are entered in the BIOS settings.
- Port 16992 used by AMT must be available.

Tip

You can configure AMT in agent configurations which you can then apply to computers with the agent installed. This means that the administrator does not need to configure the BIOS on each computer individually.

Tip

You can register one combination of AMT user ID and password on a given management server. For this reason, when using AMT to turn computers on and off, the same ID and password must be used on each computer.

When using Wake on LAN

- The computer is connected to the management server.
- The agent is installed on the computer.
- The computer supports Wake on LAN.
- Magic Packet mode is enabled in the Wake on LAN settings.

Conditions for turning off a computer

The following conditions must be met to turn off a computer:

> **Important note**
>
> A relay system cannot turn off a computer.

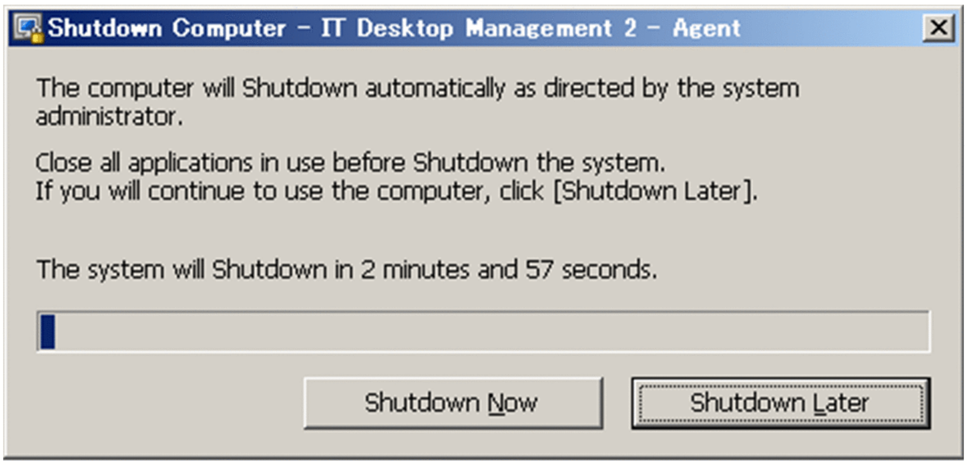
Conditions on the management server

None.

Conditions on the computer

- The computer is connected to the management server.
- The agent is installed on the computer.

A **Shutdown Computer** dialog box appears on a computer you are turning off.



Shutdown Computer - IT Desktop Management 2 - Agent

The computer will Shutdown automatically as directed by the system administrator.

Close all applications in use before Shutdown the system.
If you will continue to use the computer, click [Shutdown Later].

The system will Shutdown in 2 minutes and 57 seconds.

If there is no intervention by the user, the computer will shut down automatically after 180 seconds.

Note the following when shutting down a computer:

- A computer will not shut down automatically if its screen saver is active and password protected.
- A locked computer will not shut down automatically.
- A computer will not shut down automatically if a user is working on an open file.
- A computer will not shut down automatically if another user is logged on to the computer.
- If the user has not yet logged on to the computer, the computer shuts down without displaying the **Shutdown Computer** dialog box.
- If the computer is instructed to turn off by the management server while the **Shutdown Computer** dialog box is displayed, the latter instruction is ignored.

Conditions for restarting a computer

The following conditions must be met to restart a computer:

Important note

A relay system cannot restart a computer.

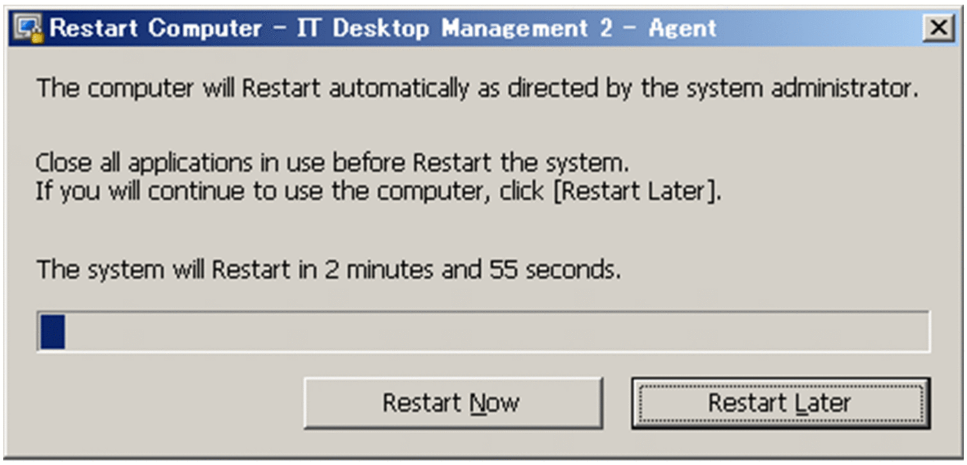
Conditions on the management server

None.

Conditions on the computer

- The computer is connected to the management server.
- The agent is installed on the computer.

A **Restart Computer** dialog box appears on a computer you are restarting.



Restart Computer - IT Desktop Management 2 - Agent

The computer will Restart automatically as directed by the system administrator.

Close all applications in use before Restart the system.
If you will continue to use the computer, click [Restart Later].

The system will Restart in 2 minutes and 55 seconds.

A computer is restarted at a time specified in the **Settings to shut down and restart the computer** area in the **User notification settings** view in the agent configuration. If the **Automatically start if no response is received from the user within the specified period** check box is selected in the agent configuration, and the user does not respond to the dialog box, the computer automatically restarts after the time period specified in the agent configuration elapses from when the dialog box was displayed. If the **Follow the response of the user in the dialog box that instructs the user to shut down or restart the computer** check box is selected in the agent configuration, the dialog box remains on screen, and the computer does not restart until the user clicks the appropriate button.

Note the following when restarting a computer:

- A computer will not restart automatically if its screen saver is active and password protected.
- A locked computer will not restart automatically.
- A computer will not restart automatically if a user is working on an open file.
- A computer will not restart automatically if another user is logged on to the computer.
- If the user has not yet logged on to the computer, the computer restarts without displaying the **Restart Computer** dialog box.
- If the computer is instructed to turn off by the management server while the **Restart Computer** dialog box is displayed, the instruction to turn off takes precedence. In this scenario, the **Restart Computer** dialog box is replaced with a **Shutdown Computer** dialog box.

(2) Prerequisites for using AMT

If the AMT version is lower than 6.0, a DHCP environment is a prerequisite. A wireless LAN environment is not supported.

The features of JP1/IT Desktop Management 2 have different requirements in terms of the AMT version required on the computer.

The following table shows the version of AMT required to use each feature.

Feature		Description	Required AMT version
Power control		Turns remote computers on and off.	3.0 to 9.5
Collecting AMT firmware versions		Collects the AMT version as part of a computer's device information.	
Using IDE redirection#		Allows you to use CD-ROM drives remotely when using the remote control feature.	
Remote control over RFB connections		Allows you to use the remote control feature over a RFB connection.	6.1 to 9.5
AMT configuration	Enable IDE redirection	This feature allows the use of the IDE redirection feature of AMT.	6.1 to 9.5
	Enable remote KVM	By enabling remote KVM on a computer in the agent configurations, you can remotely control the computer over an RFB connection. You can also set the authentication information needed to remotely control the computer.	
	Enable AMT and set passwords for AMT users with administrator permission	This feature enables AMT if disabled. You can also set the password for AMT users with administrator permission (the admin user).	7.0 to 9.5

#: In AMT versions 7.0 and 8.0, you cannot use the IDE redirection feature on computers on which AMT is enabled in the **AMT Settings** view in the Settings module.

To automatically enable AMT on a computer:

AMT must be enabled on a computer before you can use AMT-based features.

To automatically enable AMT on a computer, set an administrator-permission password used by AMT in the **AMT Settings** view of the Settings module.

You can then enable AMT automatically on computers and access them with administrator permission.

If there is no administrator password set for AMT on the computer, the password you enter in the **AMT Settings** view is registered in AMT. You cannot set a new password if one is already registered in AMT. In this case, specify the registered password. If an administrator password is set but AMT is disabled, you need to first enable AMT on the computer.

To use these features, the management server must be configured in the following ways:

To control the power of a computer using AMT:

Set the credentials needed to communicate with AMT on the computer in the **Set Credentials** area of the **AMT Settings** view of the Settings module.

Thereafter, AMT will be used to control the power state of the computer.

To collect the AMT firmware version from a computer:

Set the credentials needed to communicate with AMT on the computer in the **Set Credentials** area of the **AMT Settings** view of the Settings module.

Thereafter, the AMT firmware version will be collected at the time when the device information is collected.

To remotely control a computer via RFB connection:

The remote KVM feature must be enabled in AMT on the remote computer.

You can edit agent configurations in the **Agent Configuration and Installation Set Creation** view of the Settings module. In the **AMT** view, select the **Allow Remote KVM** check boxes.

If AMT is enabled on the computer, changes to AMT settings take effect each time the agent configurations are applied to the computer. If AMT is disabled on the computer, you need to configure the agent configurations to enable ATM automatically.

When you set up the computer in this manner, when an attempt by the remote control feature to connect to a computer using a standard connection fails, the remote control feature then attempts to connect using RFB. You can configure the system to use RFB when connecting from the **Connect** item in the **File** menu of the **Remote Control** view.

To use IDE redirection:

The IDE redirection feature must be enabled in the AMT settings on the computer. However, in AMT versions 7.0 and 8.0, you must set AMT from BIOS because you cannot use the IDE redirection feature, even if AMT is enabled on the computers.

Edit the agent configuration in the **Agent Configuration and Installation Set Creation** view in the Settings module. At this time, select the **Enable IDE redirection** check box in **AMT Settings**.

If AMT is enabled on the computer, the AMT settings will be changed as soon as the agent configurations are applied. If the AMT is disabled on the computer, a configuration to automatically enable AMT on the computer is required.

In this way, you can use the IDE redirection feature when remotely controlling a computer.

Related Topics:

- (1) Conditions for power control

2.6.4 Managing offline computers

Besides network-accessible computers, JP1/IT Desktop Management 2 can manage computers that it cannot access over the network, including standalone computers and computers connected to an isolated network at a remote site.

The management of computers that cannot be accessed over a network is achieved by using external media to install the agent on the computer and collect device information.

This process of using external media to manage computers that the management server cannot access over the network is called `offline management`, in contrast to`online management` which involves the management of computers that are connected to the management server by a network.

Storage capacity required on external storage devices

Device information is collected from offline-managed computers by an information collection tool stored on external media. The following free space must be available on the external media:

5 MB + (50 KB x the number of computers for which device information is collected)

There are some differences in management server capabilities depending on whether a computer is managed online or offline. For details on these differences, see (1) Functional differences between agent/agentless management.

(1) Functional differences between agent/agentless management

There are some differences in management server capabilities depending on whether the managed computers have an agent installed or are agentless. In the case of computers with an installed agent, other differences arise depending on whether the computers are managed online or offline.

The following table describes functional differences by configuration type:

Function		Managed computers		
		Agent installed		Agentless
		Online management	Offline management	
Acquisition of device information#1		Y	Y	D
Security diagnostics	Assign security policies	Y	Y	Y
	Evaluate security	Y	Y	D#2
Actions at security policy violation	Automatic security measures	Y	N	N
	Restrict printing	Y	N	N
	Disable data export	Y	N	N
	Disable software startup	Y	N	N
	Acquire operation logs	Y	N	N
	Send warning messages	Y	N	N
	Power on/off	Y	N	N
Management of asset information	Manage hardware	Y	Y#3	D
	Manage software licenses	Y	Y	D
	Manage software	Y	Y	Y
	Manage contracts	Y	Y	Y
Distribution of software and files	Distribute software	Y	Y#4	N
	Distribute files	Y	Y#4	N
	Uninstall software	Y	N	N
Remote control of devices	Remote control of computers	Y	N	D#5
	Connection requests from computers	Y	N	N
	File transfer	Y	N	N
	Chat	Y	N	N

Function		Managed computers		
		Agent installed		Agentless
		Online management	Offline management	
Management of device network connections	Enable network access control	Y	N	N
	Control network connections	Y	N	Y
Report creation		Y	Y	D

Legend: Y: Supported. D: Depends on the collectable device information. N: Not supported.

#1: The device information that can be collected depends on whether the computers have installed agents or are agentless. See the following for details on the information collected from each type of computer.

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

#2: Use the Windows Administrative Share feature to evaluate the security of agentless computers. Screensaver security cannot be determined on a per-account basis when using agentless management.

#3: USB devices cannot be registered.

#4: Only distribution using Remote Installation Manager can be performed. ITDM-compatible distribution cannot be performed.

#5: RFB protocol must be used for remote control.

2.6.5 Agentless management

JP1/IT Desktop Management 2 can perform management without an agent having to be installed on the computers (agentless computers). This means that a computer used in research or a server used for business purposes, for example, on which management software cannot be installed for practical reasons, can still be managed under JP1/IT Desktop Management 2 in the same way as a user computer.

To use agentless management, configure computers discovered during a network search as managed computers.

Important note

Configuring a computer for agentless management has security implications. Fully consider the effects before deciding to use agentless management.

Agentless management can be performed using Windows administrative shares, SNMP, or Active Directory. The three methods are described below:

Agentless management using Windows administrative shares

Non-resident executable programs are sent periodically to agentless computers via login to Windows administrative shares. The distributed programs collect device information using WMI.

Information is acquired at the following times:

- When a network search is executed
- At the update interval specified in the **Agentless Management** view
- When you select **Update Device Details** from the **Action** menu in the Device list in the Device module.

Tip

You can also collect device information by selecting **Update Device Details** from the pop-up menu that appears when you right-click a computer name.

Important note

Agentless management is based on executable programs for acquiring device information, sent from the management server to the managed computers. The Windows security settings block this operation by default. You must therefore lower the security level setting to allow the executable programs to be distributed. Consider how this will affect your system before deciding to change the security level.

Agentless management using SNMP

In this method, device information is collected periodically by SNMP, using authentication via the standard SNMP communication protocol. The information is collected at the same times as for agentless management based on Windows administrative shares.

Agentless management using Active Directory

In this method, device information is collected for devices managed by Active Directory.

Information is acquired at the following times:

- When a network search is executed
- When you select **Update Device Details** from the **Action** menu in the Device list in the Device module

Important note

Agentless management using Active Directory collects information on the domain controller. If the domain controller and managed devices are out of sync, the collected information might differ from the information of the managed devices.

Setup must be performed on the computers to use Windows administrative shares, SNMP, or Active Directory. For details, see 4.2.7 Prerequisites for agentless management.

In agentless management, the functionality available from the management server differs in some respects from the functionality available when using installed agents. For details about the differences, see (1) Functional differences between agent/agentless management.

Important note

To perform agentless security management, use Windows administrative shares.

(1) Functional differences between agent/agentless management

There are some differences in management server capabilities depending on whether the managed computers have an agent installed or are agentless. In the case of computers with an installed agent, other differences arise depending on whether the computers are managed online or offline.

The following table describes functional differences by configuration type:

Function		Managed computers		
		Agent installed		Agentless
		Online management	Offline management	
Acquisition of device information[#1]		Y	Y	D
Security diagnostics	Assign security policies	Y	Y	Y
	Evaluate security	Y	Y	D[#2]
Actions at security policy violation	Automatic security measures	Y	N	N
	Restrict printing	Y	N	N
	Disable data export	Y	N	N
	Disable software startup	Y	N	N
	Acquire operation logs	Y	N	N
	Send warning messages	Y	N	N
	Power on/off	Y	N	N
Management of asset information	Manage hardware	Y	Y[#3]	D
	Manage software licenses	Y	Y	D
	Manage software	Y	Y	Y
	Manage contracts	Y	Y	Y
Distribution of software and files	Distribute software	Y	Y[#4]	N
	Distribute files	Y	Y[#4]	N
	Uninstall software	Y	N	N
Remote control of devices	Remote control of computers	Y	N	D[#5]
	Connection requests from computers	Y	N	N

Function		Managed computers		
		Agent installed		Agentless
		Online management	Offline management	
Remote control of devices	File transfer	Y	N	N
	Chat	Y	N	N
Management of device network connections	Enable network access control	Y	N	N
	Control network connections	Y	N	Y
Report creation		Y	Y	D

Legend: Y: Supported. D: Depends on the collectable device information. N: Not supported.

#1: The device information that can be collected depends on whether the computers have installed agents or are agentless. See the following for details on the information collected from each type of computer.

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

#2: Use the Windows Administrative Share feature to evaluate the security of agentless computers. Screensaver security cannot be determined on a per-account basis when using agentless management.

#3: USB devices cannot be registered.

#4: Only distribution using Remote Installation Manager can be performed. ITDM-compatible distribution cannot be performed.

#5: RFB protocol must be used for remote control.

(2) Prerequisites for agentless management

When using agentless management, setup must be completed on both the management server and user computer to collect device information. The range of information that can be acquired depends on the authentication method. The range of information that can be acquired depends on the authentication method. A limited range of information may result in unknown security states and missing data in reports, causing risks to system operation. Select the best authentication method for your security needs.

Setup to collect most of the available device information is easy if you are using Active Directory to manage the computers in your organization. If you are thinking of using agentless management, first make sure that your computers are managed in Active Directory.

For differences between the types of device information that can be collected, see 2.6.2 Collecting device information.

Important note

Agentless management is not supported in a NAT environment.

Important note

Do not delete the discovery range or authentication information for any agentless managed device discovered in a network search. Likewise, do not delete the Active Directory setting for any agentless managed device discovered by an Active Directory search. Deleting this setting information prevents device information from being collected. If you mistakenly delete the discovery range, authentication information, or Active Directory setting, add them and then re-execute the network search or Active Directory search to discover the devices.

Important note

In a DHCP environment, if a device's IP address changes, moving outside the discovery range, no information will be collected about that device.

When using Windows administrative shares to perform agentless management

All the following conditions must be satisfied:

- Windows firewall is disabled on the user's computer#1.
- Simple file sharing is disabled on the user's computer.
- File and Printer Sharing is enabled on the user's computer.
- Windows Administrative Share (ADMIN$) is enabled on the user's computer.
- Access to the Interprocess Communications share (IPC$) is enabled on the user's computer.
- The information used for logging in to the target computer by using Windows administrative shares is set on the management server as authentication information for network searches.#2

#1: Even if Windows Firewall is enabled, the condition is still satisfied if TCP (port 445) is open for traffic.

#2: The authentication information for logging in to the target computer by using Windows administrative shares must satisfy either of the following conditions:

- The built-in Administrator account and password of the user's computer is used.
- The UAC function is disabled on the user's computer.

How to enable Windows administrative shares differs depending on the OS on the user's computer. The following settings are required to enable Windows administrative shares:

OS	Setting
Windows 8.1	• Disable UAC or enable the Administrator account.#1 • Enable **File and Printer Sharing** in the Network and Sharing Center window.
Windows 8	
Windows 7	
Windows Vista	• Disable UAC or enable the Administrator account. • Enable **File sharing** in the Network and Sharing Center window.

OS	Setting
Windows XP#2	• Disable simple file sharing. • Add file shares.
Windows Server 2012	Enable **File sharing** or **File and Printer Sharing** in the Network and Sharing Center window.
Windows Server 2008	
Windows Server 2003	Setup unnecessary (enabled by default).
Windows 2000	Add file shares.
Computer other than Windows	Not supported (cannot be configured).
Network device	Not supported (cannot be configured).

#1: If you are using Windows 8.1 or Windows 8 (no edition), perform this setup by executing the `net user` command at the command prompt. You cannot enable the Administrator account from the Windows Control Panel.

#2: In Windows XP Home Edition (Service Pack 2 and 3), Windows administrative shares cannot be used.

If these conditions are satisfied, you can acquire most of the available device information. The information collected hardly differs from that collected via agents installed on the managed computers.

When using SNMP to perform agentless management

The following conditions must be satisfied:

- SNMP can be used.
- The community name can be authenticated.

The following table describes the setup required to acquire device information using SNMP:

OS	Setting
Windows 8.1	• Install an SNMP agent. • Set up the SNMP agent.
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Computer other than Windows	
Network device	

When using Active Directory to perform agentless management

Both the following conditions must be satisfied:

- Windows firewall is disabled on the user's computer.#

- Using the Active Directory linkage feature, the management server can acquire device information managed by Active Directory.

#: If Windows firewall is enabled, the condition is still satisfied if connection via a port number specified in **Active Directory settings** view accessed from **General** view in the Settings module is open for traffic.

When using ICMP to perform agentless management

ICMP must be available for use.

The following table describes the setup required to acquire device information using ICMP:

OS	Setting
Windows 8.1	Allow incoming ICMP echo requests.#
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Computer other than Windows	
Network device	

#: In Windows XP or later, you must configure the Windows Firewall to allow ICMP traffic or disable Windows Firewall.

Related Topics:

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

(3) Configuring authentication information for agentless devices

In the case of agentless devices, information is acquired using a combination of the discovery range and authentication information set for network searches. The acquisition process uses the authentication information set for the discovery range that contains the devices' IP addresses.

The authentication information used for agentless devices can be also set after completion of a discovery.

To set authentication information for an agentless device:

1. Open the Device module.
2. Select a group under **Device Information** in the menu area.
3. Select an agentless device in the information area.
4. From the **Action** menu, select **Set Credentials**.
5. Set authentication information in the displayed dialog box.
6. Click the **OK** button.

The authentication information to be used for the selected agentless device is now set.

> **Tip**
>
> You can also set authentication information in the **IP Address Range** view accessed from **Configurations** in the Settings module.

(4) Acquiring information from agentless devices

The following methods are available for acquiring device information from agentless devices.

Administrative shares

Device information is acquired using authentication to Windows administrative shares. Almost the same level of information is collected as when using installed agents.

SNMP

Device information is acquired using SNMP authentication. Only a portion of the device information can be collected.

Active Directory

Device information is acquired with reference to the device information managed by Active Directory. Only a part of device information (that can be acquired by Active Directory) can be collected.

ARP

Device information is acquired from ARP. Only a portion of the available device information can be collected.

ICMP

Device presence is verified using ICMP (PING). Only IP address information can be collected.

Information is acquired from managed agentless devices using administrative shares or SNMP. ARP and ICMP are used only for devices on which administrative shares or SNMP authentication have failed. ARP and ICMP are never used for devices on which administrative shares or SNMP authentication have succeeded.

Whether acquisition is based on administrative shares or SNMP depends on the discovery range and authentication information set in the discovery settings. Information is collected from an agentless device using the authentication information set for the discovery range in which the device's IP address falls. No information is collected if the IP address is outside the discovery range, or if no authentication information has been set, or if authentication fails.

For agentless devices, the available collection methods differ according to the device type, as shown in the table below:

Collection method	Device type		
	Windows computer	OS other than Windows	Network device
Administrative shares	Y	N	N
SNMP	Y	Y	Y
Active Directory	Y	N	N
ARP	Y	Y	Y
ICMP	Y	Y	Y

Legend: Y: Can be used. N: Cannot be used.

Timing of device information acquisition

Device information is collected from agentless devices at the following times:

- When a network search is executed
- When you select **Update Device Details** from the **Action** menu in the Device list in the Device module.

To change the collection interval, set the update interval in the **Agentless Management** view under **Agent** in the Settings module. The default update interval is one hour.

By selecting **Update Device Details** in the **Device** module, you can collect device information at any time you wish.

Device information is not acquired during intensive discovery.

> **Important note**
>
> If Active Directory is used, the device information is collected when a search for a device registered in Active Directory is performed.

Related Topics:

- (5) Mechanism for acquiring device information from agentless devices
- (3) Configuring authentication information for agentless devices

(5) Mechanism for acquiring device information from agentless devices

To acquire device information from an agentless computer using authentication to administrative shares, executable programs are sent to the computer.

Three executable programs are sent:

- jpngmain.exe
- jpnmspushlauncher.exe
- jpnmspushservice.exe

These three executable programs generate administrative share files for reporting the collected device information on the computer. The files are then relayed to the management server and device information about the agentless computer is updated.

The executable programs are distributed only at the first run and when the executable programs are upgraded. They are not deleted automatically. If the management server is upgraded or if any of the executable program files are deleted, the executable programs are resent.

Important note

Never delete these executable programs. Deleting them might stop the agentless management functionality from working properly. Anti-virus products installed on a computer can result in an executable program being mistakenly detected as a virus and failing to execute correctly. In such cases, install a management agent

Tip

If login to a Windows administrative share is successful, approximately 2.5 MB of executable code is sent to each computer.

2.6.6 Linking with an MDM system

You can manage smart devices in JP1/IT Desktop Management 2 by linking with an MDM system and collecting information about the smart devices it manages. You can then manage the information in JP1/IT Desktop Management 2, and use the features of JP1/IT Desktop Management 2 to control smart devices.

The following table shows the features made possible by linking with an MDM system:

Feature	Description
Collecting information about smart devices	You can collect information about the smart devices managed by an MDM system, and use the information to manage those devices in JP1/IT Desktop Management 2. By collecting information periodically from the MDM system, you can manage the device information, asset information, and security status of individual smart devices.
Control smart devices	JP1/IT Desktop Management 2 can lock, wipe, and reset passcodes on smart devices managed by an MDM system.

Related Topics:

- (1) Collecting information for smart devices managed by an MDM system
- (2) Device information that can be acquired from MDM systems
- (3) Notes on MDM linkage
- 2.22 Controlling smart devices

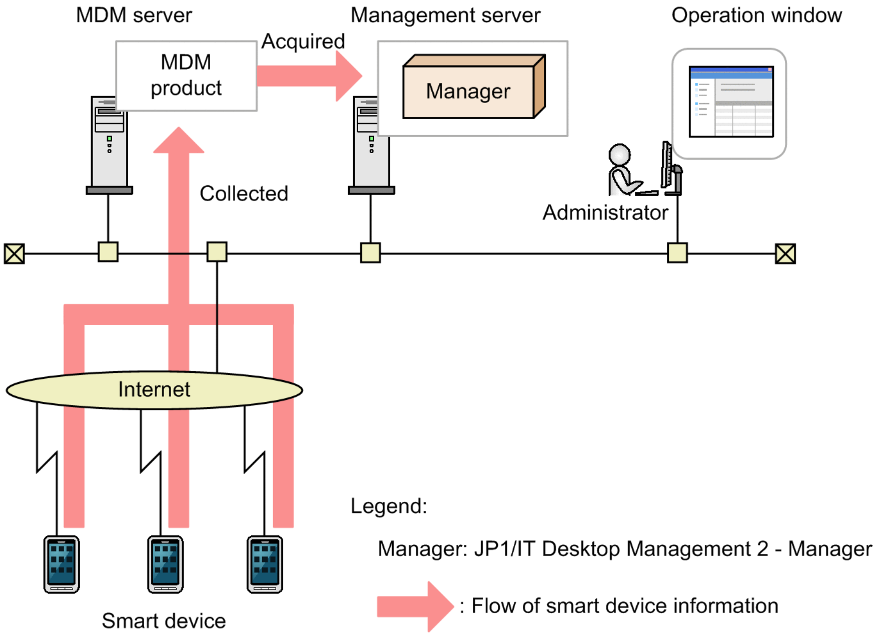
(1) Collecting information for smart devices managed by an MDM system

You can collect information about smart devices managed by an MDM system, allowing you to use the features of JP1/IT Desktop Management 2 to manage the device information, asset information, and security status of smart devices. You can keep the information up-to-date by collecting the latest information.

Tip

Like other devices, each smart device managed by JP1/IT Desktop Management 2 uses one product license.

The following figure shows how smart device information is collected from an MDM system.



You can use the following methods to collect information about smart devices managed by an MDM system:

Immediate

JP1/IT Desktop Management 2 connects to the MDM system immediately and collects information about smart devices. Use this option when you first install JP1/IT Desktop Management 2 or when you want changes to the information in the MDM system to be immediately reflected in the JP1/IT Desktop Management 2 database.

Scheduled

Smart device information is collected regularly according to the MDM linkage settings. Discovered devices are automatically made management targets. The schedule is determined by the values in **Start At**, **Repeat Interval** (daily, weekly, or monthly), and **Repeat** in the Settings module. By default, no schedule is set.

Tip

When you delete a smart device from an MDM system, the corresponding information is not deleted from JP1/IT Desktop Management 2. When you remove a smart device from an MDM system, you can remove the device from JP1/IT Desktop Management 2 by deleting its device information.

(2) Device information that can be acquired from MDM systems

The following table lists the device information you can obtain from an MDM system.

System information

Device information item		Can be acquired	MDM system item name on MobileIron	Contents
Device Type		Y	--	Smart Device is set as the device type.
Computer Details	Computer Name (Description)	Y	--	The user name, contract phone number, and model name used to identify the smart device in the MDM system.

Device information item		Can be acquired	MDM system item name on MobileIron	Contents
Computer Details	Host Name	Y	--	The user name, contract phone number, and model name used to identify the smart device in the MDM system.
	Model (Manufacturer)	Y	--	The name of the manufacturer of the smart device, and the model name assigned by the manufacturer.
	Serial #	Y	SerialNumber	The serial number of the smart device.
	Memory	Y	--	The total memory installed in the smart device.
System Drive	Total	Y	--	The total capacity of the hard disk.
OS Details	OS	Y	OS	The name and version of the operating system.
Network Details	MAC Address	Y	• WiFiMAC • wifi_mac_addr • BluetoothMAC	The MAC address of the device.
Smart device information	IMEI	Y	imei	The IMEI that identifies the smart device.
	UDID	Y	udid	The UDID assigned to Apple devices.
	IMSI	Y*	• imsi • registration_imsi • current_SIM_module_number	The IMSI assigned to the SIM card that the telecommunications company uses to identify the subscriber.
	ICCID	Y	--	The ICCID assigned to the SIM card of the smart device.
	Model (Manufacturer)	Y	--	The name of the manufacturer of the smart device, and the model name assigned by the manufacturer.
	Serial #	Y	SerialNumber	The serial number of the smart device.
	Contract phone number	Y	Number	The telephone number used by the smart device.
	E-mail	Y	--	The E-mail address used by the smart device.
	Carrier	Y	• current_operator_name • Operator	The communications provider of the smart device.
	Passcode setting	Y	PasscodePresent	Whether a passcode is set on the smart device.
	RAM (free)	Y	total_ram_size_bytes (free_ram_size_bytes)	RAM The total amount of RAM on the device. free The amount of free RAM on the device.
	Internal storage (free)	Y	total_storage_size_bytes	Internal storage The amount of internal storage on the device.

Device information item		Can be acquired	MDM system item name on MobileIron	Contents
Smart device information	Internal storage (free)	Y	(free_storage_size_bytes)	free The amount of free internal storage space.
	External storage (free)	Y*	total_media_card_size_bytes (free_media_card_size_bytes)	External storage The total capacity of the external storage connected to the device. free The amount of free external storage space.

Legend:

Y: Indicates device information that can be collected from any MDM system

Y*: Indicates device information that can be collected from MobileIron systems

--: Item names do not appear for these items regardless of whether device information is collected

You can also collect the information in the following table:

Device information item	Description
Management Type	MDM linkage management is set as the management type.
Device Status	Unknown is set if you collect smart device information from an MDM system, or re-register a wiped smart device. Warning is set if the smart device was successfully wiped.
Management Status	Agent not Installed is set.
Last Alive Confirmation Date/Time	The date and time when the smart device connected to the MDM system is set.

See the following for details about device information:

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

(3) Notes on MDM linkage

Note the following when linking with an MDM system:

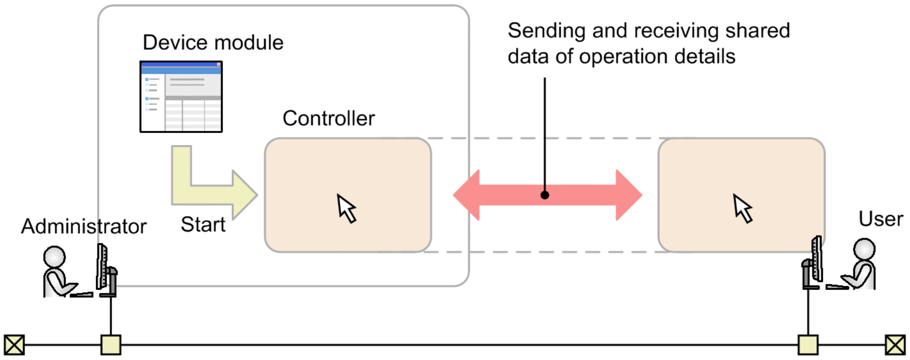
- You cannot use underscores (_) in the host name of an MDM server.
- The device information that can be collected by the MDM linkage function depends on the OS of the smart device and the MDM system from which the information is being collected. JP1/IT Desktop Management 2 only displays the items it was able to collect.

- If you swap the SIM card in a smart device, the IMEI stays the same but the contract phone number changes. As a result, a situation might arise in which the device information does not match the IMEI, causing the device to be recognized as a new smart device.

2.7 Controlling devices remotely

With the rapid advance in information technology in recent years, users who are not equipped to set up applications or troubleshoot problems are increasingly common. To handle their computer problems, organizations typically rely on a system administrator with specialist knowledge. If workplaces are dispersed, it becomes difficult to respond in a timely manner.

By using the remote control feature, an administrator can remotely operate a computer where a problem has occurred from his or her own computer, dealing with problems quicklythrough actions such as sharing operating procedures and sending and receiving data.



2.7.1 Process for remotely controlling devices

This section describes the workings of the remote control feature provided by JP1/IT Desktop Management 2.

The remote control feature allows an administrator to connect to a remote computer and control its GUI using keyboard and mouse operations.

The *controller* program must be installed on the computer you use to control a remote computer. You can install the controller program by starting the remote control feature from the JP1/IT Desktop Management 2 operation window. If the controller is not installed on the computer you are using, the program is automatically downloaded and installed.

> **Tip**
>
> You can then start the controller directly on the computer, allowing you to start a remote control session quickly without needing to log in to the operations window.

You initiate a remote control session by using the controller to connect to the remote computer. There are two ways the controller can connect to a remote computer:

Standard connection

A method of connecting to a computer using the remote control feature provided by JP1/IT Desktop Management 2. In this method, a remote control session is established between the controller and the remote control agent component of the agent. Due to its faster speeds and the fact that all remote control functions become available when a standard connection is used, we recommend that you use this method where possible. To use a standard connection, the agent program must be installed on the computer you are controlling.

RFB connection

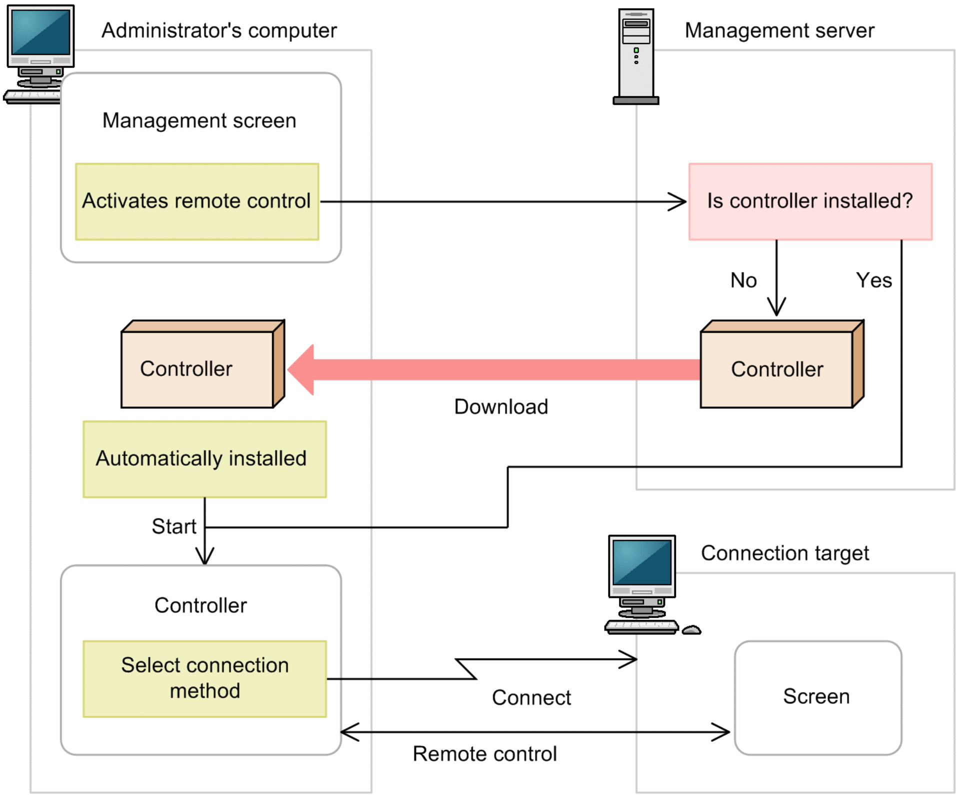
A method of connecting to a computer using the RFB protocol. In this method, a remote control session is established using AMT or VNC server software. Use this method to remotely control computers where you cannot log on to Windows, and agentless computers running Linux or Mac OS. Note that limited functionality is available in a remote control session that uses an RFB connection.

To use an RFB connection, the computer you are controlling must support connections using the RFB protocol.

You can select the connection method when connecting to the remote computer from the controller. If you do not select a connection method, a standard connection is used. If the controller cannot establish a standard connection, it will use an RFB connection.

When you select a connection-target computer in the operations window and start the remote control feature, the controller program starts and automatically connects to the computer. If you started the controller program directly, you can specify a connection target in the controller interface.

If the connection is successful, the user interface of the remote computer appears in the controller. You can then use the remote control function to operate the remote computer.



Related Topics:

- 4.3.3 Prerequisites for remote control
- 2.7.2 Remote control features
- 2.7.3 Functional differences between remote control connection methods

2.7.2 Remote control features

The remote control feature of JP1/IT Desktop Management 2 provides the following functionality:

- Remote control of computers

  You can control a remote computer as if you were seated in front of it. If an unforeseen problem occurs on a user's computer, an administrator can take action such as investigating the cause of the problem and restarting the computer, without having to travel to its location. For details about how to remotely control a computer, see 2.7.14 Controlling the interface of a computer during a remote control session.

- File transfers

  You can send and receive files to and from computers you are controlling remotely. Because you can browse the contents of the remote computer's hard disk in the same way as you browse a local disk in Explorer, you can easily find and transfer the files you need without setting up file sharing or installing special software. For details about how to transfer files, see 2.7.15 Transferring files during remote control sessions.

- Management of connection targets

  You can create a list of the computers that you connect to frequently, and manage the list separately from the JP1/IT Desktop Management 2 modules. You can also search the network for computers you can control remotely. For details about how to manage connection targets, see 2.7.17 Managing connection targets for the remote control feature.

- Sending a connection request to the controller

  If your network is configured in a way that prevents the controller from connecting to a computer directly, you can start a remote control session by having the user send a connection request to the controller from his or her computer. For details about how to send a connection request from a computer to a controller, see 2.7.16 Issuing connection requests from remote computers to controllers.

- Record and play back remote control sessions

  You can record the screen activity during a remote control session, and convert the recorded data to a video file to be used for user training or to give troubleshooting advice. For details about how to record and play back remote control sessions, see 2.7.18 Recording and playback of remote control sessions.

- Chat

  You can chat with several users at once. Use this feature when you want to issue instructions to multiple users, or communicate with users who you cannot contact by telephone. For details about how to use the chat feature, see 2.7.19 Using the chat feature.

Related Topics:

- 4.3.3 Prerequisites for remote control

2.7.3 Functional differences between remote control connection methods

There are some differences in remote control capabilities depending on the connection method and the computer environment. The following table describes functional differences by connection method:

Feature		Description	Available	
			Standard	RFB
Controller features	Connection to a remote computer	Lets you connect to a remote computer.	Y	Y
	Use of authentication information	Uses authentication information when connecting to a remote computer.	Y	Y
	Connection mode	Restricts the operations available to the users of the controller and the remote computer during a remote control session.	Y	Y*

Feature		Description	Available	
			Standard	RFB
Controller features	Connection status display	Displays the status of the connection to the remote computer.	Y	Y
	Remote desktop display	Reproduces the user interface of the remote computer in the controller program.	Y	Y
	Keyboard and mouse operations	Lets you use keyboard and mouse commands to interact with the remote computer.	Y	Y
	Clipboard	Synchronizes your clipboard contents with those of the remote computer.	Y	Y*
	Terminate remote control session	Disconnects from a remote computer and terminate the remote control session.	Y	Y
	Power control	Controls the power status of the remote computer.	Y	Y*
	Remote CD-ROM	Makes a CD/DVD drive on the controller (a drive with the device type `CD-ROM`) available to the remote computer.	Y*	Y*
	Recording, playback, and format conversion of remote control sessions	• Records the screen activity during a remote control session, and plays it back as a video file. • Converts video files to AVI files.	Y	Y
	Controller environment setup	Customizes the configuration of the controller.	Y	Y
Connection target management	Manage connection lists	Manages connection-destination computers independently of the JP1/IT Desktop Management 2 modules.	Y	Y
	Search for computers	Searches the network for potential connection targets.	Y	Y
	Receive connection requests from remote computers	Initiates a remote control session in response to a connection request received by the controller from a remote computer.	Y	N
Remote control agent	Confirm connection	Lets users choose to accept or reject connection requests from the controller.	Y	N
	Check connection mode	Checks which connection mode is being used.	Y	N
	Check connection status	Lets the user of the remote computer check the status of the connection with the controller.	Y	N
	Disconnect	Lets users disconnect from the controller.	Y	N
	Hide user interface	Hides or locks the screen of the remote computer during a remote control session.	Y	N
	Configure the remote control agent environment	Customizes the configuration of the remote control agent.	Y	N
File transfer	View file lists	Displays the hard drive contents of the controller and the remote computer.	Y	N

Feature		Description	Available	
			Standard	RFB
File transfer	Edit file properties	Lets you edit the properties of files on the controller and the remote computer.	Y	N
	Edit files	Lets you edit files on the controller and the remote computer.	Y	N
	Transfer files	Transfers files between the controller and the remote computer.	Y	N
	Customized transfer	Transfers files to several computers at once.	Y	N
	manage transfer information	Automatically downloads and caches files opened on a remote computer.	Y	N
Chat	Chat server	Initiates chat sessions in response to requests received from other computers.	Y	N
	Chat client	Allows you to connect to a chat server and participate in a chat session.	Y	N
	Chat log	Keeps a record of the contents of a chat session.	Y	N
	Print logs	Prints the contents of a chat log.	Y	N
	Initiate remote control session	Initiates a remote control session with a computer involved in a chat session.	Y	N
Operation window linkage	Controller installation	Automatically downloads and installs the controller program on computers without the controller installed.	Y	Y
	Automatic controller update	Automatically updates the controller program on computers with the controller installed.	Y	Y
	Launch and connect to a computer	Starts the controller program and connects to a computer you select in the operation window.	Y	Y
Link with other programs		Connects to a remote computer by calling the controller from another program using a command.	Y	Y
VNC server connection		Remotely controls a computer using software with VNC server functionality.	N	Y
BIOS configuration		Lets you display and configure the BIOS of a remote computer.	N	Y

Legend: Y: Available. Y*: Functionality is limited or depends on computer environment. N: Not available.

2.7.4 Notes on using the remote control feature in multi-language environments

If the controller and the remote computer use different keyboard types, key entry might not work as intended.

2.7.5 Notes on files generated by the controller in user environments

The following files associated with the controller program increase in number over time. We recommend that you delete the files before the disk space they occupy becomes an issue.

Temporary files used in file transfer

If you clear the **Delete local copy on the controller** check box on the **Files** tab of the **Environment Settings** dialog box displayed from the **File Transfer** window, the temporary files are not automatically removed from the controller system. The files remain in the storage folder for file transfers specified on the **Files** tab of the **Environment Settings** dialog box.

Video files

The files containing video recordings of remote control sessions are not deleted automatically. The files are created in a location chosen by the user, and their size depends on the length of the recording.

2.7.6 Automatically updating the controller program

When the controller program is updated as part of an JP1/IT Desktop Management 2 upgrade, the controller program is automatically replaced with the new version the next time you start a remote control session from the operation window.

Important note

In the following situations, the controller program is not automatically replaced:

- In an environment where you connect to JP1/IT Desktop Management 2 via a proxy server, the proxy server is configured incorrectly in the Internet Options
- Internet Explorer is in offline mode

2.7.7 Setting a connection mode for remote control sessions

You can limit the operations available during a remote control session by specifying a *connection mode*. This allows you to impose restrictions such as preventing users from using the remotely controlled computer during the remote control session, or limiting the administrator to viewing the user interface in the controller program.

There are three connection modes: *Exclusive*, *Shared*, and *View*. Each mode is described below.

Exclusive

In this mode, only the controller side can control the computer. The user cannot use his or her keyboard or mouse to control the computer. Use this mode if you want to prevent the user from using his or her computer while the controller side is controlling the computer. If you select *Exclusive* mode and then connect using RFB, the mode automatically goes into *Shared* mode.

Important note

You cannot use *Exclusive* mode over an RFB connection.

Shared

In this mode, the administrator using the controller program and the user of the remote computer are both able to control the computer. Connect using this mode when the administrator and the user might both need to operate the computer.

View

In this mode, you can view the screen of the remote computer, but not control it using keyboard or mouse operations. Connect using this mode when you just want to view the activity taking place on the remote computer.

Determining the connection mode

The connection mode is determined from the combination of controller settings and agent configurations. The following table shows combinations of the selected connection mode and the mode name displayed on the status window of the remote control agent.

Agent configuration	Setting in the controller		
	Exclusive	Shared	View
Exclusive	Pattern 1 Controller: *View* Agent: *Exclusive*	Pattern 2 Controller: *View* Agent: *Exclusive*	Pattern 2 Controller: *View* Agent: *Exclusive*
Shared	Pattern 3 Controller: *Exclusive* Agent: *View*	Pattern 1 Controller: *Shared* Agent: *Shared*	Pattern 2 Controller: *View* Agent: *Shared*
View	Pattern 3 Controller: *Exclusive* Agent: *View*	Pattern 3 Controller: *Shared* Agent: *View*	Pattern 1 Controller: *View* Agent: *View*

The following describes Patterns 1 through 3 in the table above.

Patterns 1 and 2

If both the agent and controller are set to the same remote control mode (Pattern 1) and when the agent has a higher-level mode (Pattern 2), the agent configuration takes precedence. Therefore, if the agent is set to *Exclusive* mode, the controller will go into *View* mode regardless of the controller's own setting. If the agent is set to *Shared* or *View* mode, the controller will use its own setting.

Pattern 3

If the controller has a higher-level mode (Pattern 3), the controller setting takes precedence. Therefore, if the controller is set to *Exclusive* mode, the agent will go into *View* mode regardless of the agent's own setting. If the controller is set to *Shared* mode, the agent will use its own setting.

(1) Changing the connection mode from a remotely controlled computer

A user cannot use his or her computer if it is being remotely controlled in exclusive mode.

If a need arises for the user to control the computer, he or she can change the connection mode to *shared* by pressing **Ctrl** + **Alt** + **Delete**.

When a user uses this method to change the connection mode from exclusive to shared, the controller is notified and displays a message asking whether the administrator wants to allow it. If the administrator does not permit the mode change, the computer reverts to exclusive mode and the user is unable to operate the computer again.

Tip

The connection mode changes to shared as soon as the user presses **Ctrl** + **Alt** + **Delete** on his or her computer. This means that by the time the message appears in the controller, the connection has already entered shared mode.

(2) Connection modes when using multiple remote control connections

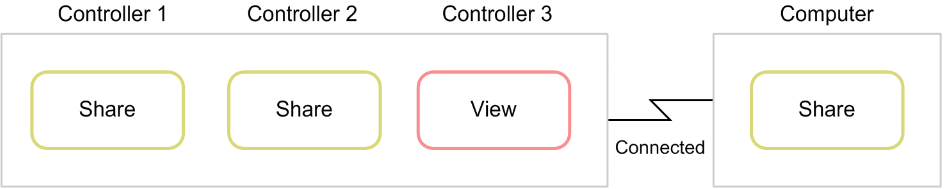
When several controllers connect to one computer, only one of those controllers can work in exclusive mode. All other controllers work in view mode.

If the controller working in exclusive mode changes to another mode or leaves the session, a message appears on the other controllers indicating that the session is no longer in exclusive mode.

The following figures show examples of how the connection mode changes when you use multiple remote control connections.

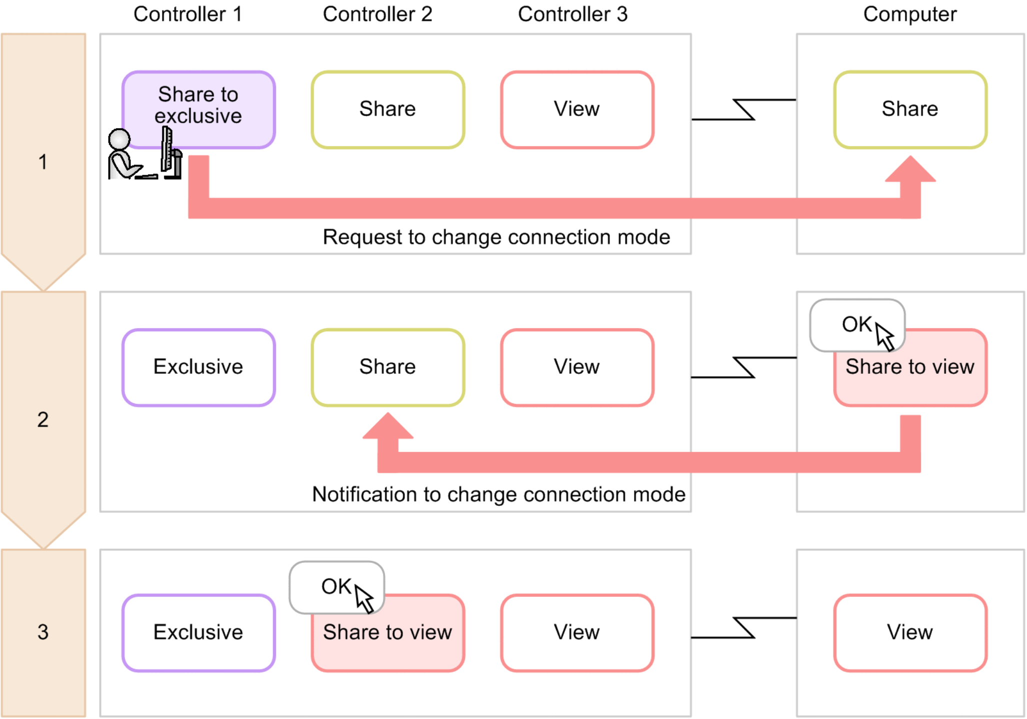
Example 1: Initial state

Suppose that three controllers connect to a single remote computer using the connection modes illustrated below.



Example 2: Controller 1 changes to exclusive mode

When controller 1 changes to exclusive mode from its initial state, the connection modes of the other controllers change as shown below.



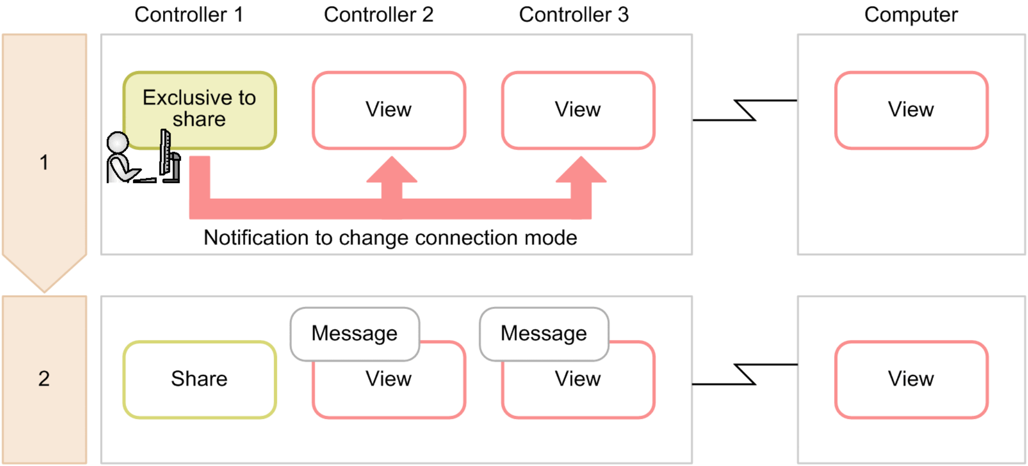
1. Controller 1 changes to exclusive mode.
   A message reporting the change appears on the remote computer.

2. The user clicks **OK** on the remote computer.
   The remote computer enters view mode. A message indicating that another controller has entered exclusive mode appears on controller 2.

3. The administrator clicks **OK** in controller 2.
   Controller 2 enters view mode.

Example 3: Controller 1 changes to another mode from exclusive mode

From the state in example 2, if controller 1 changes to another mode from exclusive mode, the other controllers do not change mode. The result is the same if controller 1 disconnects from the remote computer.

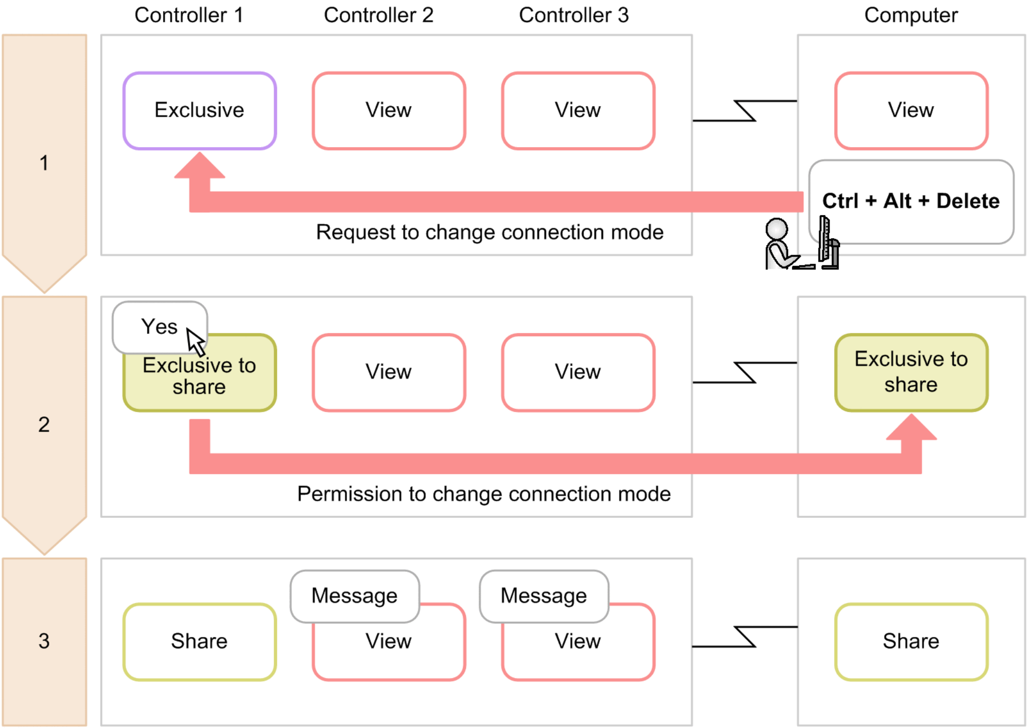


1. Controller 1 changes to shared mode.

2. A message appears in controller 2 and controller 3 indicating that controller 1 is no longer in exclusive mode. However, controller 2 remains in view mode.

Example 4: The user presses Ctrl + Alt + Delete on the remote computer after controller 1 has entered exclusive mode.

In the state in example 2, if the user of the remote computer presses **Ctrl** + **Alt** + **Delete**, the connection modes of the other controllers change as follows:



1. The user presses **Ctrl** + **Alt** + **Delete** on the remote computer.
   A message requesting confirmation of the change of connection mode appears in controller 1.
2. The administrator clicks **Yes** in controller 1.
   Controller 1 and the remote computer enter shared mode. If the user clicks **No** instead, the mode does not change.
3. In controller 2 and 3, a message appears indicating that the other controller is no longer in exclusive mode. Controller 2 and 3 remain in view mode.

2.7.8 Displaying the connection status of remote control sessions

When you connect to a remote computer, information about the remote control session appears in the status bar of the controller program. This information is described in the following table.

Item	Description	Shown by default
Bytes sent	The number of bytes sent. You can change the display format or reset the number from the pop-up menu displayed when you right-click the item.	N
Bytes received	The number of bytes received. You can change the display format or reset the number from the pop-up menu displayed when you right-click the item.	N
Time elapsed	The length of time since the connection to the remote computer was established. You can reset the time from the pop-up menu displayed when you right-click the item.	N
Remote CD-ROM status	The status of the remote CD-ROM (or DVD-ROM). You can permit or deny remote access to the CD-ROM (or DVD-ROM) drive from the pop-up menu displayed when you right-click the item.	Y#
Recording status	An icon showing whether the remote control session is being recorded. You can start, stop, and pause a recording from the pop-up menu displayed when you right-click the icon.	N

Item	Description	Shown by default
Transmission status	Shows how much data was sent and received and the encryption status. You can reset the numbers from the pop-up menu displayed when you right-click the item.	A
Protocol	Shows the protocol (HRC or RFB) used for the connection.	A
Connection mode	Shows the connection mode of the controller. You can change the connection mode from the pop-up menu displayed when you right-click the item.	Y

Legend: Y: Displayed by default. A: Displayed while a connection is active. N: Not displayed.

#: Always displayed when using an RFB connection.

You can show or hide the following items by selecting the **Status bar** command in the **View** menu of the **Remote Control** window:

- Elapsed time
- Bytes sent and received

2.7.9 Using the remote control feature in NAT and DHCP environments

In NAT environments

NAT is a process of translating network addresses to mask a private address space from the public network. There are two types of address translation: Fixed address allocation (static mode) and dynamic address allocation (dynamic mode).

Note the following when using the remote control feature in a NAT environment:

When using fixed address allocation (static mode)

No restrictions apply to use of the remote control feature.

When using dynamic address allocation (dynamic mode)

You cannot connect to a computer from the controller. You can initiate a remote control session by having the user send a connection request from the computer to the controller.

In DHCP environments

DHCP is a network protocol that automatically allocates IP addresses to computers as they connect to the network. Because computers in a DHCP environment have a different IP address each time they connect to the network, you cannot connect to a computer from the controller. You can initiate a remote control session by sending a connection request from the computer to the controller.

Note that if you use static DHCP, computers retain the same IP address, allowing you to connect to computers directly from the controller.

Related Topics:

- 2.7.16 Issuing connection requests from remote computers to controllers

2.7.10 User permissions required for remote control using Windows authentication

If you enable Windows authentication in the authentication information settings of the remote control agent, you must have the appropriate user permissions to access the remote computer over the network. User permission settings are a Windows feature. The following table shows the user permissions required for each OS situation.

Operating system usage	Required permission
Local computer	Administrators permission or other appropriate privileges. If the computer belongs to a domain, you must have Domain Admins group permission.
A workstation or server that belongs to a domain	Active Directory Domain Admins group, Enterprise Admins group, or other appropriate privileges.
Domain controller or workstation with the Windows Server 2003 Administrative Tools Pack installed	
Domain controller	

Note: For added security, consider logging on as a non-administrator user and elevating your account to administrator privileges when setting security information.

2.7.11 Setting user permissions required for remote control using Windows autpagehentication

This section describes how to set the user permissions for each OS situation.

To set user permissions on a local computer:

1. In the **Control Panel**, select **Administrative Tools**.
2. Double-click **Local Security Policy**.
3. In the console tree, click **Security Settings**.
4. Under **Local Policies**, select **User Rights Assignment**.
5. In the right pane, double-click **Access this computer from the network** or **Deny access to this computer from the network**.

Set the user permissions in the dialog box that appears.

To set user permissions on a workstation or server in a domain:

1. In the Windows **Start** menu, select **Run**.
2. Enter `mmc` and click **OK**.
3. From the **File** menu of the Console, select **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Group Policy Object Editor** and then click **Add**.
5. In the **Select Group Policy Object** dialog box, click **Browse**.
6. Select the group policy object that you want to change.

7. In the console tree, under **Group Policy Object**, select *computer-name* **Policy**, **Computer Configuration**, **Windows Settings**, and then **Security Settings**.
8. Under **Local Policies**, select **User Rights Assignment**.
9. In the right pane, double-click **Access this computer from the network** or **Deny access to this computer from the network**.

Set the user permissions in the dialog box that appears. If there is no security setting defined for the policy, select the **Define this policy setting** check box.

To set user permissions on a domain controller or workstation with the Windows Server 2003 Administrative Tools Pack installed:

1. From the Windows **Start** menu, open the **Control Panel** and select **Administrative Tools**.
2. Double-click **Active Directory Users and Computers**.
3. In the console tree, double-click the group policy object whose security settings you want to edit.
4. Click **Properties** and display the **Group Policy** tab.
5. To edit an existing group policy object, select **Edit**.
   To create a new group policy object, click **New** and then **Edit**.
6. In the console tree, under **Group Policy Object**, select *computer-name* **Policy**, **Computer Configuration**, **Windows Settings**, and then **Security Settings**.
7. Under **Local Policies**, select **User Rights Assignment**.
8. In the right pane, double-click **Access this computer from the network** or **Deny access to this computer from the network**.

Set the user permissions in the dialog box that appears. If there is no security setting defined for the policy, select the **Define this policy setting** check box.

To set user permissions on a domain controller:

1. From the Windows **Start** menu, open the **Control Panel** and select **Administrative Tools**.
2. Double-click **Domain Controller Security Policy**.
3. In the console tree, under **Group Policy Object**, select *computer-name* **Policy**, **Computer Configuration**, **Windows Settings**, and then **Security Settings**.
4. Under **Local Policies**, select **User Rights Assignment**.
5. In the right pane, double-click **Access this computer from the network** or **Deny access to this computer from the network**.

Set the user permissions in the dialog box. If there is no security setting defined for the policy, select the **Define this policy setting** check box.

2.7.12 Setting authentication information for remote control

You can set user-level authentication information for connections made from controllers to computers with the agent installed. Set authentication information when you want to permit specific administrators to participate in remote control sessions. If you do not set any authentication information, connections are permitted from all administrators.

There are two types of user authentication you can use when setting authentication information:

Standard authentication

User authentication provided by JP1/IT Desktop Management 2. Only an administrator with the user name and password set in the authentication information can connect to a remote computer.

Windows authentication

User authentication implemented by linking with Windows authentication. Only the Windows users and groups set in the authentication information can connect to a remote computer. This approach allows you to apply detailed security policies that define password expiry dates, auditing, and other security measures.

You can register and manage authentication information for multiple administrators. You can then assign shared mode or exclusive mode to specific administrators, or limit the operations the administrator is able to perform in a remote control session. For example, you might want to prevent an administrator from shutting down a remote computer. You can further enhance the security of remote control sessions by linking user authentication with Windows authentication.

You can define authentication information in the agent configurations.

2.7.13 Connecting from a controller to a remote computer

If you start the controller program directly or the connection to a remote computer is lost, you need to specify the connection destination in the controller to connect to the remote computer. You can specify a connection destination by:

- Directly specifying a host name or IP address
- Selecting a computer from a list
- Connecting to a computer listed in the connection log
- Searching for a connection-target computer

If authentication information is set on the remote computer, a dialog box asking for your credentials appears when you attempt to establish a connection, regardless of the method you use. Enter the authentication information set in the **User Authentication** area under **Remote Control Settings** in the agent configurations, or the authentication information set on the connection-target VNC server. In the default agent configuration, the user ID is `system` and the password is `manager`.

If the remote control feature is configured to display connection requests on the remote computer, and the user rejects the request, a message reporting this fact appears in the controller.

Tip

A maximum of 255 controllers can connect to a single remote computer.

Tip

If access to the remote computer is denied or the connection times out, the system attempts to connect again using RFB. Note that if the controller is configured to turn on a remote computer, and the RFB reconnection fails (times out) because the computer is turned off, the remote control feature uses Wake on LAN and AMT to start the remote computer before attempting to connect again.

Related Topics:

- 2.7.17 Managing connection targets for the remote control feature

2.7.14 Controlling the interface of a computer during a remote control session

When using the remote control feature to operate a remote computer, the controller can perform the following operations on the computer it controls:

Keyboard and mouse operations

You can use keyboard and mouse operations, such as entering text and dragging icons, to control the user interface of the remote computer as you do on your own PC. You can also use shortcuts like **Ctrl** + **C** by registering them as special keys.

Use of CD-ROM and DVD-ROM drives

You can make the controller's CD and DVD drives (drives with the drive type CD-ROM) available on the remote computer. This allows you to install software without having to transfer the data first.

Shutdown and restart

From the controller, you can direct a remote computer to shut down or restart. If you configure the controller to reconnect after the remote computer restarts, it will automatically reconnect allowing you to continue the remote control session.

Clipboard sharing

You can send and receive clipboard data between the controller and the remote computer. This allows you to copy and paste text and bitmap data between the controller, and the computer being controlled.

Tip

The controller can control computers in a multi-display environment.

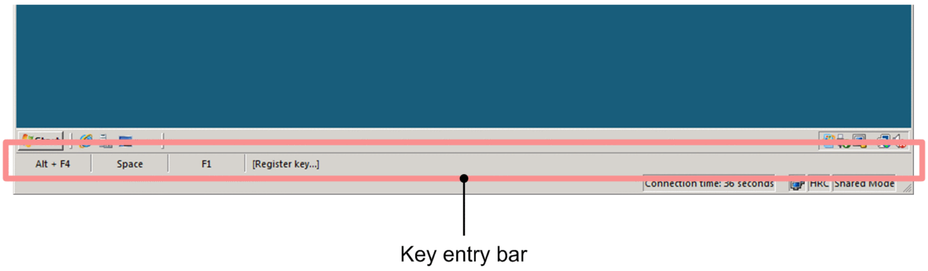
Related Topics:

- (1) Registering and entering special keys for use in remote control sessions
- (3) Transferring clipboard data during remote control sessions

(1) Registering and entering special keys for use in remote control sessions

When you use your keyboard to enter special keys like function keys and keyboard shortcuts, those keystrokes apply to the controller itself. To use special keys on the remote computer, you need to register them in the controller first.

The special keys you register appear in the key input bar of the **Remote Control** window. By clicking the buttons in the key input bar, you can enter the associated special key in the remote computer.



Tip

If the controller computer and the remote computer have different input environments (for example, the controller system uses an English-language keyboard while the remote system uses a Japanese layout), you might not be able to enter certain characters using your keyboard. In this case, you can enter such characters without needing to be conscious of the different input environments by using special keys or transferring the data using the clipboard.

Related Topics:

- (2) Default special keys registered in the controller
- (3) Transferring clipboard data during remote control sessions

(2) Default special keys registered in the controller

The following table lists the special keys provided by default in the controller program. You can add a default special key by selecting the **Default** option under **Action key type** when you register a special key.

No.	Special keys
1	**F1**
2	**Shift** + **F1**
3	**Shift** + **F10**
4	**SpaceBar**
5	**Esc**
6	**Alt**
7	**Alt** + **Tab**
8	**Alt** + **Esc**
9	**Alt** + **SpaceBar**
10	**Alt** + **-**
11	**Alt** + **Enter**
12	**Alt** + **F4**
13	**Alt** + **F6**
14	**Alt** + **PrintScreen**

No.	Special keys
15	**PrintScreen**
16	**Ctrl** + **C**
17	**Ctrl** + **O**
18	**Ctrl** + **P**
19	**Ctrl** + **S**
20	**Ctrl** + **V**
21	**Ctrl** + **X**
22	**Ctrl** + **Z**
23	**Ctrl** + **Esc**
24	**Ctrl** + **F6**
25	**Ctrl** + **Tab**
26	**Kanji**

(3) Transferring clipboard data during remote control sessions

You can configure the remote control feature to automatically transfer clipboard data from the controller to the remote computer, or vice versa, each time the clipboard contents change. This ensures that the clipboard contents are always the same on both computers, which means you can work seamlessly between them when performing operations like the following:

- Displaying a Web site in a Web browser on the remote computer by pasting a URL recorded on the controller PC
- Paste screenshots or other data collected on the remote computer into documents being created on the controller computer

There are some differences in the types of data that can be transferred depending on the connection type.

For standard connections:

You can transfer the following types of data or any combination thereof:

- Text
- Bitmaps
- Metafiles
- Rich text
- Color palettes

For RFB connections:

You can send and receive ASCII text only. The ability to send and receive non-ASCII text depends on the environment of the remote computer.

Clipboard data is transferred when the controller window becomes active. If you are using an RFB connection, data is transferred when the clipboard contents are updated on the remote computer.

Tip

When using a standard connection, to prevent the system from slowing down when a large amount of data is copied to the clipboard, you can configure the remote control feature to only transfer text on the **Optimize Transaction** tab of the **Environment Settings** dialog box.

Tip

While clipboard data is being transferred, the system displays a message and progress bar in the status bar at the bottom of the **Remote Control** window. If you start transferring an unexpectedly large file that appears to be taking too long to transfer, you can cancel the transmission by right-clicking the progress bar and selecting **Cancel**. The data being transferred is discarded, and the clipboard reverts to its previous contents.

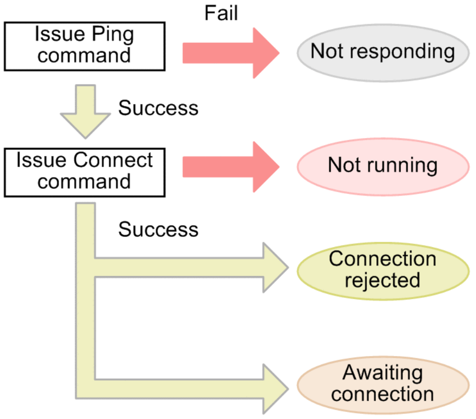
(4) Setting search ranges for connection-target computers

There are five ways to set the search range for connection-target computers, as described in the table below.

No.	Method	Example	Actual search range
1	Specify a single IP address.	172.17.11.10	172.17.11.10
2	Enter the first three bytes of the IP address. As the last byte, enter two numbers joined by a hyphen (-). Use this format to search within a group of consecutive IP addresses.	172.17.11.10-20	172.17.11.10 to 172.17.11.20
3	Enter the first three bytes of the IP address. As the last byte, enter several numbers separated by commas (,). Use this format to search within a group of non-consecutive IP addresses.	172.17.11.10,11,100,200	172.17.11.10,172.17.11.11,172.17.11.100,172.17.11.200
4	Use a combination of methods 2 and 3.	172.17.11.10,50-100,200	172.17.11.10, 172.17.11.50 to 172.17.11.100, and 172.17.11.200
5	Specify the first three bytes of the IP address. Use this format to search among all the IP addresses within a given subnet.	172.17.11	172.17.11.0 to 172.17.11.255

(5) Status of connection-target computers

Computers in the **Search Agents** dialog box can be in Awaiting connection, Connection rejected, Not running, or Not responding status. The figure below shows how a computer transitions between these statuses.



Not responding

The computer does not exist or is turned off.

Not running

The computer cannot be controlled remotely, or the remote control agent is not running on the computer.

Connection rejected

The remote control agent is running on the computer (with the agent installed), but a connection cannot be established. Possible causes include the agent not being registered as a permitted controller, and the port used by the remote control feature being used by another application. Check the message on the **Details** tab of the **Search Agents** dialog box.

Awaiting connection

The computer is ready to accept connections.

(6) Operating the menu bar during a full-screen remote control session

In full screen mode, you can use the menu bar to, for example, define the remote control settings, view how much data has been sent and received, and change the display settings.

The following table shows the icons in the menu bar and describes their function.

Icon	Name	Description
📌	Pin icon	Click this icon to keep the menu bar displayed at all times. After you click the pin button, the menu bar remains on screen regardless of where the mouse pointer is located. This feature is disabled by default.
C A D	Ctrl + Alt + Delete button	Clicking this icon has the same effect as pressing **Ctrl** + **Alt** + **Delete** on the remote computer.
⟳	Refresh button	Click this button to refresh the contents of the controller window. You can use this button to correct glitches in the display, for example.
🖧	Send/Receive icon	This icon shows whether data is being sent to and received from the remote computer, and whether the data is encrypted. Encryption is indicated by a key icon. You can reset the values from the pop-up menu that appears when you right-click the icon.
—	Minimize button	Click this icon to minimize the controller window. The desktop of the computer running the controller appears.
🗗	Restore button	Click this icon to exit full-screen mode.
✕	Close button	Click this icon to end the remote control session and close the window.

(7) Notes on using the remote control feature

This section provides cautionary notes that apply to the remote control feature. It also provides cautionary notes that apply when the remote computer is using a specific operating system.

- If a remote computer displays an MS-DOS prompt in full-screen mode, the controller cannot display the computer's screen. When using the remote control feature, always use the MS-DOS prompt in a window.
- The controller might be unable to display graphics generated on the remote computer using Direct X (Direct Draw) or OpenGL.
- Animation generally takes a large amount of data to send. Do not display animation on the remote computer while a remote control session is in progress.
- When the controller attempts to reconnect to a remote computer that did not recognize the controller's disconnection, the **Duplicate connection** dialog box appears. In this case, select the disconnect option in the dialog box and then reconnect to the remote computer.
- Use a color palette with at least 256 colors.
- If the **Enable pointer shadow** check box is selected on the **Pointers** tab of the **Mouse Properties** dialog box in the **Control Panel**, the cursor appears as a double image in the controller, and its shape might be inconsistent between the remote computer and the controller. To resolve this problem, use one of the following methods:
    - On the remote computer, in the **Control Panel**, select **Mouse**, select the **Pointers** tab, and clear the **Enable pointer shadow** check box.
    - In the **Properties** dialog box of the **Remote Control** window, click the **Optimize Transaction** tab and select the **Do not show the window animation, etc.** check box.
- The connection mode changes to shared mode if one of the following occurs while the remote computer is in view mode:
    - The user presses **Ctrl** + **Alt** + **Delete** on the remote computer
    - A hardware error or system error message is displayed or closed
    - A message from the Windows Messenger service is displayed or closed
- Applications that simulate keyboard entry or change key assignments will not work correctly while the remote computer is in view mode.
- Note the following before hiding the screen of a remote computer you are controlling in exclusive mode. We recommend that you thoroughly check operation in a test environment before using this feature.
    - The graphics card and monitor of the remote computer must support power saving mode.
    - The CPU usage might reach 100% on the remote computer, or a residual image might appear on the screen every few seconds.
    - The blackout of the remote computer's screen might be forcibly lifted. the following table describes when this can happen.

Cause	Description
Disconnection	• The administrator disconnects from the remote computer or ends the remote control session. • The user disconnects from the controller or ends the remote control session. • The remote control session was terminated due to a communication error.
Leaving exclusive mode	• The user presses **Ctrl** + **Alt** + **Delete** on the remote computer. • A hardware error or system error message is displayed or closed on the remote computer.

Cause	Description
Leaving exclusive mode	• A message from the Windows Messenger service is displayed or closed on the remote computer.

Notes on connections to remote computers running Windows 8.1, Windows 8, and Windows Server 2012

- Do not disable the following applications in the **Startup** tab of the System Configuration. If you disable these applications, some remote control features will not work correctly.
  - jdngrcagent.exe
  - jdngrcchat.exe
- Pointer trails do not appear in the controller when you select the **Display pointer trails** check box in the **Visibility** area of the **Pointer Options** tab, displayed by opening the **Control Panel** and selecting **Hardware and Sound**, **Devices and Printers**, and then **Mouse**.
- If you hide the screen of a remote computer you are controlling in exclusive mode, you cannot send the **Ctrl** + **Alt** + **Delete** key combination from the controller to the remote computer.
- If no mouse is connected to a remote computer with the agent installed, the mouse pointer will always be shaped as an arrow in the controller.

Notes on connections to remote computers running Windows 7, Windows Server 2008, or Windows Vista

- During remote control sessions, Windows Aero features such as window transparency, taskbar thumbnails, and Windows Flip 3D are disabled.
- When you use a Windows Aero mouse pointer, performance of remote mouse control drops. To prevent this, change the mouse pointer design to None. To change the mouse pointer design:
  1. In the Windows **Control Panel**, click **Mouse**.
  2. In the **Mouse Properties** dialog box, display the **Pointers** tab.
  3. In the **Scheme** list box, select (**None**).
  4. Click **OK**.

Notes on connections to remote computers running Windows 8.1, Windows 8, Windows 7, and Windows Vista

- If any of the following operations take place on the remote computer during a remote control session, the session is ended.
  - The user logs off
  - The user is switched
  - A remote connection is established using the Remote Desktop feature

Notes on connections to remote computers running Windows Server 2012 and Windows Server 2008

- If any of the following operations take place on the remote computer during a remote control session, the session is ended.
  - The user logs off
  - The user is switched
  - A console connection is established using the Remote Desktop feature

Notes on connections to remote computers running Windows Server 2003

- The remote control feature does not support console connections established by the Remote Desktop feature of Windows Server 2003. If a console connection is established by Remote Desktop, subsequent connection attempts from the controller will be rejected. If the controller is already connected, it will be disconnected.

  To connect again, unlock Windows Server 2003 on the remote computer.

Notes on connections to remote computers running Windows XP

- The remote control feature does not support the User Switching feature or Remote Desktop feature of Windows XP.

  If the remote computer uses user switching or remote connection by the Remote Desktop feature in Windows XP, subsequent connection attempts from the controller will be rejected. If the controller is already connected, it will be disconnected.

  To re-establish the connection, take the following action:

  - If the connection was rejected due to user switching:

    Log off all users from Windows XP, and log on again as the first user.

  - If the connection was rejected due to the Remote Desktop feature:

    Unlock Windows on the remote computer.

> **Important note**
>
> You cannot use the remote control feature with a computer running Windows 7 in Windows XP Mode.

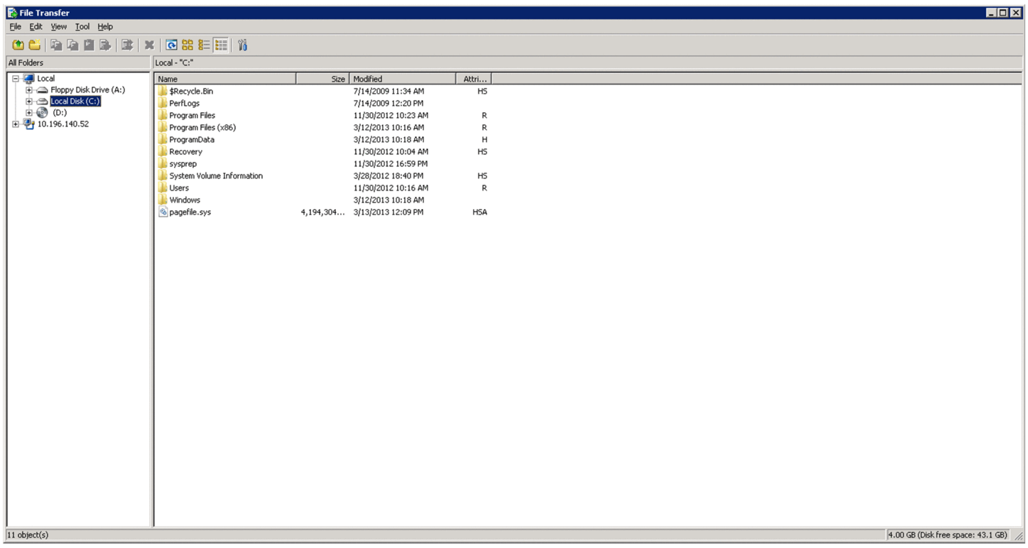
2.7.15 Transferring files during remote control sessions

You can send and receive files to and from the controller and the remote computer during remote control sessions.

Practical uses include copying files that require maintenance from the remote computer to be worked on locally by the administrator, and transferring troubleshooting tools to run on the remote computer.

> **Important note**
>
> You cannot transfer files when using a RFB connection to the remote computer. To transfer files, **Allow File Transfer** must be selected in the **Remote Control Settings** in the agent configurations assigned to the remote computer.

Use the **File Transfer** window opened from the controller to transfer files.



Name	Size	Modified	Attri...
$Recycle.Bin		7/14/2009 11:34 AM	HS
PerfLogs		7/14/2009 12:20 PM	
Program Files		11/30/2012 10:23 AM	R
Program Files (x86)		3/12/2013 10:16 AM	R
ProgramData		3/12/2013 10:18 AM	H
Recovery		11/30/2012 10:04 AM	HS
sysprep		11/30/2012 16:59 PM	
System Volume Information		3/28/2012 18:40 PM	HS
Users		11/30/2012 10:16 AM	R
Windows		3/12/2013 10:18 AM	
pagefile.sys	4,194,304...	3/13/2013 12:09 PM	HSA

11 object(s)

4.00 GB (Disk free space: 43.1 GB)

In the **File Transfer** window, you can view and work with files in a similar manner to Windows Explorer, including the use of simple drag and drop operations. You can also transfer files to multiple destinations in one operation.

Tip

You can transfer files by dragging them onto the screen of the remote computer displayed in the controller. In this case, the **File Transfer** window appears and file transfer begins immediately. The transferred data is saved to the desktop of the remote computer.

Important note

In Windows 8.1 or Windows Server 2012 R2, you cannot transfer files in an environment with OneDrive.

(1) Viewing the file transfer status and canceling file transfer during remote control sessions

When file transfer starts, a **File Transfer Progress** dialog box appears on the controller and the remote computer (the dialog box is minimized on the remote computer).

To cancel file transfer, click **Cancel** in the **File Transfer Progress** dialog box. The **Cancel** button is available on the controller and on the remote computer. If the button is clicked in the controller, a confirmation dialog box appears asking whether the transfer should be canceled. If the button is clicked on the remote computer, file transfer is canceled immediately.

When you cancel file transfer, files that have already been transferred remain at the destination. If you are moving rather than copying files, files that have already been transferred are deleted from the source computer.

When you transfer files within the same remote computer or from one remote computer to another, files are transferred indirectly via a temporary folder on the controller. In this scenario, the **File Transfer Progress** dialog box appears twice, once when the files are being transferred from the remote computer to the temporary folder, and again when the files are being transferred from the temporary folder to the remote computer.

(2) Notes on file transfers during remote control sessions

Note the following when using the file transfer feature:

- You cannot perform file transfer in the following situations:
  - The controller is not connected to a remote computer in the **Remote Control** window
  - The controller is connected in view mode
  - The user has not logged on to the remote computer
- You cannot transfer files to or from a remote computer that is not configured to allow file transfer. However, if the option to prohibit file transfer is enabled on the remote computer while the **File Transfer** window is open, you will be able to continue to transfer files until the remote control session is terminated.
- When transferring files over a low-speed connection, you can reduce the likelihood of a memory shortage causing a failed transfer by refraining from remote control operations in the **Remote Control** window during the transfer.
- If a network error occurs during file transfer, the system does not always detect that the connection has been lost, and attempts to re-establish the file transfer connection might fail. In this case, you can use the remote control feature or other means to cancel the file transfer in the **File Transfer Progress** dialog box on the remote computer.

2.7.16 Issuing connection requests from remote computers to controllers

A controller cannot initiate a connection to a remote computer in NAT or NAPT environment where the remote computer is invisible to the administrator's computer. In DHCP environments where IP addresses are assigned dynamically, there is a significant amount of work involved in finding out the IP address you need to specify in the controller.

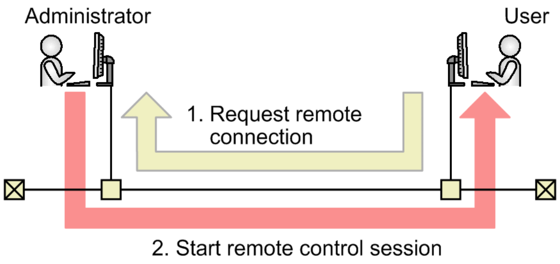
In this type of environment, because the end user's computer does not have this issue when connecting to the administrator's computer, you can initiate a remote control session by having the user send a connection request to the controller.

Important note

Only online-managed computers can send connection requests to a controller.

Having the user send a connection request saves the administrator the trouble of entering a connection destination. This helps avoid situations in which the connection fails because the administrator enters the wrong IP address, and prevents unauthorized controllers from remotely controlling the computer.

The following figure shows the process of starting a remote control session in response to a connection request from a user.



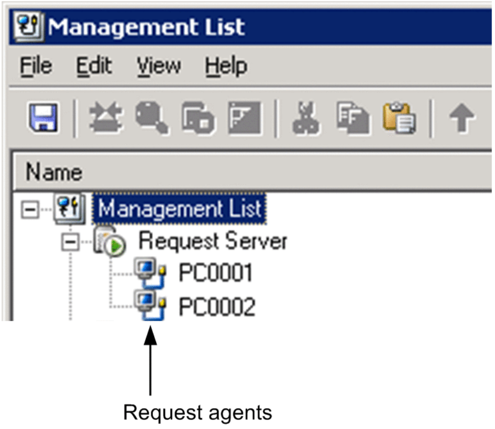
A request server must be present in the connection list in order to receive connection requests from remote computers. After starting the request server, if a request for a remote connection is received from a user (step 1 in the figure), an icon representing the user's computer appears in the connection list. You can then initiate a remote control session by double-clicking the icon (step 2 in the figure).

Related Topics:

- (1) Receiving requests from request agents

(1) Receiving requests from request agents

When the request server receives a connection request, the computer that issued the connection request appears below the request server. This computer is referred to as a `request agent`. The following figure shows an example of a connection list that contains request agents.



By double-clicking the icon for a request agent, the administrator can connect to the remote computer and begin a remote control session.

You can reject a connection request by deleting the request agent or closing the connection list.

When a request server stops, the request agent icon automatically disappears from the connection list. The icon is active as long as the connection request is in effect. It becomes inactive when the connection request is declined.

Important note

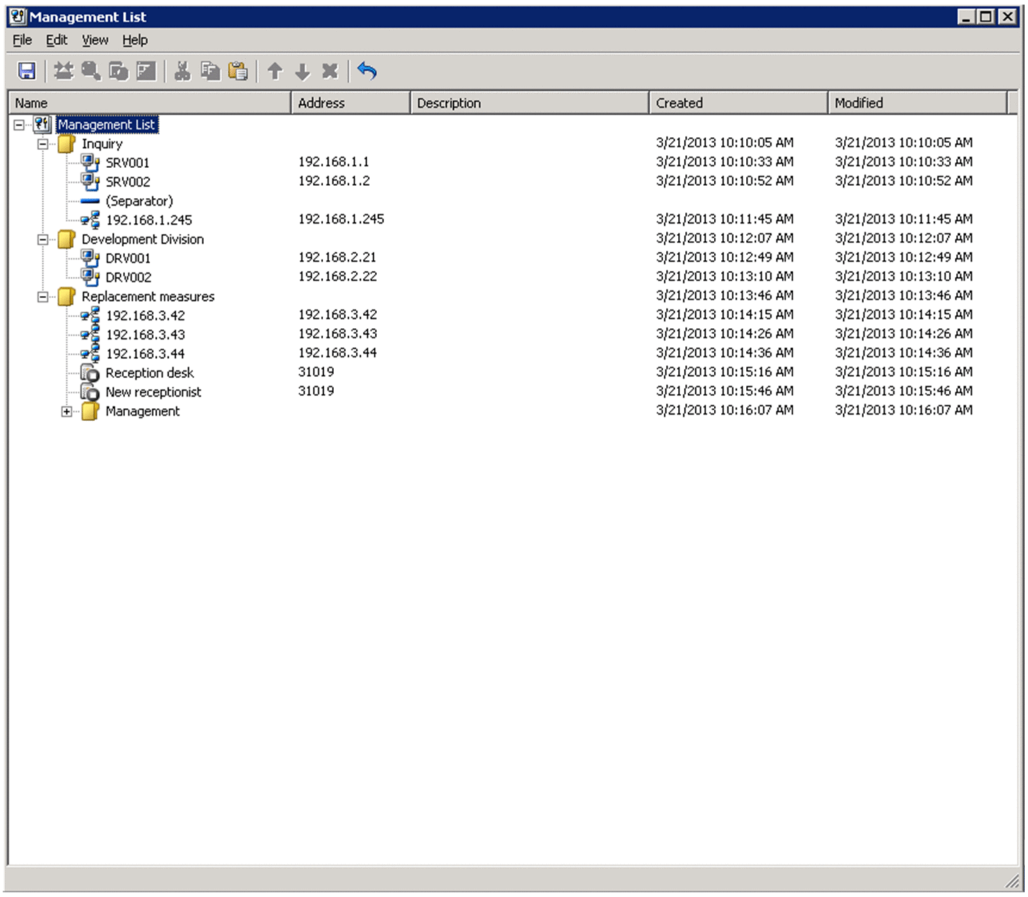
A request agent icon is a temporary representation of an agent that has issued a connection request. It is not retained after the connection list has closed. To save the information for an agent that issued a connection request, drag the icon to a group of your choice. After you move the icon to another folder, you can save the icon as an item in the agent list. You can then treat the agent as an ordinary computer and change its name and description.

2.7.17 Managing connection targets for the remote control feature

You can manage connection targets for the remote control feature independently of the JP1/IT Desktop Management 2 modules.

By registering remote computers, you can select connection targets directly from the controller, saving you the trouble of searching for connection destinations in the operation window. You can also create groups that let you organize connection destinations in a hierarchy.

Connection destinations are managed in a connection list.



Name	Address	Description	Created	Modified
Management List				
Inquiry			3/21/2013 10:10:05 AM	3/21/2013 10:10:05 AM
SRV001	192.168.1.1		3/21/2013 10:10:33 AM	3/21/2013 10:10:33 AM
SRV002	192.168.1.2		3/21/2013 10:10:52 AM	3/21/2013 10:10:52 AM
(Separator)				
192.168.1.245	192.168.1.245		3/21/2013 10:11:45 AM	3/21/2013 10:11:45 AM
Development Division			3/21/2013 10:12:07 AM	3/21/2013 10:12:07 AM
DRV001	192.168.2.21		3/21/2013 10:12:49 AM	3/21/2013 10:12:49 AM
DRV002	192.168.2.22		3/21/2013 10:13:10 AM	3/21/2013 10:13:10 AM
Replacement measures			3/21/2013 10:13:46 AM	3/21/2013 10:13:46 AM
192.168.3.42	192.168.3.42		3/21/2013 10:14:15 AM	3/21/2013 10:14:15 AM
192.168.3.43	192.168.3.43		3/21/2013 10:14:26 AM	3/21/2013 10:14:26 AM
192.168.3.44	192.168.3.44		3/21/2013 10:14:36 AM	3/21/2013 10:14:36 AM
Reception desk	31019		3/21/2013 10:15:16 AM	3/21/2013 10:15:16 AM
New receptionist	31019		3/21/2013 10:15:46 AM	3/21/2013 10:15:46 AM
Management			3/21/2013 10:16:07 AM	3/21/2013 10:16:07 AM

From the connection list, you can search for computers on the network and add remotely controllable computers to the connection list.

(1) Configuring the remote control environment

The remote control feature might be used in diverse environments where computers are distributed across several LANs, or several interconnected WANs and LANs. In these environments, the connection parameters (the environment settings related to the remote control connection) differ between computers, and you need to set the appropriate connection parameters in the controller each time you connect to a remote computer.

You can save time and effort by setting the appropriate connection parameters for individual computers. This allows you to use the correct settings when connecting to remote computers without having to change them each time you connect to a different computer. You can also assign connection parameters when you create items such as computers in the connection list.

> **Tip**
>
> The connection parameters you can assign to individual computers are the same as those set in the **Advanced** and **Connection** tabs of the **Environment Settings** dialog box for the controller. If there are no connection parameters set for a computer, the options set for the controller apply to the connection.

Inheritance of connection parameters

Connection parameters for a computer are inherited as follows:

- If you move or copy an agent, the connection options are retained by the moved agent and inherited by the copy of the agent.
- If you create a group, a computer, or a network below a group, the connection parameters for the upper-level group are inherited by the group, computer, or network.

(2) Remote control connection log

When you connect to a remote computer with a connection method specified, or you connect to a remote computer from the connection list, the path of the computer appears in the connection log in the **Remote Control Agent Specification** area of the **Remote Control** window. Paths are displayed in one of three formats:

hrc://computer-name

A computer for which a standard connection was specified in the connection parameters.

rfb://computer-name

A computer for which an RFB connection was specified in the connection parameters.

list://group-name/computer-name

A computer to which a connection was established from the connection list.

In each path, computer-name is replaced by the IP address or host name of the remote computer, and group-name is replaced by the group configuration of the connection list. If the groups in the connection list are configured in a hierarchy, the names of the groups at each level in the hierarchy are shown.

Example: The path of PC0001 registered in the group /Development Department/3rd Division is displayed as follows:

list:///Development Department/3rd Division/PC0001

2.7.18 Recording and playback of remote control sessions

You can record screen activity at a remotely controlled computer and save the recording as a video file. You can then play back the recorded file on a controller.

Recorded files can also be converted to AVI format and played back on video player software such as Windows Media Player. You can use video recordings in this way to give troubleshooting advice or program operating instructions to a user, even if no controllers are installed in the environment.

Recordings of computer screen activity can be used in the following ways:

Troubleshooting

Some level of proficiency is needed for users to handle computer problems on their own. Understanding what to do is easier if the administrator can describe procedures using a video recording. Problems can be resolved more efficiently without any need for written instructions.

Training

Program operating instructions and work procedures can be recorded and used as training materials. For example, a complicated operation that is difficult to describe in a manual can be more easily conveyed in a video clip.

(1) Viewing the recording status of a remote control sessions

You can check the recording status of a remote control session by displaying the recording status icon in the status bar.

To display the recording status icon, navigate to the **Logging** tab of the **Options** dialog box which opens from the **Remote Control** window. The recording status icon appears only during remote control sessions.

The following icons show the recording status of a remote computer desktop:

- 🔴 : Recording
- ⏸ : Paused
- ⚪ : Stopped

> **Tip**
>
> You can start or stop a recording from the pop-up menu that appears when you right-click the displayed icon.

(2) Settings for efficient video recording of remote control sessions

Selecting a destination file each time you start recording screen activity is an inefficient way of working. You can save time by setting the destination file and file name in advance. You can also set an option to begin recording as soon as you connect to the remote computer.

To set up recording, click the **Options** button in the tool bar of the **Remote Control** window. Then go to the **Logging** tab of the displayed dialog box.

Setting recording files

When you specify a recording file on the **Logging** tab, all recordings will be automatically saved to that file, which means that the specified file will be overwritten at each recording or you will need to set up a new file each time you record screen activity. However, if you need to manage multiple files of individual recordings, you can set the recording file name using variables. When recording begins, the recording will be saved under the file name with the variables replaced by values. Three different variables can be used in file names:

- $(Agent)
  Represents the computer name. The value set in this variable is the destination specified on the controller (IP address, host name, or alias).
- $(Date)
  Represents the date. The date on which the recording started is set in *MM-YYYY-DD* format (*MM*: month; *YYYY*: year; *DD*: day).
- $(Time)
  Represents the time. The time at which the recording started is set in *hhmmss* format where *hh* is in 24-hour clock notation (*hh*: hour; *mm*: minute; *ss*: second).

You specify a file name incorporating these variables, or you can select one of three file name templates supplied by default.

Some examples of file names that incorporate variables are given below. The computer name in these examples is 10.xxx.xxx.4, the date is April 1, 2011, and the time is 15:05:45. To set file names like these, select a template in the **Select Recording File** dialog box which opens from the **Logging** tab.

Selecting a supplied template

From the **File type** list, select one of the following file name templates:

- Recording file (name.jcr)
  Example: 10.xxx.xxx.4.jcr
- Recording file (name date time.jcr)

Example: 10.xxx.xxx.4 2011-04-01 150545.jcr

- Recording file (date time name.jcr)
  Example: 2011-04-01 150545 10.xxx.xxx.4.jcr

Specifying a file name that includes variables

In the **File name** box, type the file name using variables.

- $(Agent) $(Date).jcr
  Example: 10.xxx.xxx.4 2011-04-01.jcr
- UserName (*nnn*)_ $(Date).jcr
  Example: *nnn*_2011-04-01.jcr

Setting to begin recording at remote connection

To start recording as soon as you connect to the remote computer, select the **Start recording when connected** check box.

(3) Remote control operations at the user side

The remote control agent is part of an agent program that allows remote control on the user computer. Usually no operations are required on the remotely controlled side, but if necessary the user can deny connection or check remote connection status. The remote control agent can issue connection requests to controllers as well as waiting for connections from controllers.

From **Remote Control Settings** in the **Agent Configurations** view, you can set up the remote control agent to start automatically. The remote control agent will then start automatically whenever any computer on which it is installed is started.

If automatic startup is not specified, you will need to ask the user to start the remote control agent manually. To start the remote control agent manually, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Remote Control Agent**, and then **Remote Control Agent**.

When Remote Control Agent starts, the **Remote Control Agent** icon ( ) appears in the task bar.

If you did set up the agent configuration for status icon display, the **Remote Control Agent** icon and status window will not appear when the remote control agent is active.

Tip

The **Remote Control Agent** icon ( ) indicates that no controllers are connected. When a controller connects with the remote computer, the icon changes according to the connection mode.

Tip

The **Remote Control Agent** icon does not appear in the task bar in Windows 7 or Windows Server 2008 R2. If you want to display the icon, from the Control Panel select **Customizing the desktop** and then **Customizing the taskbar icon**. Set **Show icon and notifications** for the **Remote Control Agent** icon.

(4) Checking controller connection status

You can check the following information from the status window or from the **Remote Control Agent** icon that appears when the remote control agent starts:

- Whether any controllers are connected
- How many controllers are connected
- The Agent connection mode

Remote Control Agent icon displays

The **Remote Control Agent** icon is color-coded as follows to indicate controller connection status:

- Gray: Not connected
- Orange: Connected in view mode
- Yellow: Connected in shared mode
- Green: Connected in exclusive mode

When you position the mouse pointer on the **Remote Control Agent** icon, the number of connected controllers appears.

Display in the status window

The color of the title bar of the status window shows controller connection status. The color coding is the same as for the **Remote Control Agent** icon. The connection status, connection mode, and number of connected controllers are shown in the title bar.

The number in parentheses in the title bar is the number of connected controllers.

2.7.19 Using the chat feature

While engaged in a remote control session over a standard connection, you can use the chat feature to communicate with users who you cannot contact by telephone. Because the chat feature uses text data, it is also a useful way to provide IP addresses, URLs, and other text-based information in real time.

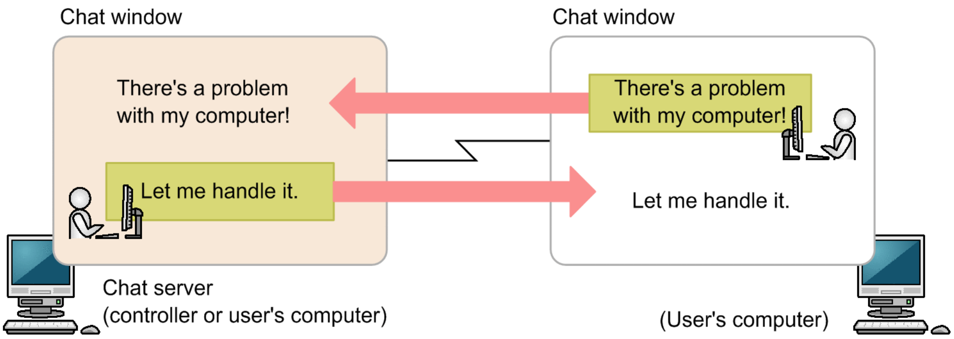
You can also chat with several users at once.

One use for the chat feature is as a training tool. Because all trainees can be given the same instructions, you can save time by reducing the need to give the same explanation over and over. When trainees raise questions, you can send answers to specific users, or to all users if appropriate.

Important note

You cannot use chat over a RFB connection.

The following figure shows an overview of the chat feature:


Chat window
There's a problem with my computer!
Let me handle it.
Chat server
(controller or user's computer)
Chat window
There's a problem with my computer!
Let me handle it.
(User's computer)

The chat server must be running before you can initiate a chat session. After you start the chat server, a chat session begins when a computer connects to the chat server from the **Chat** window. A user can also connect to several chat servers from the **Chat** window.

During a chat session, you can send the messages entered in the **Chat** window to other computers. You can send messages to all computers taking part in the chat session, or to individual computers.

(1) Using the chat server icon

When the chat server starts, the **chat server** icon ( ) appears in the taskbar.

You can perform the following operations from the **chat server** icon:

- View users connected to the chat server
  You can view a list of users who are connected to the chat server. This operation (and the corresponding menu item) is unavailable if there are no users connected to the chat server.
- Disconnect chat users
  You can disconnect users from the chat server. You can disconnect all users, or select specific users to disconnect.
- Set parameters
  You can set the port number, password, and other parameters of the chat server.

Tip

The chat server icon does not appear in the taskbar in Windows 7 and Windows Server 2008 R2. If you want to display the icon, from the Control Panel select **Customizing the desktop** and then **Customizing the taskbar icon**. Set **Show icon and notifications** for the **chat server** icon.

2.7.20 Remote control menus

(1) Menus in the Remote Control window

Menu heading	Menu item	Description
File	Connect	Connects to a remote computer. If you are already connected to a computer, the connection is established in a new **Remote Control** window.
	Reconnect	Reconnects to the last connected computer.

Menu heading	Menu item		Description
File	Disconnect		Disconnects from the selected computer.
	Search		Searches for computers on the network.
	Save Screen		Saves an image of the current screen.
	Record Screen	Start	Starts recording the on-screen activity of the remote control session.
		Pause	Pauses recording of the on-screen activity of the remote control session.
		Restart	Resumes the paused recording.
		Stop	Stops recording the on-screen activity of the remote control session.
	Play Screen	Play	Plays back a remote control session.
		Convert	Converts a recording of on-screen activity to an AVI file.
	Terminate		Closes the controller program.
	Terminate All		Closes all open controller programs.
View	Toolbar	Toolbar	Shows or hides the toolbar.
		Button Text Labels	Shows or hides the text-based description of the tool buttons.
	Status Bar	Status Bar	Shows or hides the status bar.
		Elapsed Time	Shows or hides the time that has elapsed since the connection with the computer was established.
		Transfer data	Shows the amount of data transferred to and from the computer.
	Key input bar	Action key	Shows registered special keys at the bottom of the Remote Control window.
		Register key	Registers a special key.
	Refresh		refreshes the screen contents.
	Screen Color	Gray Scale	Displays the on-screen activity in grayscale.
		256-Color Decrease	Reduces the color palette to 256 colors.
		65,536-Color Decrease	Reduces the color palette to 65,536 colors.
		65,536-Color Decrease + JPEG Compression	Reduces the color palette to 65,536, and compresses the image data.
		No Color Decrease	Shows on-screen information in a full color palette.
	Zoom	Cancel	Returns the screen to its original size.
		Auto-zoom	Automatically zooms the on-screen information in and out to fit the **Remote Control** window.
	Full Screen		Displays the remote control session in full screen mode.
Tools	Properties		Lets you set the operating environment for the controller.
	Mode	View	Sets the connection mode to *view*.
		Shared	Sets the connection mode to *shared*.
		Exclusive	Sets the connection mode to *exclusive*.
	Shut Down		Shuts down the remote computer.

Menu heading	Menu item	Description
Tools	Reboot	Restarts the remote computer.
	Send Ctrl+Alt+Del	Sends the **Ctrl** + **Alt** + **Delete** command to the remote computer.
	Mount CD/DVD	Makes the CD or DVD drives on the administrator's computer available to the remote computer as a remote CD-ROM drive.
	Unmount CD/DVD	Makes the remote CD-ROM unavailable.
	Enable IDER Boot	Allows the remote computer to boot from the remote CD-ROM drive.
	Transfer File	Displays the **File Transfer** window.
	Chat	Displays the **Chat** window.
Agent Manager	Add to List	Adds the currently connected computer to the connection list.
	Change List	Displays the connection list.
Window	Arrange Vertically	Arranges multiple **Remote Control** windows vertically.
	Arrange Horizontally	Arranges multiple **Remote Control** windows horizontally.
	Arrange All	Arranges multiple **Remote Control** windows in a uniform tile pattern.
	Minimize All	Minimizes all **Remote Control** windows to icons.
	Remote Control	Brings the selected **Remote Control** window to the front.
Help	Contents	Displays the online help.
	Version	Displays version information.

Menu items displayed from the Connect button

Menu item	Description
Connect	Connects to a computer. You can also search for connection-target computers.
Add to List	Adds the currently connected computer to the connection list.
Change List	Displays the connection list.

(2) Menus in the File Transfer window

Menu bar	Menu item		Description
File	Open		Opens the selected file or folder.
	New	Folder	Creates a new folder.
	Delete		Deletes the selected file or folder.
	Rename		Renames the selected file or folder.
	Properties		Changes the attributes of the selected file or folder.
	Disconnect		Terminates the file transfer connection.
	End		Closes the **File Transfer** window.
Edit	Register for Copying		Registers a file to be copied.
	Register for Moving		Registers a file to be moved.
	Transfer Files		Starts file transfer.

Menu bar	Menu item		Description
Edit	Select All		Selects all items in the selected drive or folder.
	Switch		Inverts the selection.
	View	File List	Shows information about files registered for copying or moving.
		Selected File	Shows information about the selected file.
	Customize		Transfers files to the same folder on multiple computers.
View	Toolbar		Shows the toolbar.
	Status bar		Shows the status bar.
	Large Icons		Displays files and folders using icons.
	List		Displays files and folders in a list.
	Details		Shows detailed information (name, size, date modified, attributes) for files and folders.
	Parent Folder		Displays the contents of the parent folder of the current folder.
	Refresh		Updates the information in the **File Transfer** window.
	Download Manager		Displays the **Download Manager** window.
Tools	Transfer Options		Allows you to set options related to the appearance and functionality of the **File Transfer** window.
Help	Contents		Displays the online help.
	Version		Shows version information.

(3) Menus in the File Transfer window of the Download Manager

Menu bar	Menu item	Description
File	Delete	Deletes a file saved in the controller.
	Close Automatically	Specifies whether the **File Transfer** window automatically closes when all the files are deleted from the window.
	Close	Closes the **File Transfer** window of Download Manager.
Edit	Transfer Files	Copies files back to their original location on the remote computer.
	Delete After Transfer	Moves files back to their original location on the remote computer.
	Select All	Selects all the files in the list.
	Switch	Inverts the selection.
View	Refresh	Updates the information in the window.
Help	Contents	Displays the online help.
	Version	Shows version information.

(4) Menus in the Agent Manager window

Menu bar	Menu item		Description
File	New	Group	Creates a new group.

Menu bar	Menu item		Description
File	New	Agent	Creates a new remote computer.
		Network	Creates a network in which you can define a search range for connection-target computers.
		Request server	Creates a new request server.
		Separator	Inserts a separator.
	Import From...	System File	Creates a connection list from the contents of a backup file.
		Hosts File	Creates a connection list from the contents of a hosts file.
	Connect		Connects to the selected computer. This menu item is unavailable when a network or request server is selected.
	Search		Searches for computers in the selected network.
	Start		Starts the selected request server.
	Stop		Stops the selected request server.
	Delete		Deletes the selected item.
	Rename		Renames a group, computer, or request server.
	Properties		Lets you view or change the properties of a group, computer, or request server.
	Save		Saves the current configuration information to the default backup file.
	Save As		Saves the current configuration information under a new name.
	Close		Closes the connection list.
Edit	Undo		Reverses the last deletion, movement, or modification of data.
	Cut		Cuts the selected item.
	Copy		Copies the selected item.
	Paste		Pastes a cut or copied item to the connection list.
	Select All		Selects all items in a folder.
	Switch		Inverts the selection.
	Shift Up		Moves the selected item up one position in the list.
	Shift Down		Moves the selected item down one position in the list.
	Find		Lets you specify a keyword to search for in the connection list.
	Find Next		Searches for the next occurrence of the keyword in the connection list.
View	Toolbar		Shows the toolbar.
	Status bar		Shows the status bar.
	Word Wrap		Wraps selected items to fit the window.
	Separate	Lines	Displays a separator after each line. You can simultaneously display row separators.
		Rows	Displays a separator after each row. You can simultaneously display line separators.

Menu bar	Menu item	Description
View	Highlight Selected Line	Highlights the address, description, and creation date/time of the selected item.
	Adjust Column Position	Changes the column position so that the address, description, and creation date/time are accommodated within the window.
Help	Contents	Displays the online help.
	Version	Shows version information.

(5) Menus in the Remote Control Player window

Menu bar	Menu item		Description
File	New		Starts a new instance of the remote control player.
	Open		Lets you select a recording to play back.
	Properties		If a file is open, information about the recording is displayed.
	Exit		Closes the remote control player.
Play	Play		Starts playing a file that was paused or stopped.
	Pause		Pauses playback.
	Stop		Stops playback.
	Fast forward		Fast forwards through the recording.
	Slow		Plays the recording in slow motion.
View	Toolbar		Shows or hides the toolbar.
	Status bar		Shows or hides the status bar.
	Seek bar		Shows or hides the seek bar.
	Zoom	Automatically	Automatically zooms the player window in and out to fit the remote control player window.
		50%	Reduces the size of the player window to 50% of its original size.
		100%	Displays the player window at its original size (100%).
		200%	Enlarges the player window to 200% of its original size.
	Full Screen		Displays the view in full screen in the controller.
Window	Arrange Vertically		Arranges the remote control player windows vertically.
	Arrange Horizontally		Arranges the remote control player windows horizontally.
	Arrange All		Arranges multiple remote control player windows in a uniform tile pattern.
	Minimize All		Minimizes all remote control player windows to icons.
	Fit to Frame		Resizes the playback window to fit the remote control player.
Help	Contents		Displays the online help.
	Version		Shows version information.

(6) Menus in the Chat window

Menu bar	Menu items		Description
File	Connect		Connects to the chat server. If you are already connected to a chat server, you can use this item to connect to another chat server.
	Disconnect		Disconnects from the connected chat server.
	Properties		Displays detailed information about the selected user.
	Send Message		Sends the chat message entered in the message input box.
	Send Beep		Sounds a single beep on the computers of the other users participating in the chat session.
	Save		Overwrites the save file with the transcript of the current chat session.
	Save As		Saves the transcript of the current chat session to a new file.
	Print		Prints the transcript of the current chat session.
	Print Preview		Displays a print preview of the transcript of the current chat session.
	Exit		Closes the **Chat** window. The connection with the chat server is automatically disconnected.
View	Toolbar		Shows or hides the toolbar.
	Status Bar		Shows or hides the status bar.
Tools	Options		Lets you set the operating environment for the **Chat** window.
	Chat Server	Start Chat Server	Toggles the chat server on and off. A tick appears beside this item when the chat server is on.
		Hide When Minimized	Causes the Chat window to disappear from the taskbar when minimized. A tick appears beside this item if enabled.
		Start When Windows Starts	Registers or removes the chat server in the Windows startup group. A tick appears beside this item when the chat server is registered in startup.
	Remote Control		Initiates a remote control session by connecting to the selected user. This item is unavailable if the **Chat** window was opened on an agent.
Help	Contents		Displays the online help.
	Version		Shows version information.

(7) Menus during remote control sessions (full screen mode)

When you use the remote control feature in full screen mode, you can display menus by right-clicking the menu bar. From these menus, you can change the screen color depth, connection mode, and other settings.

To close the menu, click **Cancel** in the menu.

The following table lists the items that appear in the menus.

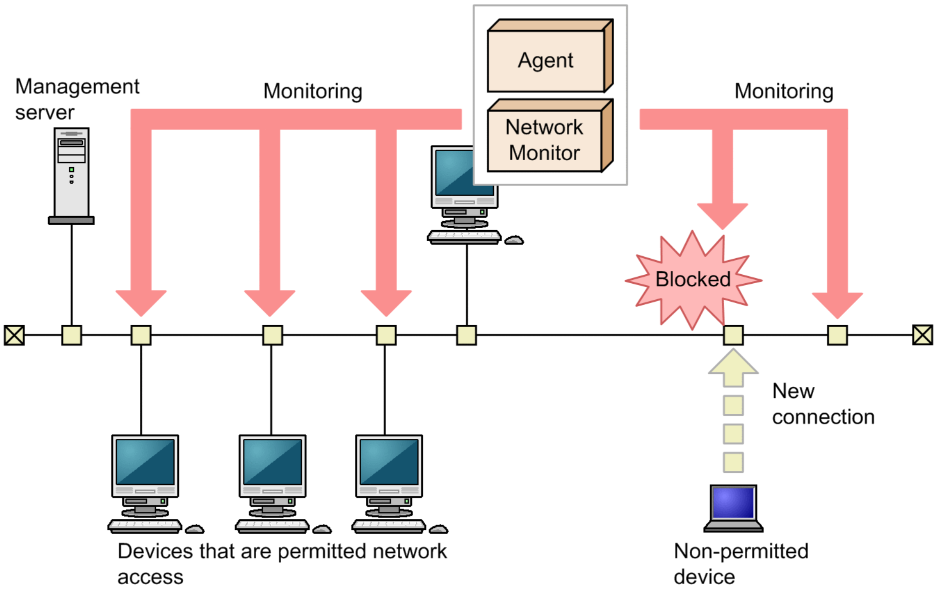
Item			Description
View	Menu bar	Display Automatically	Select this option to automatically display the menu bar when you move the mouse cursor to the top of the window.
		Display at All Times	Select this option to keep the menu bar displayed at all times regardless of where the mouse pointer is located.

Item			Description
View	Refresh		Refreshes the information in the remote control window.
	Screen Color	Gray Scale	Reduces the color palette to 8-color grayscale.
		256-Color Decrease	Reduces the color palette to 256 colors.
		65,536-Color Decrease	Reduces the color palette to 65,536 colors.
		65,536-Color Decrease + JPEG Compression	Reduces the color palette to 65,536, and applies JPEG compression to screens that display a high number of colors.
		No Color Decrease	Shows on-screen information in a full color palette.
	Minimize		Minimizes the remote control window.
	Restore		Exits full screen mode and displays the remote control session in a window.
Tool	Mode	View	Changes the connection mode to view.
		Shared	Changes the connection mode to shared.
		Exclusive	Changes the connection mode to exclusive.
	Send Ctrl + Alt + Del key		Sends the **Ctrl** + **Alt** + **Delete** command to the remote computer.
Cancel			Closes the pop-up menu.
Exit			Terminates the remote control session and closes the window.

2.8 Managing network connections

With the proliferation of wireless LANs and mobile devices, there is a risk of employees or outsiders bringing their personal devices onto company premises and connecting to your company network. Unsecured devices are a potential source of virus infections and a way to remove data without authorization. To avoid these and other issues, you need to have a clear picture of the devices that connect to your network, and manage them proactively.

By using the network monitor feature, you can protect your corporate network by blocking unauthorized devices. You can also use this feature to detect, in real time, attempts by unknown devices to connect to the network.



Legend:

Agent: A computer with the agent installed

Network Monitor: A network monitor agent

Note that you cannot block the network connection of a management server, a relay system, or a computer with the network monitor agent installed.

2.8.1 Detecting devices by using the network monitoring function

You can detect a new device attempting to access the network by enabling the network monitor for the network segment groups displayed in the Network List view. To display the Network List view, in the Device module, select **Device Inventory** and then **Network List**. A network search is automatically performed for the detected device. If the device is discovered, its access to the network is controlled according to the network monitor settings.

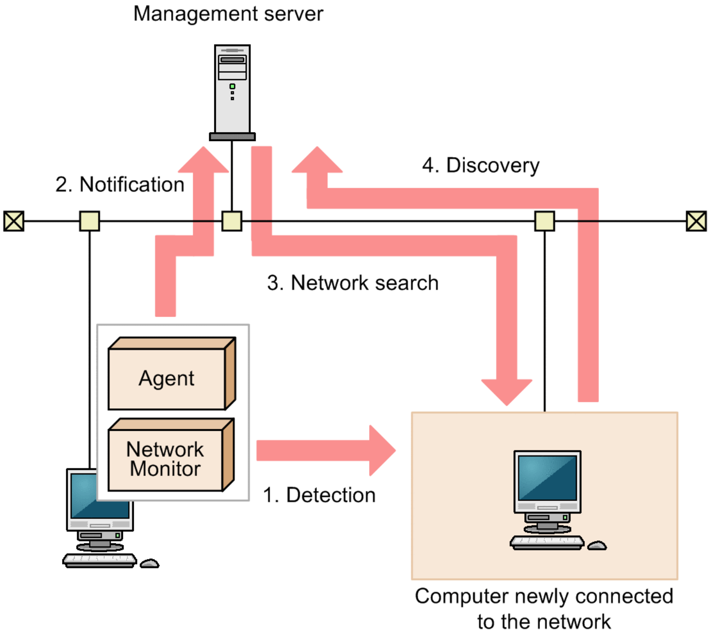
Important note

Before using the network monitoring function, make sure that you are fully aware of the devices to which network access is granted and those to which network access is denied. If network access control is applied incorrectly, network access control can cause unexpected business interruptions, for example, by disabling network access for devices used for business operations.

Tip

To detect devices, enable the network monitor for a single computer on which an agent is installed per network segment. By installing an agent on and enabling the network monitor for a computer capable of accessing multiple networks using multiple network cards, you can monitor multiple network segments using just one computer. Set an appropriate IP address range for the network segment and assign the corresponding authentication information. If a detected device has a network address that is outside the IP address range, a search is performed without using the authentication information. In this case, only the MAC address and IP address information is acquired from that device.

The following figure shows how a device connected to the network is detected and registered inJP1/IT Desktop Management 2:



Legend:

Agent: A computer with the agent installed

Network Monitor: A network monitor agent

1. The computer on which an agent is installed and for which the network monitor is enabled detects a device attempting to access the network.

2. The computer on which an agent is installed and for which the network monitor is enabled notifies the management server that a device has been detected.

3. Based on the received information, the management server searches the network for the detected device.

Tip

If you want to perform agentless authentication when the device is discovered, you need to set the IP address range that includes the IP addresses monitored by the network monitor as well as the corresponding authentication information in advance.

4. If the device is discovered during the search, it is automatically included as the management target or an agent is automatically deployed to it, depending on the search conditions.

Important note

The network monitoring function cannot detect devices in the network segments that cannot be accessed directly from the management server, such as networks through NAT.

Important note

If you have enabled the setting for automatically deploying an agent to a device discovered during network search, an agent is deployed to a discovered computer even when that computer is denied network access.

Under this circumstance, an agent is installed on a computer that is denied network access. Depending on the network control setting specified in the security policy and the result of a security check performed for that computer, the computer might be able to access the network.

Important note

If you remove a device that has been discovered by the network monitoring function, that device cannot be rediscovered until you disconnect from the network and then reconnect to it. If the time interval between network disconnection and reconnection is too short, the device might not be rediscovered.

Tip

Regardless of whether **Permit** or **Not Permit** is specified in the network monitor settings, devices accessing the network can be discovered. If the network monitor discovers a device, a network search is automatically performed for that device. If you have enabled the **Auto-Manage Discovered Nodes** or **Auto-Install Agent** setting for the network search, the device discovered by the network monitor is automatically included as a management target or an agent is automatically deployed to the device. The device then becomes a management target, and a product license is used for that device.

If you do not want to automatically include a discovered device as a management target, clear the **Auto-Manage Discovered Nodes** and **Auto-Install Agent** check boxes in **Configurations** so that you can manually select management targets.

The network monitoring function monitors the following networks:

- IPv4 networks. The IPv6 networks are not supported.
- The network monitoring function monitors computers running the OSs listed below. Computers running other OSs can be included as management targets only if such computers use standard TCP/IP network protocols.
  - Windows 95
  - Windows 98
  - Windows Me
  - Windows XP
  - Windows NT 3.51 and 4.0
  - Windows 2000
  - Windows Server 2003

    - Windows Vista
    - Windows Server 2008
    - Windows 7
    - Windows Server 2012
    - Windows 8
    - Windows 8.1
- The network monitoring function monitors TCP/IP network protocols. Protocols such as NetBEUI and IPX are not supported.
- To control devices accessing a wireless LAN, make sure that the access point relays MAC address information. If the access point does not relay MAC address information, network control cannot be performed.

2.8.2 Settings for controlling network connections

By enabling the network monitor feature in a network segment, you can control the network access of all devices in that segment. This section describes how to configure the network monitor feature to control access to the network.

Implementing the network monitor feature

To implement the network monitor feature, enable the network monitor in each segment where you want to monitor network access. You can then configure whether to permit devices to access the network in each of those segments. You can enable the network monitor on one computer in each network segment. The computer must have the agent installed. If you attempt to enable the network monitor on a second computer, an error message is displayed.

> **Tip**
>
> By viewing the **Topic** panel of the Home module, you can find out if there are any network segments without the network monitor enabled. A warning message appears if there are any such network segments.

Setting the control method for network access

The following settings govern how network connections are controlled in network segments with the network monitor enabled:

1. Whether newly discovered devices are permitted to connect to the network (network monitor settings)

   In the network monitor settings, you can set whether newly discovered devices in each network segment are permitted to connect to the network. Network monitor settings are assigned to computers with the network monitor installed. You can select which network monitor settings to assign when you enable the network monitor. You can later change the network monitor settings assigned to a network segment, or assign a different set of network monitor settings.

   For details about how to manage network monitor settings, see 2.8.6 Using network monitor settings to control network access.

2. Whether specific devices are permitted to connect to the network (network control list)

   In a network control list, you can define whether individual devices are permitted to connect to the network. When a device is discovered, it is automatically added to the network control list. Whether that device can connect to the network depends on the network monitor settings. By editing the settings in the network control list, you can control the network connectivity of individual devices. You can also permit a device to connect to the network only within a certain time period by setting a start date/time and end date/time.

Tip

You cannot specify a time period for network access by a management server, relay system, or a computer with network monitor enabled.

Tip

When you designate a discovered device as a management target or exclusion target, that device is automatically granted network access in the network control list. This is because the device is now seen as belonging to your organization.

Important note

To prevent routers, printers, servers, and other business-critical devices from being blocked due to automatic update of the network control list, we recommend that you manually enter the IP addresses of these devices in the network control list. When doing so, leave the **MAC address** field blank. If you enter a MAC address, the device might disappear from the network control list when its device information is updated. For details about the automatic update of the network control list, see 2.8.15 Automatic updating of the network control list.

For details about how to manage the network control list, see 2.8.8 Managing the network control list.

The network monitor settings and the network control list together govern a device's ability to connect to the network. By combining these settings, you can implement the following forms of network control:

- Permit newly connected devices to connect to the network, but deny network access to specific devices registered in the network control list (blacklist method)

  For **Discovered Nodes Option** in the network monitor settings, select **Allow Network Access**. New devices added to the network will have access to the network.
- Permit network access by devices registered in the network control list, and deny access to all other newly connected devices (whitelist method)

  For **Discovered Nodes Option** in the network monitor settings, select **Deny Network Access**.

  To automatically grant network access to new devices in this situation, permit connections for devices whose danger level is `Safe` in **Network Connection Control** under **Action Items** in the security policy. New devices are initially blocked from the network when they connect to the management server, but are permitted access to the network as soon as they are judged safe.

Exclusive communication destinations for blocked devices

Devices blocked by the network monitor feature can communicate with only computers with the network monitor enabled in the network segment and computers registered in the **Exclusive Communication Destination for Access-Denied Devices** list. For details about communication by blocked devices, see 2.8.13 Registering devices that are accessible to blocked devices.

You might have to specify the exclusive communication destination depending on the network environment of the organization. The following describes the cases in which exclusive communication destinations must be specified and examples of **Exclusive Communication Destination for Access-Denied Devices** settings.

When the exclusive communication destination must be specified	Description	Example of **Exclusive Communication Destination for Access-Denied Devices** settings
The DNS server is used to resolve the device names in the organization.	If the DNS server is used to resolve the device names in the organization, set the IP address of the DNS server for **Exclusive Communication Destination for Access-Denied Devices**. If the DNS server's IP address is not set and another IP address is set for **Exclusive Communication Destination for Access-Denied Devices**, name resolution will fail. As a result, network access using the host name will not be possible when the blocked devices connect to the exclusive communication destinations.	• Destination IP Address: IP address of the DNS server • Communication Protocol: No specification • Destination Port Number: No specification • Source IP Address: No specification • Source Port Number: No specification
NetBios broadcast is used to resolve the name of a device in the organization.	If NetBios broadcast is used to resolve the name of a device in the organization, set the broadcast address for **Exclusive Communication Destination for Access-Denied Devices**. If the broadcast address is not set, name resolution will fail. As a result, devices with the network monitor enabled will no longer be able to access the network by using the host name.	• Destination IP Address: Broadcast address (example: 192.168.1.255) • Communication Protocol: UDP • Destination Port Number: 137 • Source IP Address: No specification • Source Port Number: No specification
A device with the network monitor enabled is the DHCP server#	If a device with the network monitor enabled is the DHCP server, set IP address `0.0.0.0` for **Exclusive Communication Destination for Access-Denied Devices**. If `0.0.0.0` is not set, IP address assignment will fail. As a result, the devices with no IP address assigned will no longer be able to access the network.	• Destination IP Address: 0.0.0.0 • Communication Protocol: UDP • Destination Port Number: 68 • Source IP Address: Subnet mask in CIDR format (example: 255.255.255.0/24) • Source Port Number: 67

#: The DHCP server can automatically assign IP addresses. However, if the network monitor is installed in a Windows environment, the Remote Access feature (Incoming Connections) of Routing and Remote Access Service that is enabled at installation reserves 10 IP addresses. This reduces the number of IP addresses that can be assigned by 10. You can prevent this problem in the following OSs by stopping the Remote Access feature:

- Windows 8.1
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008

To stop the Remote Access feature:

1. Open the command prompt window with Administrator permissions.
2. Execute the `netsh ras show type` command at the command prompt.
3. Confirm that `Enabled` is displayed for `IPv4 Remote Access Server` at the command prompt.
4. Execute the following command at the command prompt to stop the Remote Access feature:

```
netsh ras set type ipv4rtrtype = lanonly ipv6rtrtype = none rastype = none
```

5. Restart the Routing and Remote Access Service service.

6. Execute the `netsh ras show type` command at the command prompt.

7. Confirm that `Disabled` is displayed for `IPv4 Remote Access Server` at the command prompt.

Related Topics:

- 2.8.10 Managing network access using a whitelist
- 2.8.9 Managing network access using a blacklist

2.8.3 Notes on network monitoring

- If the network monitor is enabled on a computer, and you want to change the IP address of that computer or add a new network to be monitored by that computer, you must first disable the network monitor. In the **Assign Network Access Control Settings** window, disable the network monitor. Then change the IP address or add a new network as a monitoring target, and then enable the network monitor again.
- The Windows Firewall is automatically disabled on computers with the network monitor enabled or JP1/IT Desktop Management 2 - Network Monitor installed. Keep the Windows Firewall disabled on these computers. If you enable the Windows Firewall or the firewall feature of a security suite or other software, you might be unable to use the communication channels specified in **Exclusive Communication Destination for Access-Denied Devices**.
- Computers with the network monitor enabled or JP1/IT Desktop Management 2 - Network Monitor installed use the Routing and Remote Access service. Do not stop the Routing and Remote Access service on these computers. In Windows Server 2012 and Windows Server 2008, do not stop the Routing and Remote Access Windows role service.

  Devices with the network monitor enabled can be blocked from the network in the following circumstances. In this case, stop the Routing and Remote Access service or restart the computer.

  - The network monitor is disabled
  - JP1/IT Desktop Management 2 - Network Monitor is uninstalled
- We recommend that you use a wired LAN connection for computers with the network monitor enabled. If you use a wireless LAN, the system might have trouble detecting and rejecting the LAN connections of unauthorized computers when there are problems in the communication environment.
- A blocked device for which an exclusive communication destination is specified must be able to communicate with the computer where the network monitor is enabled (the network access control agent). For this reason, blocked devices are able to communicate with the network access control agent even if the agent does not appear in the list of exclusive communication destinations. Do not create an environment in which a file server or other business-critical machine also functions as a network access control agent. A situation might arise in which an insecure device compromises the security of the business-critical machine.
- If blocked devices are permitted to access the network, they might require several minutes to access the network. If the devices cannot access the network after several minutes have passed, restart the user's computer.
- When the network monitor monitors a network in which IP addresses are allocated dynamically by a DHCP server, the IP addresses that the DHCP server attempts to lease to unauthorized computers are managed as in-use for a fixed period of time. If the network monitor blocks a large number of these unauthorized computers, the pool of available IP addresses is depleted. For this reason, we recommend that you promptly remove blocked computers from the network.

2.8.4 Displaying the operating status of the network monitor

When monitoring a network, icons are used to indicate which network segments are being monitored. The operating statuses of the network monitor are as follows:

✓ : Managing

The network is being monitored. The network monitor is enabled on a computer in the network segment.

✓ : Starting management

The network is not being monitored. The network monitor is being enabled on a computer in the network segment.

✓☒ : Failed to start management

The network is not being monitored. The network monitor failed to start.

✓ : Non-management

The network is not being monitored. The network monitor is disabled.

✓ : Stopped management

The network is being monitored. The network monitor that was enabled on a computer in the network segment is being disabled.

✓☒ : Failed to stop management

The network is being monitored. An attempt to disable the network monitor has failed.

The operating status of the network monitor appears in the following windows:

- The menu area in the **Device Inventory** - **Network List** view in the Device module
- The menu area in the **Computer Security Status** - **Network List** view in the Device module
- The information area in the **Network Access Control** - **Assign Network Access Control Settings** view of the Settings module

2.8.5 Changing the network access control agent

If a change of circumstances such as the replacement or repurposing of hardware means that you need to change the computer on which the network monitor is enabled, disable the network monitor and then enable it on another computer.

To change the network access control agent:

1. Disable the network monitor.

   When you disable the network monitor, the network monitor agent is uninstalled from the computer and the operating status appears as Non-management in the menu area. At this time, monitoring of the network temporarily stops.

2. Enable the network monitor.

   After the network monitor is disabled, enable the network monitor on the computer that you want to use as the network access control agent.

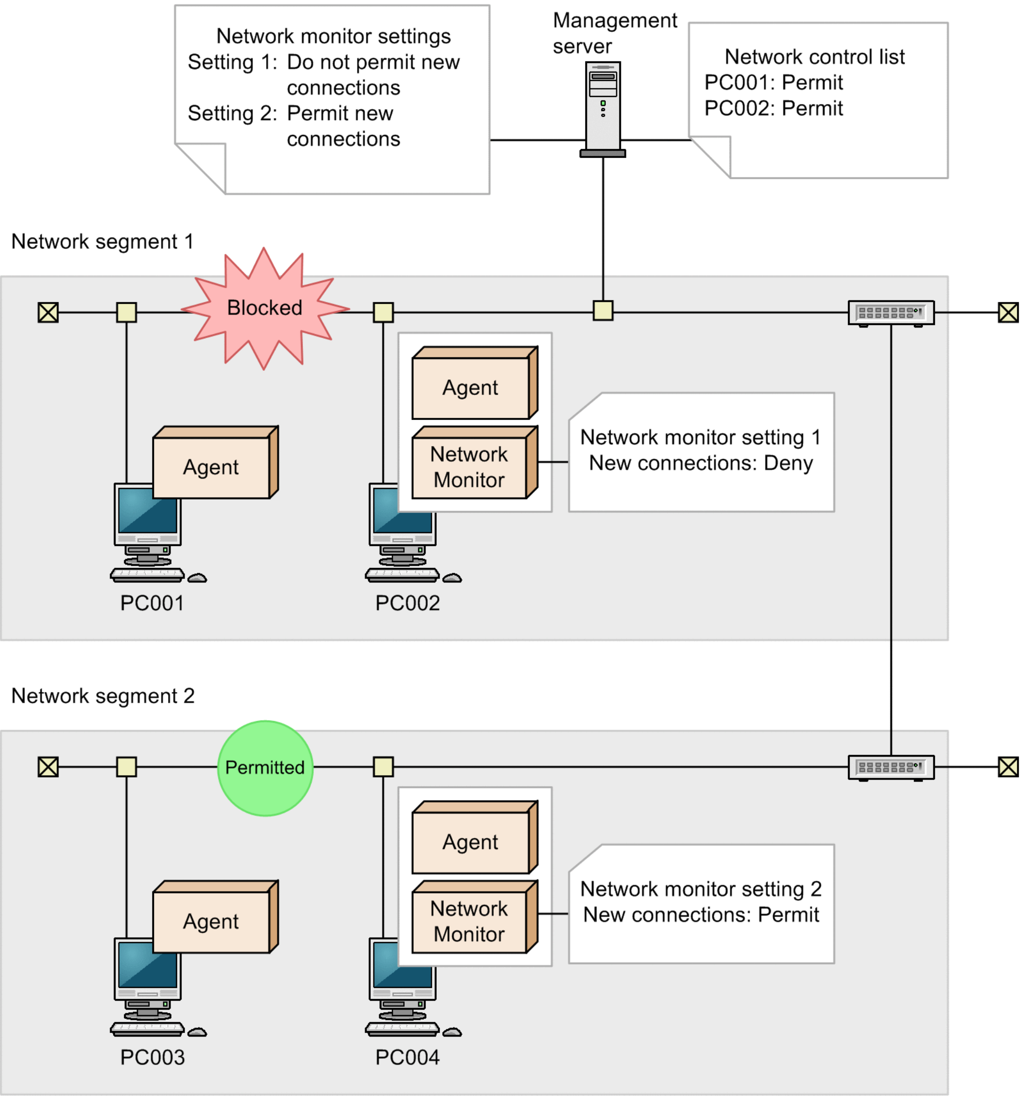
   After enabling the network monitor on a computer, you can monitor the network segment where the computer is located.

2.8.6 Using network monitor settings to control network access

By enabling the network monitor on a computer, you can control whether the devices in the network segment where the computer is located are permitted to connect to the network. To control network access differently in different network segments, you need to assign network monitor settings to each network segment.

By creating several sets of network monitor settings and assigning them to the appropriate network segments, you can create a network environment in which, for example, network segments with more stringent security requirements do not permit network access by new devices while others do.

The following figure shows an overview of allocating network monitor settings.



Legend:

Agent: A computer with the agent installed

Network Monitor: A network monitor agent

You can vary how network access is controlled in each network segment by creating several sets of network monitor settings. You can create network monitor settings in the **Network Access Control - Network Access Control Settings** view of the Settings module.

After creating network monitor settings, you need to assign them to network segments. You can assign network monitor settings in the **Network Access Control - Assign Network Access Control Settings** view of the Settings module.

Important note

If you have configured the system to automatically distribute the agent to devices discovered on the network, the agent program will be distributed to a discovered computer even if the computer is not permitted to access the network.

For this reason, depending on the network access control settings and the results of a security assessment, a situation might arise in which a computer that is not permitted network access is able to access the network.

Tip

You can detect networked devices regardless of whether **Permit** or **Do not Permit** is set in the network monitor settings. Devices detected by the network monitor are automatically subjected to network discovery. When the network monitor detects a device, any actions specified in the discovery conditions such as automatically registering the device as a management target or automatically distributing the agent program will take place. In this case, the device becomes a management target and uses one product license.

If you do not want to automatically register devices as management targets, clear the **Auto-Manage Discovered Nodes** and **Auto-Install Agent** check boxes in the discovery options, and manually register devices as management targets.

2.8.7 Managing network monitor settings

Network monitor settings allow you to control the network at the network segment level.

There are two network monitor settings: a standard setting that permits network access by default, and a setting that does not permit network access. If one set of network monitor settings is all you need, you can easily change the settings across the entire system by allocating the standard setting to every network segment.

Create network monitor settings if you need to use different network monitor settings in different network segments.

Edit network monitor settings if you need to change how network access is controlled.

Delete network monitor settings if changes to how you use the system mean that those settings are no longer required.

After creating network monitor settings, remember to allocate them to the appropriate network segments.

2.8.8 Managing the network control list

By using the network control list, you can control network access at the device level. You can also specify a time period during which a device is permitted to access the network. Newly discovered devices are automatically registered in the network control list, but an administrator can register devices manually when needed.

To control network access at the device level, add devices to the network control list.

You can change the network access of a specific device by editing its entry in the network control list.

Devices that were manually added to the network control list can be removed from the list.

Tip

By combining network monitor settings with the contents of the network control list, you can use a whitelist or blacklist approach to controlling network access.

Tip

- When the **Enable all automatic updates** check box is selected in the **Automatic Updates on Network Filter List** dialog box: If you delete a device whose network access is set to **Permit**, the device is also deleted from the network control list. This prevents the information for the device from being misused in the future. Conversely, if you delete a device whose network access is set to **Not Permit**, the device remains in the network control list to ensure the **Not Permit** setting is maintained if the device is changed.
- When the **Enable all automatic updates** check box is not selected in the **Automatic Updates on Network Filter List** dialog box (that is, automatic updating for only additions is enabled): If you delete a device, the entry for the device remains in the network control list regardless of whether **Permit** or **Not Permit** is set.

Important note

When you use a MAC address to enter a device in the network control list, the MAC address is correlated with any device information JP1/IT Desktop management collects for the device. This means that the host name or other information will be displayed instead of the MAC address. After this occurs, you can no longer delete the device from the network control list window. To delete such a device, use the Settings module.

Related Topics:

- 2.8.9 Managing network access using a blacklist
- 2.8.10 Managing network access using a whitelist

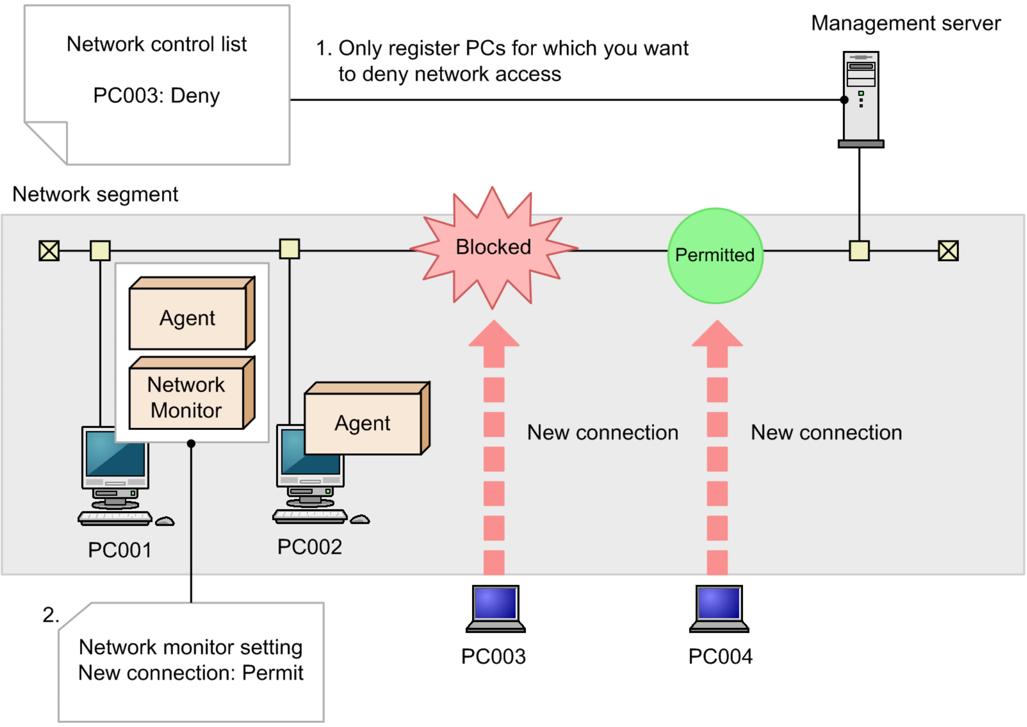
2.8.9 Managing network access using a blacklist

You can take a blacklist approach to managing network access, whereby a list is kept of devices for which you want to deny network access. We recommend this approach when there are specific devices, such as computers that must operate on a standalone basis or personal computers employees bring from home, whose network access might present a security risk.

Tip

When you first begin to monitor the network, you need to permit network access for a large number of devices. In this type of scenario, a blacklist can save you time by allowing you to permit network access for all devices, and then identify computers that should not have access to the network as time permits.

The following figure shows an overview of network access control using a blacklist approach.



Legend:

Agent: A computer with the agent installed

Network Monitor: A network monitor agent

1. Register devices for which you want to deny network access.

   In the **Network Access Control - Network Filter Settings** view of the Settings module, register devices that should not have network access. For details about how to manage the network control list, see 2.8.8 Managing the network control list.

2. Permit network access by all devices.

   In the **Network Access Control - Assign Network Access Control Settings** view of the Settings module, assign a network monitor setting to all network segments that permits network access. For details about network monitor settings, see 2.8.7 Managing network monitor settings.

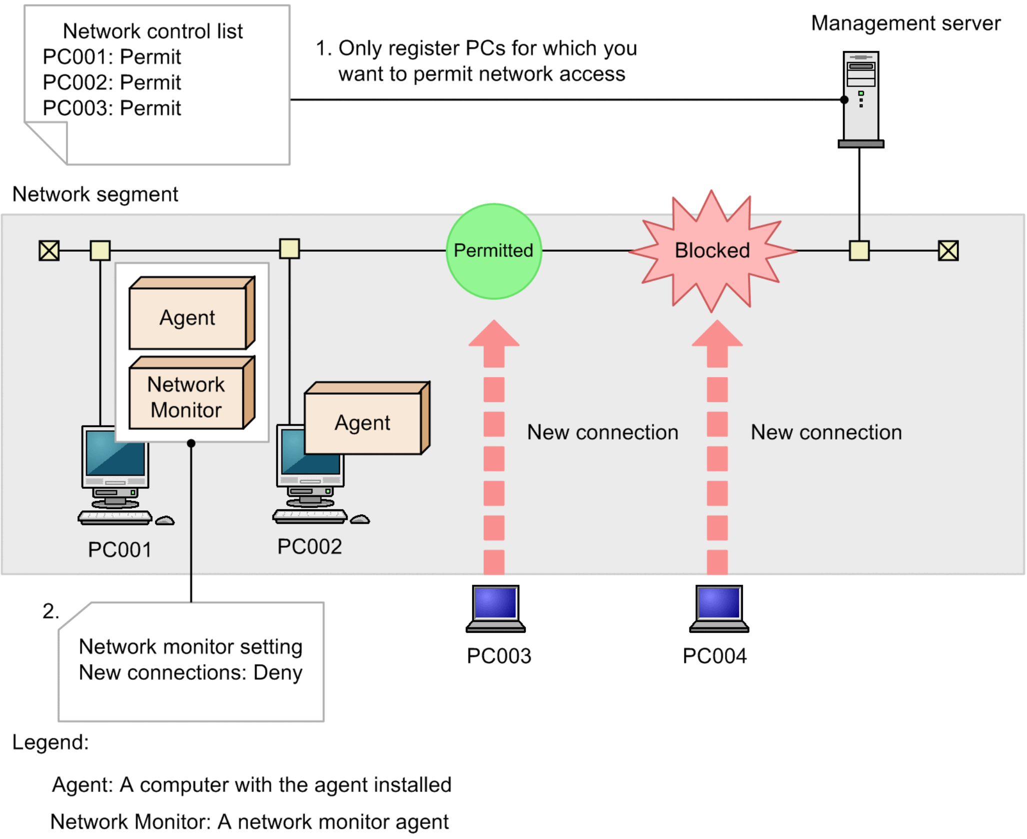
As a result, only the devices you registered in step 1 are blocked from the network.

When one of these devices attempts to connect to the network, it is blocked and an event is generated.

2.8.10 Managing network access using a whitelist

You can use a whitelist approach to managing network access, whereby only the devices you register in a list are able to connect to the network. We recommend that you use this approach when you need to provide a more robust security environment.

The following figure shows an overview of network access control using a whitelist approach.



1. Register devices for which you want to permit network access.

   In the **Network Access Control - Network Filter Settings** view of the Settings module, register the devices for which you want to permit network access. Be sure to register management servers, computers with the network monitor agent installed, and other devices that require a persistent connection to the network. Newly added devices are automatically added to the network control list. For details about how to manage the network control list, see 2.8.8 Managing the network control list.

2. Block network access by devices not registered in the network control list.

   In the **Network Access Control - Assign Network Access Control Settings** view of the Settings module, assign a network monitor setting to all network segments that denies network access. Any unlisted devices that attempt to connect to the network will be blocked. For details about network monitor settings, see 2.8.7 Managing network monitor settings.

As a result, only permitted devices are able to connect to the network. If a non-permitted device attempts to connect to the network, it is blocked and an event is generated.

Tip

If you have configured the system to block network access by new devices in the **Network Access Control** view of the Settings module, a new device is blocked when it attempts to connect to the network. In this case, you can automatically grant network access to new computers by installing the agent program on the computer and assigning a security policy whose danger level is configured to permit network access in the **Network Connection Control settings** under **Action Items**. When a computer with the agent installed connects to the network, its ability to access the network is determined based on the result of a security assessment. If it is permitted network access as a result, the computer is automatically added to the network control list.

Important note

When using the whitelist approach to manage network access, remember to permit network access by routers, switches, network printers, and other devices not directly managed by JP1/IT Desktop Management 2. A lack of network connectivity for such devices also prevents any downstream devices from accessing the network.

To use the whitelist approach to manage network access, change the automatic update setting of the network control list if necessary. By default, automatic updating for only additions is enabled.

If you want to automatically prevent a network connection device (such as a NIC) from being misused in the future, enable all automatic updates. However, if one of the conditions below exists, the system assumes that the network connection device (such as a NIC) has been removed, and deletes the device from the network control list. As a result, the device can no longer access the network.

- The network is disabled (by, for example, disabling the local area connection by using My Network Places).
- The network cable is removed from the device.
- A wireless LAN card is removed.

2.8.11 Timing of network control list updates

The following table describes the events that result in the network control list being updated.

No.	Timing of update	Example	Remarks
1	Device connection detected by network monitor	The network monitor feature detects a connection from a device while monitoring the network.	If a device connects to and then immediately disconnects from the network, a situation might arise in which the manager detects the connection but cannot acquire the IP address or MAC address of the device, preventing its addition to the network control list.
2	Device connection detected by device search	A network-connected device is discovered by a device search.	--
3	Adding or deleting a managed device	• An administrator adds a management target in the **Discovery** - **Discovered Nodes** view of the **Settings** module. • An administrator adds an exclusion target in the **Discovery** - **Discovered Nodes** view of the **Settings** module. • An administrator deletes a device from the **Discovery** - **Managed Nodes** view of the **Settings** module. • An administrator deletes a device from the **Discovery** - **Discovered Nodes** view of the **Settings** module. • An administrator deletes an exclusion target from the **Discovery** - **Ignored Nodes** view of the **Settings** module.	• If device information can be collected from the managed device, and the device incorporates more than one component with network connectivity (such as NICs), each of those components is added to the network control list. • Ordinarily, a device is added to the network control list when discovered by the network monitor or a device search. Devices are not added to the network list in response to the addition or deletion of a managed device, unless the device is deleted manually. • In environments that use a whitelist approach to network access control, a computer that becomes a management target by installation of the agent program is not initially able to access the network. To automatically grant such computers

No.	Timing of update	Example	Remarks
3	Adding or deleting a managed device	- An administrator adds a management target in the **Discovery** - **Discovered Nodes** view of the **Settings** module. - An administrator adds an exclusion target in the **Discovery** - **Discovered Nodes** view of the **Settings** module. - An administrator deletes a device from the **Discovery** - **Managed Nodes** view of the **Settings** module. - An administrator deletes a device from the **Discovery** - **Discovered Nodes** view of the **Settings** module. - An administrator deletes an exclusion target from the **Discovery** - **Ignored Nodes** view of the **Settings** module.	network access, assign a security policy that permits network access in the **Add Security Policy** dialog box, or in the **Action Items** - **Network Connection Control** view of the Edit Security Policy dialog box.
4	Network connection hardware (such as a NIC) is changed	- An administrator adds or removes a network connection device (such as a NIC) to or from a managed device. - The IP address assigned to a managed network connection device (such as a NIC) changes (including IP address changes in a DHCP environment).	When changes are made to the configuration or settings of a network connection device (such as a NIC) in an environment where device information can be collected from managed devices, the changes are reflected in the network control list.
5	Network access is manually permitted or denied	- You select **Allow Network Access** or **Deny Network Access** in the **Device Inventory** - **Device List** view of the **Device** module. - You select **Allow Network Access** or **Deny Network Access** in the **Computer Security Status** - **Device List** view of the **Security** module.	The changes you make in these windows apply to the setting (allow/deny network access) for the device in the **Connection to Network** part of the network control list.
6	Automatic network access control resulting from security assessment	A device for which a **Network Connection Control** setting is enabled and a **Violation Level (for controlling computer network connection)** is assigned in the **Edit Security Policy** view for the security policy selected in the **Security Policies** - **Security Policy List** of the **Security** module is subjected to network access control.	Depending on the security policy setting, the device is automatically permitted or denied network access. The automatic setting applies to the setting (allow/deny network access) for the device in the **Connection to Network** part of the network control list.
7	New hardware registration, modification, or disposal	- A new hardware asset is added with an IP address or MAC address specified. - The IP address or MAC address of a hardware asset is changed. - An administrator changes the **Asset Status** of a hardware asset to Disposed.	- Applies to hardware assets that are not associated with a device. Hardware assets associated with devices takes its settings from the device. - The result is the same as if the information were added, changed, or deleted manually.
8	Manual addition, modification, or deletion of network control list entries	An administrator adds, changes, or deletes data manually in the **Network Access Control** - **Network Filter Settings** view of the **Settings** module.	Data in the network control list that is associated with a device or hardware asset takes its value from the last change that was made to the device, hardware asset, or network control list, whether by an automatic or manual operation. Keep in mind that the value might be changed by an automatic process.

Legend: --: Not applicable.

Important note

If the management server is under a heavy load, it might take some time for changes to the network control list to take effect.

2.8.12 Settings in the network control list

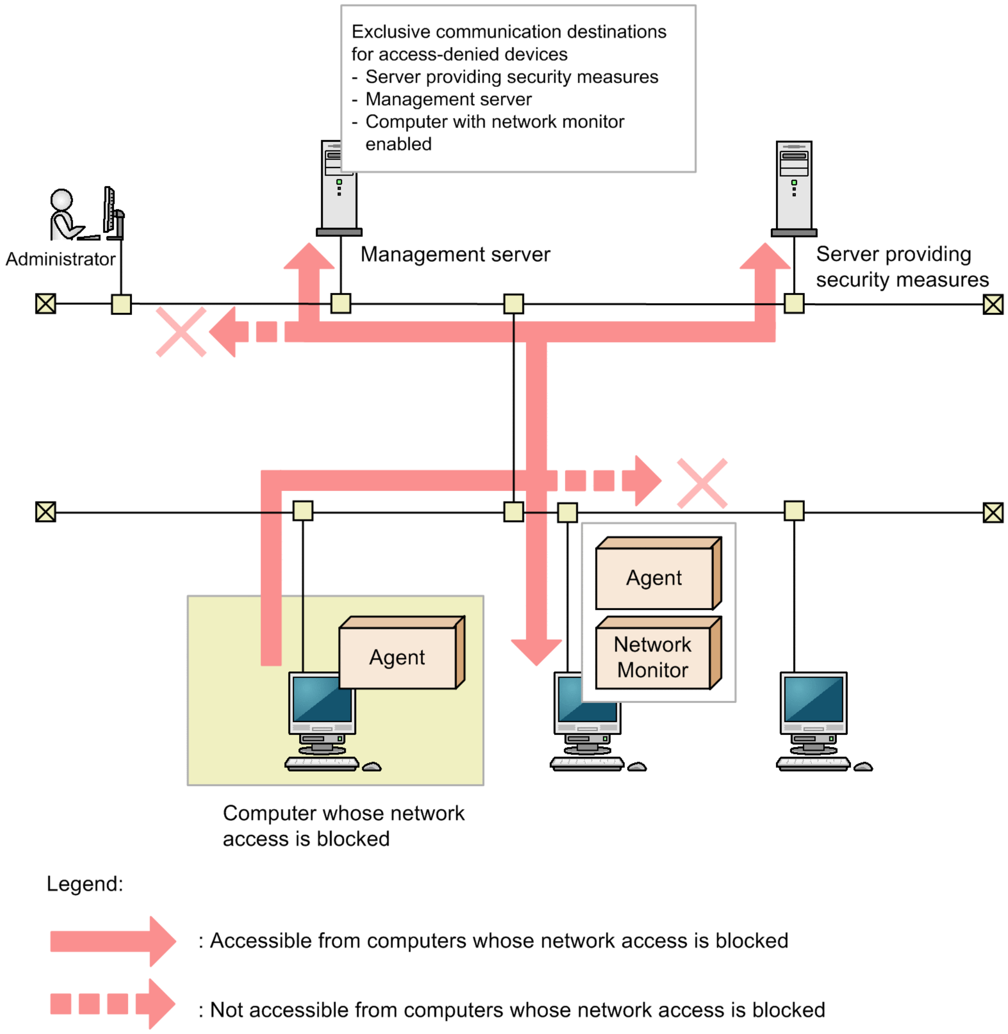
The following table describes the settings you need to enter in the network control list for devices used in particular ways.

Device usage	Settings in network control list
Used with fixed IP address	Register the MAC address and IP address of each NIC in the list, using any judgment form.
Used in DHCP environment	Set the judgment form to **MAC Address**.
Multiple IP addresses assigned to one MAC address	Set the judgment form to **MAC Address**
Using NIC teaming	Register the virtual MAC address in the list.
Used in a cluster environment	Register the physical IP address and logical IP address in the list.
Using several devices with one NIC	Register the corresponding IP addresses in the list in the following format: • Judgment form: IP address • MAC address: Do not enter • IP address: The IP address for the device.
When more than one of the following devices might have the same host ID: • Printer • Networking equipment • Devices on which the agent was installed through a disk copy	

2.8.13 Registering devices that are accessible to blocked devices

Some devices remain accessible to a device that has been blocked from the network by the network monitor feature: The computer in the same network segment that has the network monitor enabled, and any computers registered in **Exclusive Communication Destination for Access-Denied Devices**. Management servers and relay systems are automatically registered in **Exclusive Communication Destination for Access-Denied Devices**.

For example, if you register a server that provides security measures in **Exclusive Communication Destination for Access-Denied Devices**, a device that is blocked after being deemed a security risk can connect to the server to take security measures. The following figure shows an example in which a server that provides security measures is registered in **Exclusive Communication Destination for Access-Denied Devices**.


Exclusive communication destinations for access-denied devices
- Server providing security measures
- Management server
- Computer with network monitor enabled
Administrator
Management server
Server providing security measures
Agent
Agent
Network Monitor
Computer whose network access is blocked
Legend:
: Accessible from computers whose network access is blocked
: Not accessible from computers whose network access is blocked

Agent: A computer with the agent installed

Network Monitor: A network monitor agent

In **Exclusive Communication Destination for Access-Denied Devices**, only register computers that are fully secure and can communicate with quarantined devices without introducing a security risk.

Important note

When controlling network access based on the results of security assessment, do not remove the management server from **Exclusive Communication Destination for Access-Denied Devices**. If you do, you will be unable to judge the security status of devices, preventing network access from being controlled on this basis. If you inadvertently remove the server, add it again manually.

Important note

If you use Remote Installation Manager for distribution, never delete management servers or relay systems from **Exclusive Communication Destination for Access-Denied Devices**. Deleting those devices makes it impossible to perform distribution. If you delete a management server or relay system by mistake, add it in **Exclusive Communication Destination for Access-Denied Devices** manually.

Tip

You can use the remote control feature with blocked devices by adding the computer on which you use the controller to **Exclusive Communication Destination for Access-Denied Devices**.

2.8.14 Automatically controlling network access

In an environment with the network monitor enabled, devices are automatically subjected to network access control based on a number of factors, including the results of assessment against a security policy and the nature of the device information registered for the device. For example, a computer that violates a security policy might be automatically blocked from the network, and then automatically unblocked after the issue is resolved.

Levels of priority apply to network access control settings. If you manually deny a device network access, and a situation later arises in which the device would be automatically granted access to the network, the device remains blocked. If you want to prevent a particular computer from connecting to the network in any circumstances, set it to **Deny** manually to prevent it from automatically being permitted network access at a later stage. For details about how to manually control network access, see 2.8.17 Manually controlling network access.

The following table describes the situations in which the features of JP1/IT Desktop Management 2 might automatically control the network access of a device.

Situation in which network access is controlled	Description
A device violates a security policy	If you define a security policy that denies network access to devices with a specific danger level in **Action Items** - **Network Access Control**, such devices are automatically blocked when assessed against the security policy. If the security status of a blocked computer later improves, it is judged as being compliant with the security policy and is automatically permitted network access again.
A hardware asset is added or edited	If you add a hardware asset in the **Hardware Assets** view of the Assets module that has an IP address or a MAC address, the device is registered in the network control list. If you change the IP address or MAC address in asset information, the change is reflected in the network control list. Network access is similarly permitted for imported hardware assets. When a hardware asset is associated with a device, editing the hardware asset information does not result in changes to the network control list because IP addresses and MAC addresses are collected from the device. Note that if you change the status of the hardware asset to Disposed or delete the hardware asset information altogether, the corresponding entry is removed from the network control list. If you edit a MAC address in hardware asset information when the network control setting for the same MAC address already exists, the change is not applied to the network control list. If automatic updating for only additions is enabled, the new setting is added while the network control settings before the change remain. In the remaining network control settings, **Confirmation Choices** is set for **Automatic Updates Effect (Only Add Operations Enabled)**. For details about how to set automatic updating, see the description of the procedure for editing the automatic update of the network filter list in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.
A device enters the allowed time period for network access	If you permit a device to connect to the network within a specific time in the network control list, the device is automatically permitted network access when the specified start date/time arrives. When the end date/time arrives, the device is automatically blocked from the network again.
A discovered computer is designated as a management or exclusion target	When you designate a newly discovered computer as a management target or exclusion target, that computer is automatically granted network access. Even if network access is not permitted in a network segment, a discovered device that is designated a management or exclusion target is able to access the network. However, when a device discovered in a search is automatically designated a management target, it is subjected to network access control according to the network monitor settings.

Situation in which network access is controlled	Description
A new device connects to the network	When network monitor settings are assigned to a network segment, new devices that connect to the network are automatically subjected to network access control based on the network monitor settings.
Device information is updated or deleted	If the MAC address or IP address of a device changes as a result of an update to device information, the corresponding change is automatically made to the network control list[#]. If automatic updating for only additions is enabled, the new setting is added while the network control settings before the change remain. In the remaining network control settings, **Confirmation Choices** is set for **Automatic Updates Effect (Only Add Operations Enabled)**. For details about how to edit the automatic update settings, see the description of the procedure for editing the automatic update of the network filter list in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.
Information is updated for a network connection device	With all automatic updates enabled, the system determines that the network adapter information has been deleted and deletes the MAC address of the network adapter from the network control list (unless **Not Permit** is set) in the following cases: • The network is disabled (by, for example, disabling the local area connection by using My Network Places). • The network cable is removed from the device. • A wireless LAN card is removed. If automatic updating for only additions is enabled, the new setting of the network adapter is added while the network adapter settings before the change remain. In the remaining network adapter settings, **Confirmation Choices** is set for **Automatic Updates Effect (Only Add Operations Enabled)**. For details about how to edit the automatic update settings, see the description of the procedure for editing the automatic update of the network filter list in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*. If the network adapter of a device is frequently disabled, register the device in the network control list with the following information: • Judgment Form: IP Address • MAC Address: Do not enter • IP address: The IP address of the device • Connection to Network: Permit Fill in the other items as needed.

#: For details about the updates of the network control list, see 2.8.15 Automatic updating of the network control list.

Important note

While the network monitor is disabled, changes are still made to the settings that determine whether a device has network access. However, devices are not subject to network access control. Changes only take effect when the network monitor is enabled again.

Tip

An event is generated when a device is denied or permitted network access. You can also configure the system to notify the administrator by email.

Related Topics:

- 2.9.4 Managing a security policy
- 2.11.2 Managing hardware asset information
- 2.8.8 Managing the network control list

2.8.15 Automatic updating of the network control list

When you add, update, or delete hardware information or device information, the network control list is automatically updated. The following describes update operations that are performed automatically.

- If hardware asset information contains a MAC address or IP address that is not found in the network control list, information about the MAC address or IP address is added to the network control list.
- If you change the status of the hardware asset to Disposed or delete the hardware asset information, the corresponding entry is removed from the network control list.
- If you edit an IP address or MAC address in hardware asset information, the changes are applied to the network control list. However, if a hardware asset is associated with a device, editing the hardware asset information does not result in changes to the network control list because IP addresses and MAC addresses are collected from the device. If the network control setting for the same MAC address already exists, no changes are made in the network control list.
- When device information contains a MAC address not found in the network control list, the MAC address and its IP address are added to the network control list. If the device that sent the device information has already been registered in the management server, the device is registered in the network control list with the permission status below. The permission status to be registered in the network control list is set according to the permission status of the device, as described in the following table:

Permission status of the device	Permission status in the control list
Allowed	Permit
Blocked	Not permit
Forced Blocking	Not permit
Not use period	Not permit

  If the device that sent the device information has not been registered in the management server, the device is registered to the network control list with the following permission status. The permission status to be registered in the network control list is set according to the network monitor setting that is currently assigned to the network group to which the device's IP address belongs. The network monitor setting is displayed as the **Discovered Nodes Option**.

Network Monitor	Discovered nodes option	Permission status in the control list
Installed	Permit	Permit
	Not Permit	Not Permit
Not Installed		Determined based on the settings in the network control settings file#

  #: Determined based on the settings in the network control settings file. By default, the device with the "Permit" status is registered. For how to set the network control settings file, see the description of the procedure for editing the network control settings file in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Configuration Guide*.
- If the most recently collected device information lacks a MAC address that was present in the previous set, the system assumes that the network card has been removed and deletes its MAC address information from the network control list. The MAC address is also removed from the network control list if the network card is disabled.
- The system behavior when the IP address changes in the device information depends on the Judgment Form option selected in the **Add Allow or Deny Network Access Permission** dialog box or the **Edit Network Connection Permission or Denial** dialog box.
  - When the judgment form is **MAC Address**:
    The IP address information for the device is changed in the network control list.

- When the judgment form is **IP Address** or **MAC Address + IP Address**:
  The device information in the network control list is left unchanged.

For this reason, we recommend that you select MAC Address as the judgment form in environments where IP addresses change frequently.

> **Tip**
>
> By default, automatic updating of the network control list is enabled only for additions of devices. If you upgrade JP1/IT Desktop Management 2 version 10-01 or earlier, all automatic updates including additions, changes, and deletions are enabled.
>
> When automatic updating is enabled for only additions, the network control settings are retained without being changed or deleted (if you attempt to change the settings, new settings are added). In the remaining network control settings, **Confirmation Choices** is set for **Automatic Updates Effect (Only Add Operations Enabled)**.
>
> For details about how to set automatic updating, see the description of the procedure for editing the automatic update of the network filter list in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

2.8.16 Managing exclusive communication destinations for devices denied network access

By setting exclusive connection destinations, you can allow blocked devices to access specific devices on the network. For example, if you register a server that provides security measures in the **Exclusive Communication Destination for Access-Denied Devices** list, a device that is quarantined after being deemed a security risk can connect to the server to update its security. The management server is registered in the **Exclusive Communication Destination for Access-Denied Devices** list by default.

For computers on which the network monitor agent is installed, the environment is automatically configured as described below. Because this environment is a prerequisite for communication with exclusive communication destinations, do not change these settings.

- Windows Firewall is disabled
- The service (Routing and Remote Access) is enabled
- When the OS is Windows Server 2012 or Windows Server 2008, the Windows Routing and Remote Access role service is enabled.

To permit blocked devices to access specific devices on the network, create exclusive communication destination settings.

To change the devices that are accessible to a device that is blocked from the network, edit the exclusive communication destination settings.

If changes to the system mean that you no longer need an exclusive communication destination setting, delete the setting.

2.8.17 Manually controlling network access

You can manually control network access while the network monitor is enabled.

Levels of priority apply to the network access control settings. If you manually deny a device network access, and a situation later arises in which the device would be automatically granted access to the network, the device remains blocked. If you want to prevent a particular computer from connecting to the network in any circumstances, set it to **Deny** manually. For details about how to manually control network access, see 2.8.14 Automatically controlling network access.

Tip

If you manually permit a device to access the network, and a situation later arises that automatically blocks the device, the manual setting is overruled and the device is denied network access.

You can use the following method to manually change a device's network access:

Controlling network access in the Device module or Security module

> In the **Device Inventory** view of the Device module and the **Computer Security Status** view of the Security module, you can change the network connection status of individual devices.
>
> Select the computer whose connection status you want to change in the information area, and from the **Action** menu, select **Allow Connection** or **Deny Connection**. The change takes effect immediately.

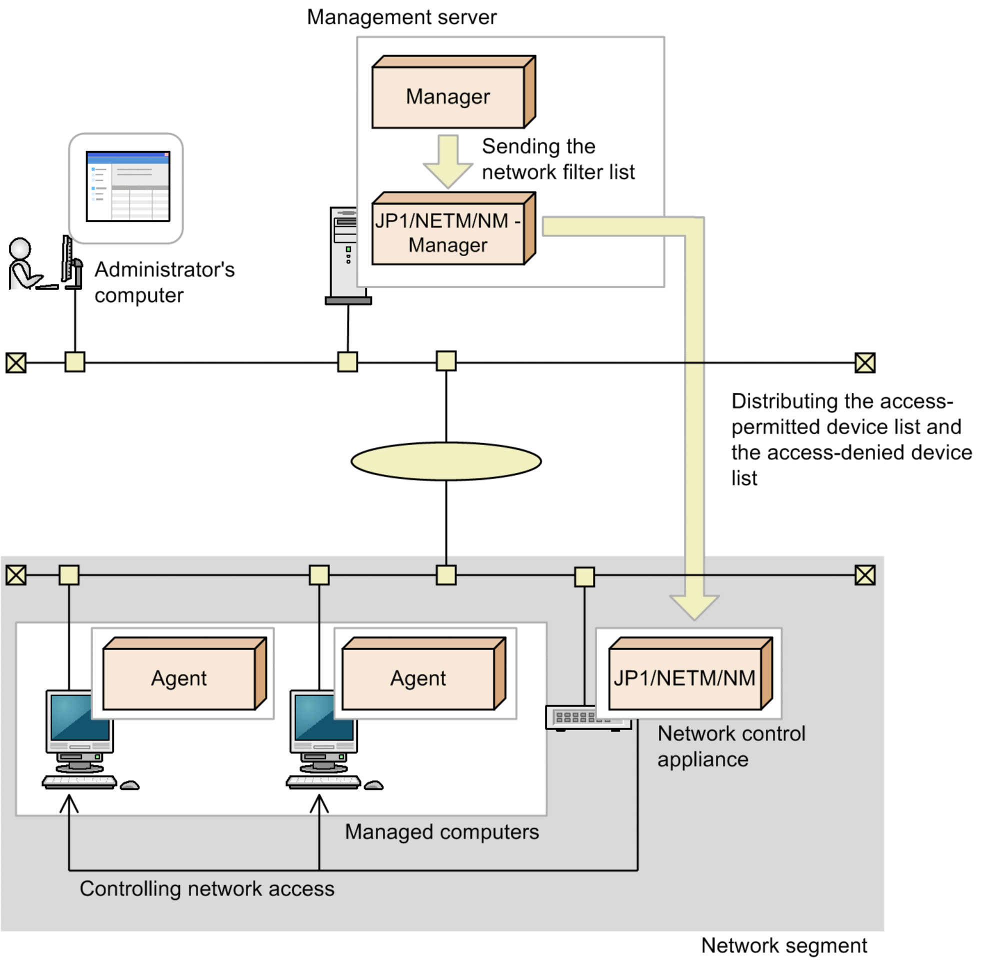
2.8.18 Network control function by linking with JP1/NETM/NM - Manager

Linking JP1/IT Desktop Management 2 with JP1/NETM/NM - Manager allows you to control network access without installing computers on which the network monitor is enabled.

To link with JP1/NETM/NM - Manager, you must install JP1/NETM/NM - Manager and a network control appliance. Japanese versions of JP1/NETM/NM - Manager 09-50 or later can be linked.

Linking with JP1/NETM/NM - Manager allows you to control network access by using the network control appliance, eliminating the necessity of installing or managing computers with the network monitor enabled in each site.

The following figure shows an overview of controlling the network by linking with JP1/NETM/NM - Manager.


Management server
Manager
Sending the network filter list
JP1/NETM/NM - Manager
Administrator's computer
Distributing the access-permitted device list and the access-denied device list
Agent
Agent
JP1/NETM/NM
Network control appliance
Managed computers
Controlling network access
Network segment

Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Agent: JP1/IT Desktop Management 2 - Agent

JP1/IT Desktop Management 2 - Manager sends the network control list containing a list of access-permitted devices and a list of access-denied devices to JP1/NETM/NM - Manager. JP1/NETM/NM - Manager distributes the access-permitted device list and the access-denied device list to the network control appliance, which then controls network access of the network segment based on these lists.

Network access of devices managed by JP1/NETM/NM - Manager can be detected. However, unlike the network monitoring function of JP1/IT Desktop Management 2, devices in the network are not automatically discovered.

Because the following settings cannot be specified in JP1/IT Desktop Management 2, specify them in JP1/NETM/NM - Manager.

- Environment setting of the network control appliance
- Exclusive communication destinations for devices managed by JP1/NETM/NM - Manager

Related Topics:

- 4.4.12 JP1/NETM/NM - Manager linkage configuration

2.9 Managing security

There are various causes of problems related to computer security within an organization. (For example, if no anti-virus product is installed, if file share software is installed, or if the security settings for an OS are not sufficient.) To maintain a safe security status in an organization, you must define security rules for such causes, and have the computer users comply with those rules. Also, you must understand the security status, and take appropriate measures for problems as necessary.

Using JP1/IT Desktop Management 2, you can set security rules within an organization as a *security policy*, and apply it to each computer. By doing so, problems can be detected and the administrator notified, or automated countermeasures can be enforced.

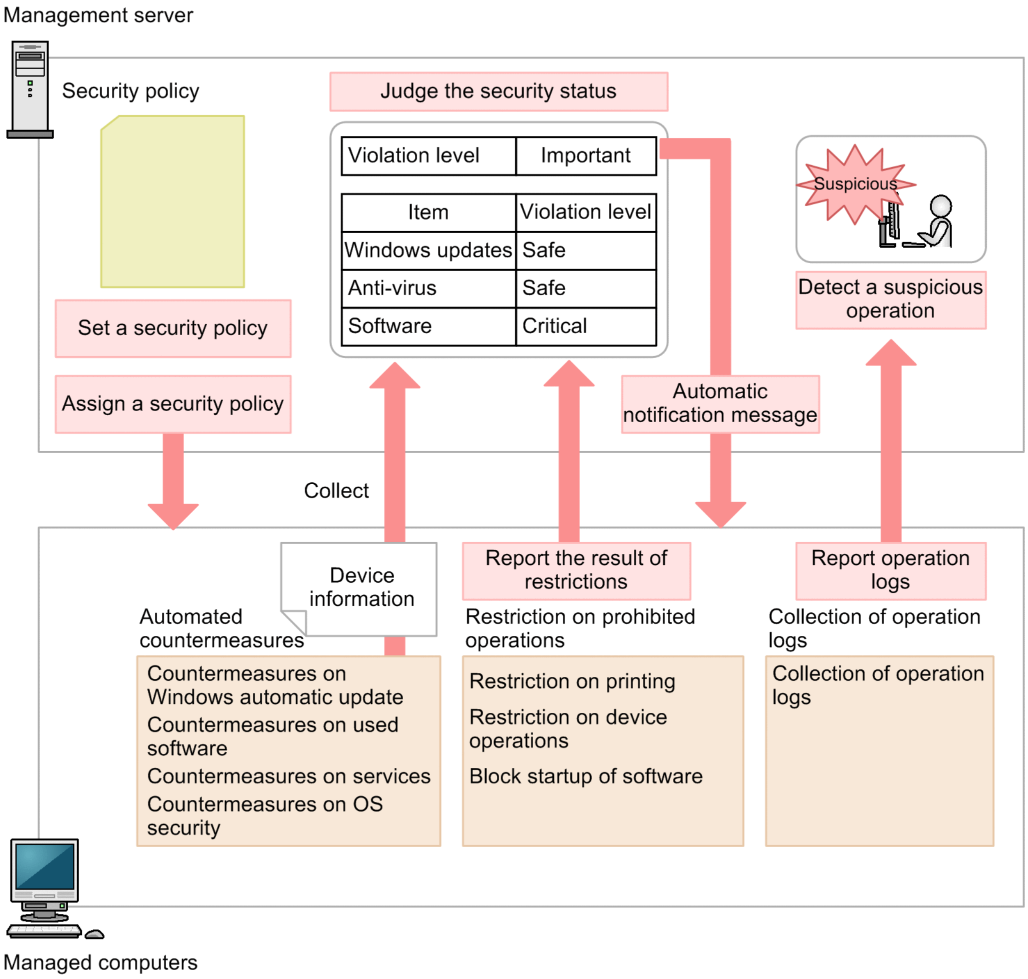
By using a security policy, you can understand the following security statuses:

- Whether updates are applied
- Whether anti-virus products are applied
- Whether mandatory software programs are installed
- Whether prohibited software programs are installed
- Operating status of services
- Status of the OS settings

You can also configure various other settings regarding security management (for example, restrictions on the use of software programs or devices, or detection of suspicious operations on computers).

2.9.1 Managing security status

The following figure shows how the security status of a computer is managed.


Management server
Security policy
Set a security policy
Assign a security policy
Judge the security status
Suspicious
Detect a suspicious operation
Automatic notification message
Collect
Device information
Automated countermeasures
Report the result of restrictions
Restriction on prohibited operations
Report operation logs
Collection of operation logs
Countermeasures on Windows automatic update
Countermeasures on used software
Countermeasures on services
Countermeasures on OS security
Restriction on printing
Restriction on device operations
Block startup of software
Collection of operation logs
Managed computers

Violation level	Important

Item	Violation level
Windows updates	Safe
Anti-virus	Safe
Software	Critical

First, define a security policy according to the security rules of an organization. JP1/IT Desktop Management 2 automatically assigns the default policy to managed computers. Therefore, you can judge the security status based on the default policy even if a new security policy has not yet been created. A recommended security policy (in which recommended security settings are defined) is also provided. For details about the default policy and the recommended security policy, see (3) Security policies provided by the product.

If you want to judge the security status based on a security policy other than the default policy, you need to add a security policy and assign it to the managed computers. After a security policy is assigned to a computer, the management server judges the security status of the computer based on the collected device information and the security policy. Also, prohibited operations are restricted and operation logs are collected on the managed computer. If automated countermeasures (Auto Enforce) are set, the countermeasures are enforced when the security policy is violated. For details about how to judge the security status, see 2.9.3 Judging security status. For details about how to restrict prohibited operations, see 2.9.5 Restricting prohibited operations.

The results of the security status judgment and the restriction of prohibited operations are notified to the management server, and the security status of the computer is displayed. The administrator must check the security status and take appropriate actions for solving problems. If automatic notification of messages is set in a security policy, messages are automatically sent to the managed computers according to the judgement results.

Operation logs are collected on the managed computers. Suspicious operations, judged based on the collected operation logs, are detected based on the security policy settings. The administrator can track suspicious operations through the operation logs, and check for information leakage. For details about tracking detected suspicious operations using operation logs, see 2.10.3 Investigating suspicious movements of files from systems using operation logs.

> **Important note**
>
> When the security settings for computers within an organization are defined by a group policy for Active Directory, the settings take precedence over the security settings defined by a security policy for JP1/IT Desktop Management 2 even if automated countermeasures are set for the latter security settings.

> **Important note**
>
> When you manage the security status of a virtual computer, install an agent on the virtual computer, as well as on the virtualization server.

Related Topics:

- (1) Items that can be set for a security policy

2.9.2 Devices available for security management

In JP1/IT Desktop Management 2, security management is available only for management-target devices.

Note that whether or not a device is a management-target depends on whether an agent is installed on that device. The following table shows the devices for which security management is available.

Device type	OS type	Whether the security management functions can be executed			
		Security judgment	Automated countermeasures (Auto Enforce)	Actions	
				Message notification	Network control
Computer	Windows 8.1	Y [#1, #2]	A [#3]	A [#3]	Y
	Windows 8				
	Windows Server 2012 R2				
	Windows Server 2012				
	Windows 7				
	Windows Server 2008 R2				
	Windows Server 2008				
	Windows Vista				
	Windows Server 2003 R2[#4]				
	Windows Server 2003[#4]				
	Windows XP				
	Windows 2000				
	Linux	N	N	N	Y
	UNIX				
	Mac OS				

Device type	OS type	Whether the security management functions can be executed			
		Security judgment	Automated countermeasures (Auto Enforce)	Actions	
				Message notification	Network control
Computer	Unknown	N	N	N	Y
Smart device	iOS	N	N	N	Y
	Android				
Storage	--	N	N	N	Y
Network device					
Printer					
Peripheral device					
USB device					
Display					
Others					
Device type added by the administrator					
Unknown device					

Legend: Y: Can be executed. A: Can be executed only on the devices on which an agent has been installed. N: Cannot be executed. --: Not applicable.

#1: The function is not supported if the edition of the OS is `Unknown`.

#2: Security judgment is not available for the computers that were selected as management targets via SNMP authentication and network search or Active Directory search. (The judgment result becomes `Unknown`.)

#3: The function can be executed only when the target computer is managed online. If the security policy is violated on a computer that is managed offline, manually take security measures.

#4: Windows Server 2003 and Windows Server 2003 R2 are regarded as the same OS. For example, in **Windows Update** view (under **Security Configuration Items**) of the Edit Security Policy dialog box, if Windows Server 2003 Standard Edition is included in the specified group, the target OS includes Windows Server 2003 Standard Edition and Windows Server 2003 R2 Standard Edition.

2.9.3 Judging security status

Once a security policy is assigned to a computer, the security status of the computer is judged based on the security policy settings. During judgment, the management items in the security policy and the device information collected from the managed computer are compared and the violation level is judged.

Note that if message notification is set as an action item in a security policy, messages can be automatically sent to the computer depending on the results of the security status judgment. The messages notify of security problems. Therefore, the administrator can reduce the workload required to solve problems by directing users to take actions according to the messages.

Tip

When OS user accounts have been automatically created by some OS components or by certain programs, if the security statuses of unused user accounts are judged, you might not be able to manage the security status correctly. In such a case, you can exclude the unused user accounts from the judgment targets so that the security status can be judged appropriately.

(1) Violation levels judged by a security policy

If you define the judgment conditions and the countermeasures in a security policy and then assign the security policy to the managed computers, the violation level for security is judged based on the level of compliance with the security policy.

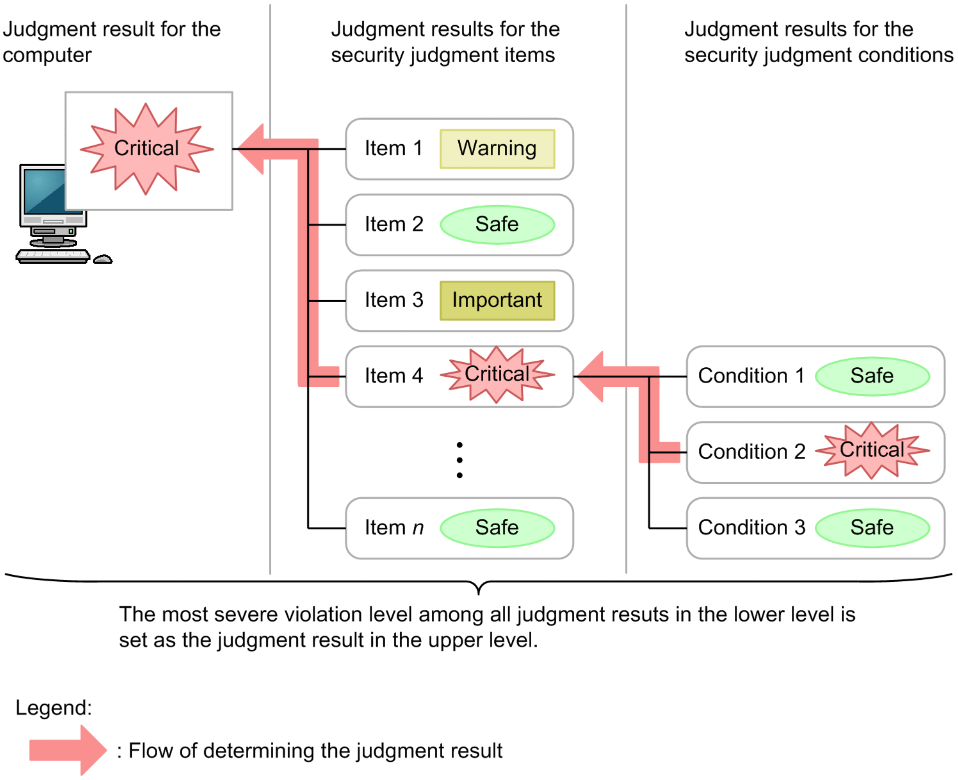
In a security policy, set the violation level (for each security judgment item) that will be displayed when the security status is judged as improper. If the security policy is not complied with, the judgment results in the violation level that has been set. The most severe violation level is displayed as the overall violation level of the computer.

The following table shows the types of violation levels in the order from the severe.

Violation level	Icon	Description
Critical	✖	This is the most severe violation level. This violation level is set when the extent of damage might extend to the whole system and it might have a significant impact on business, such as suspension of business, if an immediate action is not taken.
Important	!!	This violation level is set when negligence of security measures for computers with security vulnerability might have a significant impact on the business.
Warning	!	This violation level is set when taking security measures will improve system safety even though the impact on business might not be significant.
Unknown	?	This violation level is set when the judgment results in one of the following: • Judgment of the security status has not yet been performed. • The security status cannot be judged because there is insufficient information. In this case, you must install an agent on the computer and collect the necessary information so that the security status can be correctly judged. • The security status was not judged correctly. In this case, the security status cannot be judged correctly because of an internal failure. You must investigate the cause of the failure and take appropriate action, referring to troubleshooting information, such as logs.
Safe	✓	This violation level is set when the computer complies with the security judgment items and judgment conditions.
Out of Target	None	This violation level is set when the judgment items for the security policy are not set. This violation level is also set when the managed device is one of the following because judgment of the security policy is not performed for them: • Computer running an unknown OS • Computer with an unknown Windows edition • Computer running Linux, UNIX, or Mac OS

Judgment conditions for the violation level

The violation level is judged for security judgement conditions, security judgement items, and the computer.The following figure shows how the violation level is judged.


Judgment result for the computer
Judgment results for the security judgment items
Judgment results for the security judgment conditions
Critical
Item 1
Warning
Item 2
Safe
Item 3
Important
Item 4
Critical
Item *n*
Safe
Condition 1
Safe
Condition 2
Critical
Condition 3
Safe
The most severe violation level among all judgment resuts in the lower level is set as the judgment result in the upper level.
Legend:
: Flow of determining the judgment result

First, the violation level is judged for each security judgment item. If multiple security judgment conditions are set for a security judgment item, the violation level is judged for each judgement condition. The most severe security judgment condition result is determined to be the violation level of the relevant security judgment item.

Then the most severe security judgement item result is determined to be the violation level of the computer.

In this figure, judgment condition 2 of security judgment item 4 is judged as `Critical`, so security judgment item 4 is determined to be `Critical`, even though the other judgment conditions are judged as `Safe`. The computer is determined to be `Critical` because security judgment item 4 is judged as `Critical` even though the other judgement items are judged as `Safe` or `Important`.

For details about the security judgment conditions and security judgment items, see (1) Items that can be set for a security policy.

Note that you can check whether a computer complies with the security policy in the **Computer Security Status** view of the Security module.

Counting the number of days regarding the violation level

The number of sequential days in which no security measures are taken is counted for each device. This information is used to send messages to users who have not taken security measures during a certain period of time, or to block the network connections for relevant devices.

The number of sequential days is incremented by 1 when 24 hours has passed since the time the violation level was judged as `Critical`, `Important`, or `Warning`. The following shows an example of counting the number of sequential days:

- 2011/4/1 0:00 to 2011/4/5 5:59: Judged as `Critical`.
- 2011/4/5 6:00 to 2011/4/7 12:00: Judged as `Important`.

In this case, JP1/IT Desktop Management 2 regards that no security measures were taken during the period from 2011/4/1 0:00 to 2011/4/7 12:00 (6 days and 12 hours). The number of sequential days in which no security measures were taken is counted as 7 days.

(2) Timing of security status judgment

The security status is judged on a periodic schedule. It is also judged when key device information is updated or changed.

The following table shows the details of security-status judgment conditions.

Timing	Security policy used for judgment	Computer to be judged	Description
A security policy is assigned.	Assigned security policy	• All devices to which the security policy has been assigned • All devices that belong to the group to which the security policy has been assigned#	Judgment is performed when a security policy is first assigned. It is also performed when and existing security policy is cancelled and a new security policy is assigned to a device or group.
The security policy is updated.	Updated security policy	• All devices to which the updated security policy has been assigned • All devices that belong to the group to which the updated security policy has been assigned#	Judgment is performed when the security policy is updated.
The system administrator updates asset information in the operation window or by using a command.	The priority order of the security policies is as follows: • Security policy assigned to the device • Security policy assigned to the group	Devices related to the assets whose asset information has been updated	If the added management item has been specified for at least one security policy as a user-defined security item, judgment is performed regardless of whether that security policy is used for judgement.
The system administrator changes the hardware asset assigned to the device.	The priority order of the security policies is as follows: • Security policy assigned to the device • Security policy assigned to the group	Devices whose association with hardware assets has been changed	If the added management item has been specified for at least one security policy as a user-defined security item, judgment is performed regardless of whether that security policy is used for judgement.
Device information for the managed computer is updated in the operation window.	The priority order of the security policies is as follows: • Security policy assigned to the device • Security policy assigned to the group	All devices whose device information has been updated	For online management: Judgment is performed when the changed device information is collected on the management server and then updated. For offline management: Judgment is performed when the information collected from the computer by the information collection tool is reported to the management server.
The group to which the managed computer belongs is changed.	Security policy assigned to the new group	Devices whose group has been changed#	If the target group type for the security policy is not a user-defined group: Judgment is performed when the group to which the device belongs is changed, and a new security policy is assigned to the group.

Timing	Security policy used for judgment	Computer to be judged	Description
The group to which the managed computer belongs is changed.	Security policy assigned to the new group	Devices whose group has been changed#	If the target group type for the security policy is a user-defined group: Judgment is performed when the user-defined group condition is changed for one of the following reasons: • The system administrator changed the user-defined group condition. • An added management item specified as the target item of a user-defined group is deleted. • An option of the added management items (whose data type is Emulation) specified as the target item of a user-defined group is deleted.
Periodical judgment (0:00 every day, by default)	The priority order of the security policies is as follows: • Security policy assigned to the device • Security policy assigned to the group	All devices	Judgment is performed according to the schedule specified in the **Security Schedule** view of the Settings module.

#: If another security policy is directly assigned to a device, that security policy has priority for the device. Therefore, the device is excluded from this condition.

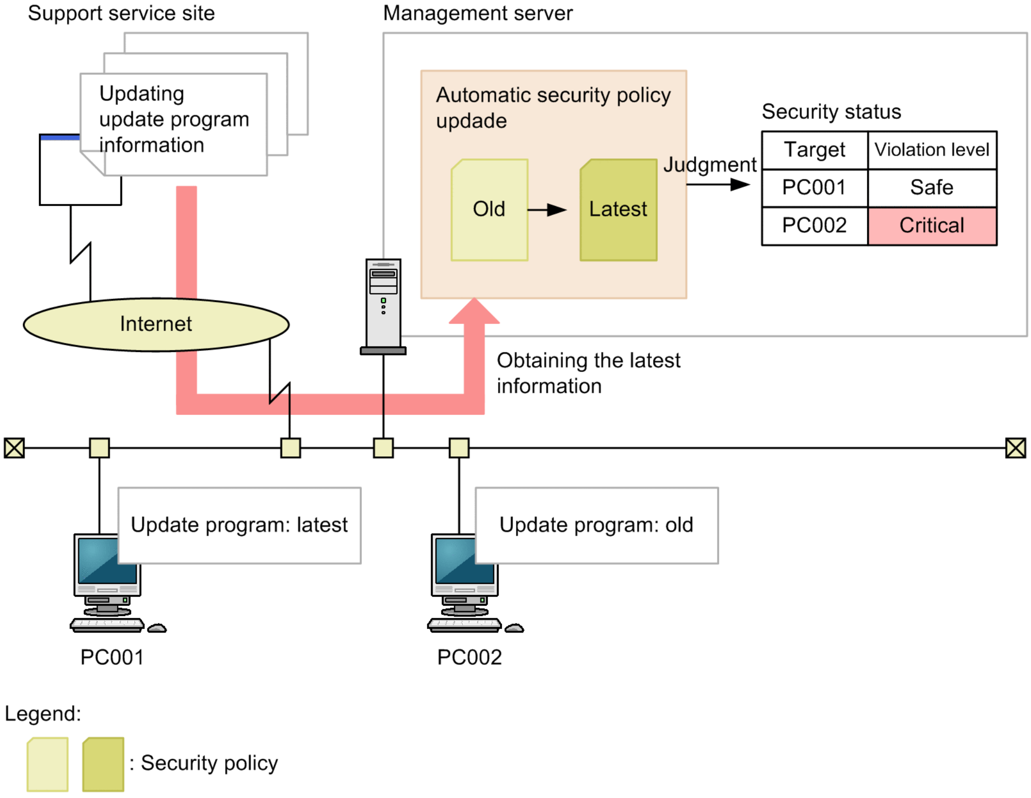
(3) Judging whether updates have been installed

To judge whether the latest updates have been installed on a computer, you must monitor the Microsoft website, determine whether it is necessary to apply judgment for new updates, and register the necessary information. These are troublesome tasks.

If you sign up for support services, the latest Windows Update information can be automatically acquired from the support service site regularly. The acquired Windows Update information is automatically applied to the security policy. Therefore, the administrator can judge whether the latest Windows Update information has been applied to the computer without the need of checking the versions of the updates. Also, depending on the security policy settings, you can distribute and apply the latest Windows Update information to the computers on which the latest updates have not yet been installed.

To automatically acquire the Windows Update information regularly, you must establish connection settings to the support service site and schedule settings for acquiring Windows Update information in the Settings module.

The following figure shows the flow from acquiring the latest Windows Update information to updating the security policy.



> **Tip**
>
> JP1/IT Desktop Management 2 can acquire the latest information about `Critical` or `Important` patches for security problems in Windows or Internet Explorer.

The status of whether updates have been installed is judged to be `All updates are installed` or `Selected updates are installed`. In the security policy, set the Windows Update information to be used when the security is judged.

Related Topics:

- 2.9.6 Managing Windows updates

(4) Judging whether the latest program updates have been installed

You can judge whether the latest program updates have been installed on a computer based on all the program update information registered in the management server. When program update information is added, the listed program updates are added to the judgment targets, so the status of whether the latest program updates have been installed is automatically acquired. You can also specify the program updates that are to be excluded from judgment.

The following table shows the information to be used for judgement.

Information	Description
Latest program update	The latest program update information acquired form the support service site. Specify this to install all program updates. Note that, in the **Update List** view of the Security module, you can check the latest program updates acquired form the support service site.

Information	Description
Program updates to be excluded	Information about the program updates to be excluded from judgment. In the Security module, create a group for the program updates, and then specify that group when you set a security policy.
Device information	Information about the program updates collected from the computer to be judged based on the security policy.

When security is judged, the device information of the computers for which the security policy is applied is compared with the latest program update information acquired from the support service site. If both the document number and the security bulletin number do not match, it is judged that the latest program updates have not been installed, and the violation level defined in the security policy is set. If the program updates that are to be excluded from judgment have not been installed, a violation level is not set.

Tip

If the management server cannot connect to the support service site, connect to the support service site by using a computer that can connect to the external network, and then download the latest support information. If you manually copy the downloaded support information to the management server and then execute the `updatesupportinfo` command, you can register the latest information in the management server. In this way, you can apply the latest program update information to the management server.

(5) Judging whether specified program updates have been installed

The status of whether the program updates have been installed on a computer can be judged based on the update information specified by the administrator. The administrator can specify the service packs and updates for Windows and Internet Explorer as required program updates.

The following table shows the information used for judgment.

Information	Description
Program updates specified by the administrator	Information about the program updates that are judged as dangerous when the service packs and program updates specified by the administrator have not been installed. In the Security module, create a group for the program updates, and then specify that group when you set a security policy.
Device information	Information about the program updates collected form the computers to be judged based on the security policy.

When the security is judged, the device information of the computers for which the security policy is applied is compared with the program update information specified by the administrator. If both the document number and the security bulletin number do not match, it is judged that the program updates specified by the administrator have not been installed, and the violation level defined in the security policy is set. In the same way, if information does not match when the device information of the computer is compared with the service pack information specified by the administrator, it is judged that the program updates specified by the administrator have not been installed, and the violation level defined in the security policy is set.

Related Topics:

- (9) Managing update groups

(6) Judging the settings for Windows automatic update

The following describes the information and judgement conditions used for judgement of the Windows automatic update settings.

Information used for judgment

- Items in the **OS Security** view (under **Security Configuration Items**)
- Items in **Update Details** of the device information (security information)

Judgment conditions

Judgement is performed by comparing the device information with each item set for the security policy, and the violation level is determined depending on the judgment results.

If automated countermeasures are set (Auto Enforce), security measures are taken as necessary.

Related Topics:

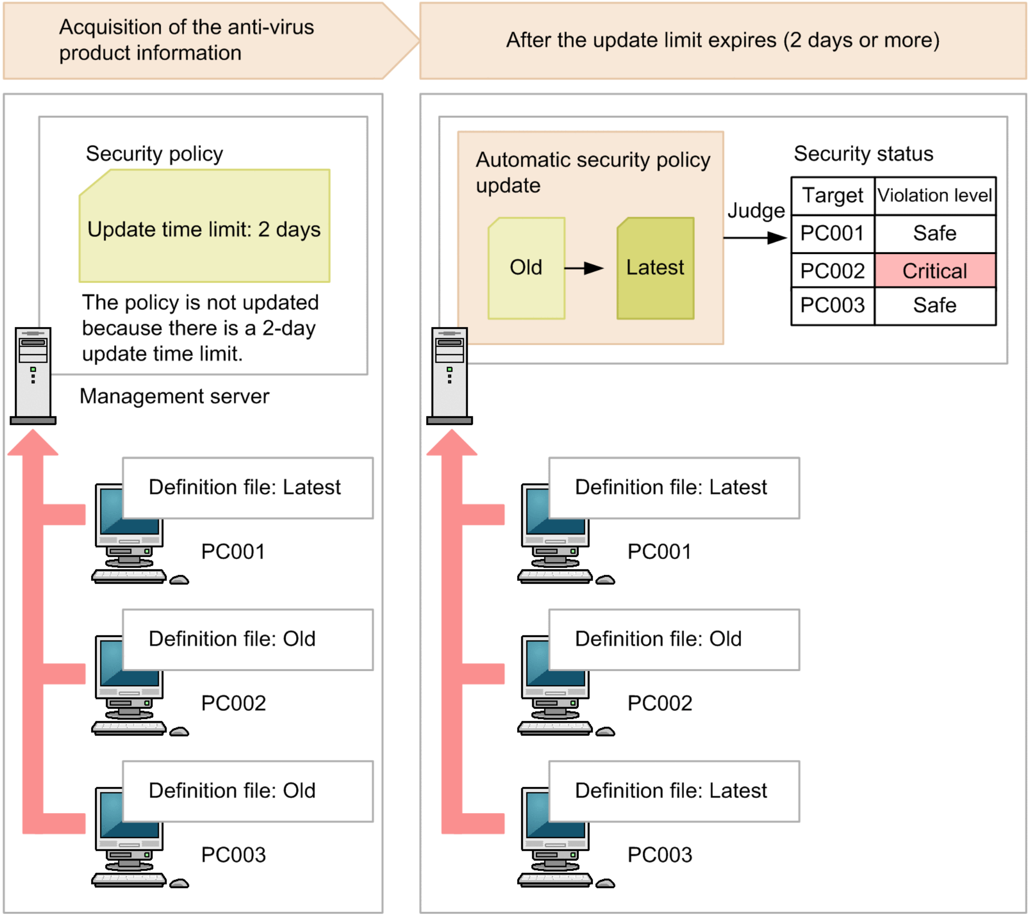
- (14) Supported anti-virus products

(7) Judging the security status for an anti-virus product

When the security status is judged for an anti-virus product, the status of the anti-virus product on each computer is compared with the latest versions of the virus detecting engine and virus definition file over all the computers to which the security policy is applied. Therefore, keep the version of the anti-virus product up to date on at least one managed computer.

However, the versions of anti-virus products on the computers within an organization are not always updated to the latest version at the same time. The latest version and an older version might coexist for a while. For this reason, you can set a grace period (which defines how many days the computer is allowed to stay in the older status) for the security policy.

The following figure shows the flow when judging whether the anti-virus product is up to date.



The security status of a device added as a managed device is judged based on the latest security policy settings. Therefore, if the following conditions exist, the security status is judged to be the violation level specified in the latest policy settings when the device is added as a managed device.

1. The grace period set for the judgment condition of an anti-virus product has expired and the security policy is updated.
2. After the security policy is updated in step 1, a device for which the security status for the anti-virus product is not up to date is added as a managed device.

Supported anti-virus products (anti-virus products to be judged)

For details about the anti-virus products supported by JP1/IT Desktop Management 2, see (14) Supported anti-virus products.

Information used for judgment

- Items in the **Antivirus Software** view (under **Security Configuration Items**)
- **Antivirus Software Details** of the device information (security information)

Judgment conditions

Judgment is performed by comparing the device information with each item set for the security policy. If all the items and the device information match, it is judged to be `Safe`. If there is a mismatch, it is judged as the corresponding violation level that has been set.

If automated countermeasures are set, security measures are taken as necessary.

Related Topics:

- (14) Supported anti-virus products

(8) Judging the security status for prohibited software

The following describes the information and the judgement conditions used for judgment of prohibited software.

Information used for judgment

- Items for prohibited software (in **Security Configuration Items**)
- Items in the device information (installed software information)

Judgment conditions

For prohibited software, the violation level is judged for each installed software program. If an information item set for prohibited software matches the name and version of an installed software program, the software program is judged to have the set violation level. If either of the name or version of an installed software program or both of them do not match any information items set for prohibited software, the software program is judged to be `Safe`. A software name is judged by partial match. A version is judged by Starts-with match.

Note that if prohibited software is not set in **Security Configuration Items**, the software program is judged to be `Safe`.

> **Important note**
>
> If automated countermeasures are set, startup of the relevant software programs might be restricted or the software programs might be uninstalled. Multiple software programs might be the target of the automated countermeasures, because a software name is judged by partial match and a version is judged by Starts-with match.

> **Important note**
>
> Do not specify a software program as both mandatory software and prohibited software when automated countermeasures are set. If you do so, the program will be alternately installed and uninstalled as the security judgments for mandatory software and prohibited software are implemented.

> **Important note**
>
> If a software program that cannot be uninstalled is set as a prohibited software program in **Programs and Features** of the Windows **Control Panel**, uninstallation cannot be performed by automated countermeasures.

(9) Judging the security status for mandatory software

The following describes the information and the judgement conditions used for judgment of mandatory software.

Information used for judgment

- Items in **Software Use** (under **Security Configuration Items**)
- Items for OS information in the device information (system information)
- Items in the device information (installed software information)

Judgment conditions

The judgment targets are the devices whose OS information (OS and service pack) matches one set for mandatory software. For mandatory software, the violation level is judged for each installed software program. If an information item set for mandatory software matches the name and version of an installed software program, the software program is judged to be `Safe`. If either of the name or version of an installed software program or both of them do not match any information items set for mandatory software, the software program is judged to have the set violation level. A software name is judged by partial match. A version is judged by Starts-with match.

Note that if a mandatory program is not set in **Security Configuration Items**, the software program is judged to be `Unknown`.

If automated countermeasures are set, the relevant software programs might be installed as necessary.

Important note

Do not specify a software program as both mandatory software and prohibited software when automated countermeasures are set. If you do so, the program will be alternately installed and uninstalled as the security judgments for mandatory software and prohibited software are implemented.

Important note

If the OS itself is set as mandatory software, installation cannot be performed by automated countermeasures.

(10) Judging the security status for prohibited services

The following describes the information and the judgement conditions used for judgment of prohibited services.

Information used for judgment

- Items in the **Windows Services** view (under **Security Configuration Items**)

Judgment conditions

The violation level is judged for each prohibited service set in the security policy, and determined by the judgment result. If the name of a running service matches a name registered as a prohibited service, the service is judged to have the violation level set in the security policy. If the name does not match, the service is judged to be `Safe`.

If automated countermeasures are set, the relevant service is stopped and disabled as necessary.

If no security policy is assigned to a computer managed offline, the service is judged to be `Safe`

(11) Difference of security judgment between different configurations for management

Whether individual configuration items for security judgment can be judged differs for agent-installed computers and an agentless computers. For agent-installed computers, it also differs for online management and offline management. For agentless computers, it also differs depending on the authentication method.

The following table shows whether judgment is available for individual configuration items for each configuration for management.

Configuration Item		Agent installed	Agentless			
			Administrative Share	SNMP	ARP/ICMP	Active Directory
Windows Update	Automatic Windows Update	Y	Y	N	N	N
	All updates are installed	Y	Y	N	N	N
	Selected updates are installed	Y	Y	N	N	N
Antivirus Software	Install	Y	Y	N	N	N
	Scan Engine Version	Y	Y	N	N	N
	Virus Definition File Version	Y	Y	N	N	N
	Auto Protect	Y	Y	N	N	N
	Last Scanned Date/Time	Y	Y	N	N	N
Software Use	Mandatory Software	Y	Y	N	N	N
	Unauthorized Software	Y	Y	N	N	N
Windows Services		Y #1	N	N	N	N
OS Security	Guest Account	Y	Y	N	N	N
	Password Strength	Y	Y	N	N	N
	Password Never Expires	Y	Y	N	N	N
	Days Since Last Password Change	Y	Y	N	N	N
	Auto Logon	Y	Y	N	N	N
	Power On Password	Y	Y	N	N	N
	Password (Screen Saver)	Y	Y	N	N	N
	Startup Time (Screen Saver)	Y	Y	N	N	N
	Shared Folder	Y	Y	N	N	N
	Administrative Share	Y	Y	N	N	N
	Anonymous Access	Y	Y	N	N	N
	Windows Firewall#2	Y	Y	N	N	N
	DCOM	Y	Y	N	N	N
	Remote Desktop	Y	Y	N	N	N
User-Defined Security Settings		Y	Y	N	N	N

Legend: Y: Can be judged. N: Cannot be judged.

Note: Automated countermeasures for security cannot be performed for offline management and agentless management.

#1: For offline management, the security settings for the services cannot be judged. If no security policy is assigned, the security status is judged to be `Safe`.

#2: The computers for which network monitor is enabled are not judged for Windows firewall.

> **Tip**
>
> For agentless computers, security judgment can be performed only by using authentication through Windows administrative share. Therefore, when you manage the security for an agentless computer, configure the computer so that authentication is performed through Windows administrative share.

Related Topics:

- 2.6.5 Agentless management

(12) Judging user-defined security settings

You can add any policy settings related to the computer's security settings as user-defined security settings to security policies. If you want to perform security judgment using conditions not provided by JP1/IT Desktop Management 2, add user-defined security settings.

When user-defined security settings are added, the security status of the computer is judged based on the specified judgment conditions. If action items are set in a security policy with user-defined security settings added, the system can send messages to the user and control network access based on the violation level indicated by the judgment result. You can view the judgment result of the security status in the **Computer Security Status** view of the Security module.

Overview of security judgment based on user-defined items

Judgment with the user-defined security settings is performed according to the target item, judgment conditions, and judgment value specified for a user-defined item. If the judgment conditions are satisfied, the security status of the device is judged as improper and the violation level changes to the value specified for **Violation level**. Note that a violation level other than **Violation level** can also be specified for devices for which the target item has no value.

Target item

The target item for the security judgment. If there are multiple data items for the target item, judgment is performed if at least one of them meets a judgment condition. The judgment result of the data item that first meets a condition will be displayed.

The target items you can select are system information in device information, hardware information in device information, and management items for hardware asset information added by the system administrator. For details about the target items that can be specified, see (1) Items that can be set for a security policy.

Judgment condition

The condition that the target item value compared with the judgment value must satisfy to judge the security status as improper.

Judgment value

The value that is compared with the value for the target item to determine whether the security status for the item is improper.

Example of setting the user-defined item

The following provides an example of setting the user-defined item to prohibit users with administrator permissions from logging on, and judge the security status to be Critical if a violation is detected.

User-defined item	Setting example
User-defined item name	Prohibit Administrator permission

User-defined item		Setting example
Definition	Type of device information	System information
	Target item	Name of the last logon user
	Judgment condition	Equals the judgment value
	Judgment value	Administrator
	Action when target item has no value	Safe
Violation level		Critical

Judgment conditions and judgment values that can be specified for user-defined items

Judgment conditions and judgment values that can be specified for user-defined items vary depending on the data type of the target item. The following table lists the judgment conditions and judgment values that can be specified for each data type of the target item.

Data type of the target item	Judgment condition	Judgment value
Text	Equals the judgment value	Character string The specified value is case sensitive. Single-byte characters are distinguished from double-byte characters during judgment.
	Does not equal the judgment value	
	Contains the judgment value	
	Begins with the judgment value	
	Ends with the judgment value	
Number	Equals the judgment value	Numbers from 0 to 9, and a decimal point (.) The following units can also be used to specify a value. • B (byte) • KB (kilobyte) • MB (megabyte) • GB (gigabyte) • TB (terabyte) • PB (petabyte) • Minute
	Does not equal the judgment value	
	Equal to or greater than the judgment value	
	Less than or equal to the judgment value	
	Greater than the judgment value	
	Less than the judgment value	
Enumeration	Equals the judgment value	Values displayed in the pull-down menu The specified value is case sensitive. Single-byte characters are distinguished from double-byte characters during judgment.
	Does not equal the judgment value	

(13) Security judgment for user accounts

When multiple user accounts are registered in an OS, some OS settings are defined for each user account. For certain setting items, the security status can be judged for each user account. This enables you to extract problematic user accounts (regarding security) and secure the computers.

The following items are judged for each user account:

- Safety of the password
- Number of days passed since the password was changed

- Password protection for the screen saver
- Waiting time before the screen saver starts

For these items, if all user accounts are in adequate status, the violation level of the device becomes `Safe`. If there is a problem with a user account, the violation level of the device changes to inadequate status. If the status is inadequate, the problematic user accounts are displayed in the **Computer Security Status** view (under the Security module). If automated countermeasures are set for a security policy, countermeasures are enforced only for the problematic user accounts.

Important note

Security judgment is not performed for user accounts in either of the following statuses because password information cannot be collected for those user accounts:

- Disabled user accounts
- Locked-out user accounts

In addition, security judgment for the screen saver is not performed for the following user accounts because information about the screen saver cannot be acquired for those accounts:

- User accounts that have not been logged in for 30 days or more since the last login

If message notification is set in **Action Items** for a security policy, a message prompting you to enforce countermeasures may be automatically displayed depending on the violation level. All user accounts receive the message. However, for the items that are judged for each user account, the description of the countermeasures is added only to the message for the problematic user accounts.

(14) Supported anti-virus products

JP1/IT Desktop Management 2 supports the anti-virus products shown below. The security status can be judged only for those anti-virus products.

Important note

The products and versions shown below are the ones as of the release of the JP1/IT Desktop Management 2 product this manual covers.

You can check the latest information about supported anti-virus products on the support service site.

Tip

You can view the product versions shown below on the **Installed Software Details** tab of the **Device Inventory** view.

Tip

The security status cannot be judged for unsupported anti-virus products. However, whether a product has been installed can be judged if the product is registered as mandatory software in the security policy.

Anti-virus products for which information can be collected

Japanese versions of anti-virus products

Product name and version			Name displayed in the operation window
Norton AntiVirus[#1, #2, #3]	2005		Norton AntiVirus 2005
	2006		Norton AntiVirus 2006
	2007		Norton AntiVirus 2007
	2008	32-bit	Norton AntiVirus 2008
		64-bit	Norton AntiVirus 2008 64-bit
	2009	32-bit	Norton AntiVirus 2009
		64-bit	Norton AntiVirus 2009 64-bit
	2010	32-bit	Norton AntiVirus 2010
		64-bit	Norton AntiVirus 2010 64-bit
	2011	32-bit	Norton AntiVirus 2011
		64-bit	Norton AntiVirus 2011 64-bit
	2012	32-bit	Norton AntiVirus 2012
		64-bit	Norton AntiVirus 2012 64-bit
	32-bit		Norton AntiVirus
	64-bit		Norton AntiVirus 64-bit
	2014	32-bit	Norton AntiVirus 2014
		64-bit	Norton AntiVirus 2014 64-bit
Symantec AntiVirus Corporate Edition	10.0	32-bit	Symantec AntiVirus Corporate Edition 10.0
		64-bit	Symantec AntiVirus 64-bit
	10.1	32-bit	Symantec AntiVirus Corporate Edition 10.1
		64-bit	Symantec AntiVirus 64-bit
	10.2	32-bit	Symantec AntiVirus Corporate Edition 10.2
		64-bit	Symantec AntiVirus 64-bit
Symantec Client Security	3.0	32-bit	Symantec Client Security
		64-bit	Symantec AntiVirus 64-bit
	3.1	32-bit	Symantec Client Security
		64-bit	Symantec AntiVirus 64-bit
Symantec Endpoint Protection	11.0	32-bit	Symantec Endpoint Protection 11.0
		64-bit	Symantec Endpoint Protection 11.0 64-bit
	12.1 (12.1.4)	32-bit	Symantec Endpoint Protection 12.1
		64-bit	Symantec Endpoint Protection 12.1 64-bit
McAfee Total Protection Service[#2, #3]	5.0		McAfee Total Protection Service

Product name and version			Name displayed in the operation window
McAfee SaaS Endpoint Protection[#3]	5.2		McAfee SaaS Endpoint Protection
	6.0	32-bit	McAfee SaaS Endpoint Protection
		64-bit	McAfee SaaS Endpoint Protection 64-bit
McAfee VirusScan Enterprise	8.5i	32-bit	McAfee VirusScan Enterprise 8.5i
		64-bit	McAfee VirusScan Enterprise 8.5i 64-bit
	8.7i	32-bit	McAfee VirusScan Enterprise 8.7i
		64-bit	McAfee VirusScan Enterprise 8.7i 64-bit
	8.8	32-bit	McAfee VirusScan Enterprise 8.8
		64-bit	McAfee VirusScan Enterprise 8.8 64-bit
ウイルスバスター	2011 クラウド[#3]	32-bit	ウイルスバスター 2011 クラウド
		64-bit	ウイルスバスター 2011 クラウド 64-bit
	2012 クラウド[#3]	32-bit	ウイルスバスター 2012 クラウド
		64-bit	ウイルスバスター 2012 クラウド 64-bit
ウイルスバスター クラウド[#3]	32-bit		ウイルスバスター クラウド
	64-bit		ウイルスバスター クラウド 64-bit
	7.0	32-bit	ウイルスバスター クラウド 7.0
		64-bit	ウイルスバスター クラウド 7.0 64-bit
ウイルスバスター コーポレートエディション	8.0[#3], 10.0[#3], 10.5[#4], 10.6	32-bit	For the 32-bit version of Windows: ウイルスバスター Corp. For the 64-bit version of Windows: ウイルスバスター Corp. 64-bit
		64-bit	
ウイルスバスター コーポレートエディション アドバンス	8.0[#3], 10.0[#3]	32-bit	
		64-bit	
ウイルスバスター コーポレートエディション サーバ版	8.0[#3], 10.0[#3]	32-bit	
		64-bit	
ウイルスバスター コーポレートエディション サーバ版 アドバンス	8.0[#3], 10.0[#3]	32-bit	
		64-bit	
Trend Micro ビジネスセキュリティ[#3]	6.0	32-bit	For the 32-bit version of Windows: ビジネスセキュリティクライアント For the 64-bit version of Windows: ビジネスセキュリティクライアント 64-bit
		64-bit	
ウイルスバスター ビジネスセキュリティ[#3]	7.0	32-bit	
		64-bit	
	9.0	32-bit	
		64-bit	
ServerProtect for Windows NT/NetWare[#5]	5.7	32-bit	For the 32-bit version of Windows: ServerProtect For the 64-bit version of Windows: ServerProtect 64-bit
		64-bit	
	5.8	32-bit	
		64-bit	

Product name and version			Name displayed in the operation window
Forefront Client Security#3	1.5.1937.14, 1.5.1993.0, 1.5.1996.1	32-bit	Forefront Client Security
		64-bit	Forefront Client Security 64-bit
Kaspersky Open Space Security Server#6	6.0.4	32-bit	Kaspersky Anti-Virus 6.0 for Windows Workstations
		64-bit	Kaspersky Anti-Virus 6.0 for Windows Workstations 64-bit
Kaspersky Open Space Security Workstation#6	6.0.4	32-bit	Kaspersky Anti-Virus 6.0 for Windows Servers
		64-bit	Kaspersky Anti-Virus 6.0 for Windows Servers 64-bit
Kaspersky Endpoint Security 8 for Windows#6	8	32-bit	For the 32-bit version of Windows: Kaspersky Endpoint Security 8 for Windows For the 64-bit version of Windows: Kaspersky Endpoint Security 8 for Windows 64-bit
		64-bit	
	8.1	32-bit	
		64-bit	
Kaspersky Endpoint Security 10 for Windows#2, #6	10.2	32-bit	For the 32-bit version of Windows: Kaspersky Endpoint Security 10 for Windows For the 64-bit version of Windows: Kaspersky Endpoint Security 10 for Windows 64bit
		64-bit	
ESET Endpoint Antivirus#1, #2, #3	5.0	32-bit	ESET Endpoint Antivirus
		64-bit	ESET Endpoint Antivirus 64-bit
ESET File Security for Microsoft Windows Server#1, #2, #3	4.5	32-bit	ESET File Security for Microsoft Windows Server
		64-bit	ESET File Security for Microsoft Windows Server 64-bit
ESET NOD32 Antivirus#1, #2, #3	4.0	32-bit	For the 32-bit version of Windows: ESET NOD32 Antivirus For the 64-bit version of Windows: ESET NOD32 Antivirus 64-bit
		64-bit	
	4.2	32-bit	
		64-bit	
	5.0	32-bit	
		64-bit	
	5.2	32-bit	
		64-bit	
	6.0	32-bit	For the 32-bit version of Windows: Sophos Anti-Virus For the 64-bit version of Windows: Sophos Anti-Virus 64-bit
		64-bit	
	7.0	32-bit	
		64-bit	
Sophos Endpoint Security and Data Protection	9.0	32-bit	
		64-bit	
	9.5	32-bit	
		64-bit	
Sophos Security Suite small business solutions	4.0	32-bit	

Product name and version			Name displayed in the operation window
Sophos Computer Security small business solutions	4.0	64-bit	For the 32-bit version of Windows: Sophos Anti-Virus For the 64-bit version of Windows: Sophos Anti-Virus 64-bit
Sophos Anti-Virus small business solutions			
Sophos Endpoint Protection - Enterprise	10	32-bit	
		64-bit	
Sophos Endpoint Protection - Advanced		32-bit	
		64-bit	
Sophos Endpoint Protection - Basic		32-bit	
		64-bit	
Sophos Endpoint Security and Control for Windows	10.3	32-bit	
		64-bit	
	10.3.7	32-bit	For the 32-bit version of Windows: Sophos Anti-Virus 10.3.7 For the 64-bit version of Windows: Sophos Anti-Virus 10.3.7 64-bit
		64-bit	
F-Secure Client Security[#1, #2, #3]	9.0	32-bit	For the 32-bit version of Windows: F-Secure Client Security For the 64-bit version of Windows: F-Secure Client Security 64-bit
		64-bit	
	9.1	32-bit	
		64-bit	
	9.11	32-bit	
		64-bit	
	9.20	32-bit	
		64-bit	
	9.31	32-bit	
		64-bit	
	9.32	32-bit	
		64-bit	
	11.50	32-bit	
		64-bit	
	11.60	32-bit	
		64-bit	

#1: The version of the virus search engine cannot be collected.

#2: The status for Auto Protect (resident setting) cannot be collected.

#3: The last scanned date and time cannot be collected.

#4: The last scanned date and time can be collected only when Patch 1 or later has been applied.

#5: If the scan was canceled, the date and time the scan was canceled is collected as the last scanned date and time.

#6: If a complete scan is performed, the last scanned date and time can be collected only when all hard disks, system memory, and startup objects are scanned.

English versions of anti-virus products

Product name and version			Name displayed in the operation window
Norton AntiVirus[#1, #2, #3]	2010	32-bit	Norton AntiVirus 2010
		64-bit	Norton AntiVirus 2010 64-bit
	2011	32-bit	Norton AntiVirus 2011
		64-bit	Norton AntiVirus 2011 64-bit
	32-bit		Norton AntiVirus
	64-bit		Norton AntiVirus 64-bit
Symantec AntiVirus Corporate Edition	10.0	32-bit	Symantec AntiVirus Corporate Edition 10.0
		64-bit	Symantec AntiVirus 64-bit
	10.1	32-bit	Symantec AntiVirus Corporate Edition 10.1
		64-bit	Symantec AntiVirus 64-bit
	10.2	32-bit	Symantec AntiVirus Corporate Edition 10.2
		64-bit	Symantec AntiVirus 64-bit
Symantec Client Security	3.0	32-bit	Symantec Client Security
		64-bit	Symantec AntiVirus 64-bit
	3.1	32-bit	Symantec Client Security
		64-bit	Symantec AntiVirus 64-bit
Symantec Endpoint Protection	11.0	32-bit	Symantec Endpoint Protection 11.0
		64-bit	Symantec Endpoint Protection 11.0 64-bit
	12.1	32-bit	Symantec Endpoint Protection 12.1
		64-bit	Symantec Endpoint Protection 12.1 64-bit
McAfee Total Protection Service[#2, #3]	5.0		McAfee Total Protection Service
McAfee SaaS Endpoint Protection[#3]	5.2		McAfee SaaS Endpoint Protection
McAfee VirusScan Enterprise	8.5i	32-bit	McAfee VirusScan Enterprise 8.5i
		64-bit	McAfee VirusScan Enterprise 8.5i 64-bit
	8.7i	32-bit	McAfee VirusScan Enterprise 8.7i
		64-bit	McAfee VirusScan Enterprise 8.7i 64-bit
	8.8	32-bit	McAfee VirusScan Enterprise 8.8
		64-bit	McAfee VirusScan Enterprise 8.8 64-bit
PC-cillin	2010	32-bit	PC-cillin 2010
		64-bit	PC-cillin 2010 64-bit
Titanium Internet Security[#3]	2011	32-bit	Titanium Internet Security 2011
		64-bit	Titanium Internet Security 2011 64-bit

Product name and version			Name displayed in the operation window
Titanium Internet Security[#3]	2012	32-bit	Titanium Internet Security 2012
		64-bit	Titanium Internet Security 2012 64-bit
	2013	32-bit	Titanium Internet Security 2013
		64-bit	Titanium Internet Security 2013 64-bit
Worry-Free Business Security-Standard	7.0[#1, #2, #3, #4], 8.0[#3]	32-bit	For the 32-bit version of Windows: Worry-Free Business Security For the 64-bit version of Windows: Worry-Free Business Security 64-bit
		64-bit	
Worry-Free Business Security-Advanced	7.0[#1, #2, #3, #4], 8.0[#3]	32-bit	
		64-bit	
OfficeScan Corporate Edition	8.0[#3], 10[#3], 10.5[#5], 10.6	32-bit	For the 32-bit version of Windows: OfficeScan Corp. For the 64-bit version of Windows: OfficeScan Corp. 64-bit
		64-bit	
ServerProtect for Windows NT/Netware	5.7	32-bit	For the 32-bit version of Windows: ServerProtect For the 64-bit version of Windows: ServerProtect 64-bit
		64-bit	
	5.8	32-bit	
		64-bit	
Forefront Client Security[#3]	1.5.1937.14, 1.5.1993.0, 1.5.1996.1	32-bit	Forefront Client Security
		64-bit	Forefront Client Security 64-bit
Kaspersky Open Space Security Server	6.0.3[#1, #2, #3], 6.0.4[#6]	32-bit	Kaspersky Anti-Virus 6.0 for Windows Servers
		64-bit	Kaspersky Anti-Virus 6.0 for Windows Servers 64-bit
Kaspersky Open Space Security Workstation		32-bit	Kaspersky Anti-Virus 6.0 for Windows Workstations
		64-bit	Kaspersky Anti-Virus 6.0 for Windows Workstations 64-bit
Kaspersky Endpoint Security 8 for Windows	8, 8.1	32-bit	For the 32-bit version of Windows: Kaspersky Endpoint Security 8 for Windows For the 64-bit version of Windows: Kaspersky Endpoint Security 8 for Windows 64-bit
		64-bit	
ESET NOD32 Antivirus[#1, #2, #3]	4.0, 4.2, 5.0, 5.2	32-bit	ESET NOD32 Antivirus
		64-bit	ESET NOD32 Antivirus 64-bit
Sophos Endpoint Security and Data Protection	9.0, 9.5	32-bit	For the 32-bit version of Windows: Sophos Anti-Virus For the 64-bit version of Windows: Sophos Anti-Virus 64-bit
		64-bit	
Sophos Security Suite small business solutions	4.0	32-bit	
Sophos Computer Security small business solutions		64-bit	
Sophos Anti-Virus small business solutions			
Sophos Endpoint Protection - Enterprise	10	32-bit	
		64-bit	

Product name and version			Name displayed in the operation window
Sophos Endpoint Protection - Advanced	10	32-bit	For the 32-bit version of Windows: Sophos Anti-Virus For the 64-bit version of Windows: Sophos Anti-Virus 64-bit
		64-bit	
Sophos Endpoint Protection - Basic	10	32-bit	
		64-bit	
F-Secure Client Security[#1, #2, #3]	9.0, 9.31, 9.32	32-bit	For the 32-bit version of Windows: F-Secure Client Security For the 64-bit version of Windows: F-Secure Client Security 64-bit
		64-bit	

#1: The version of the virus search engine cannot be collected.

#2: The status for Auto Protect (resident setting) cannot be collected.

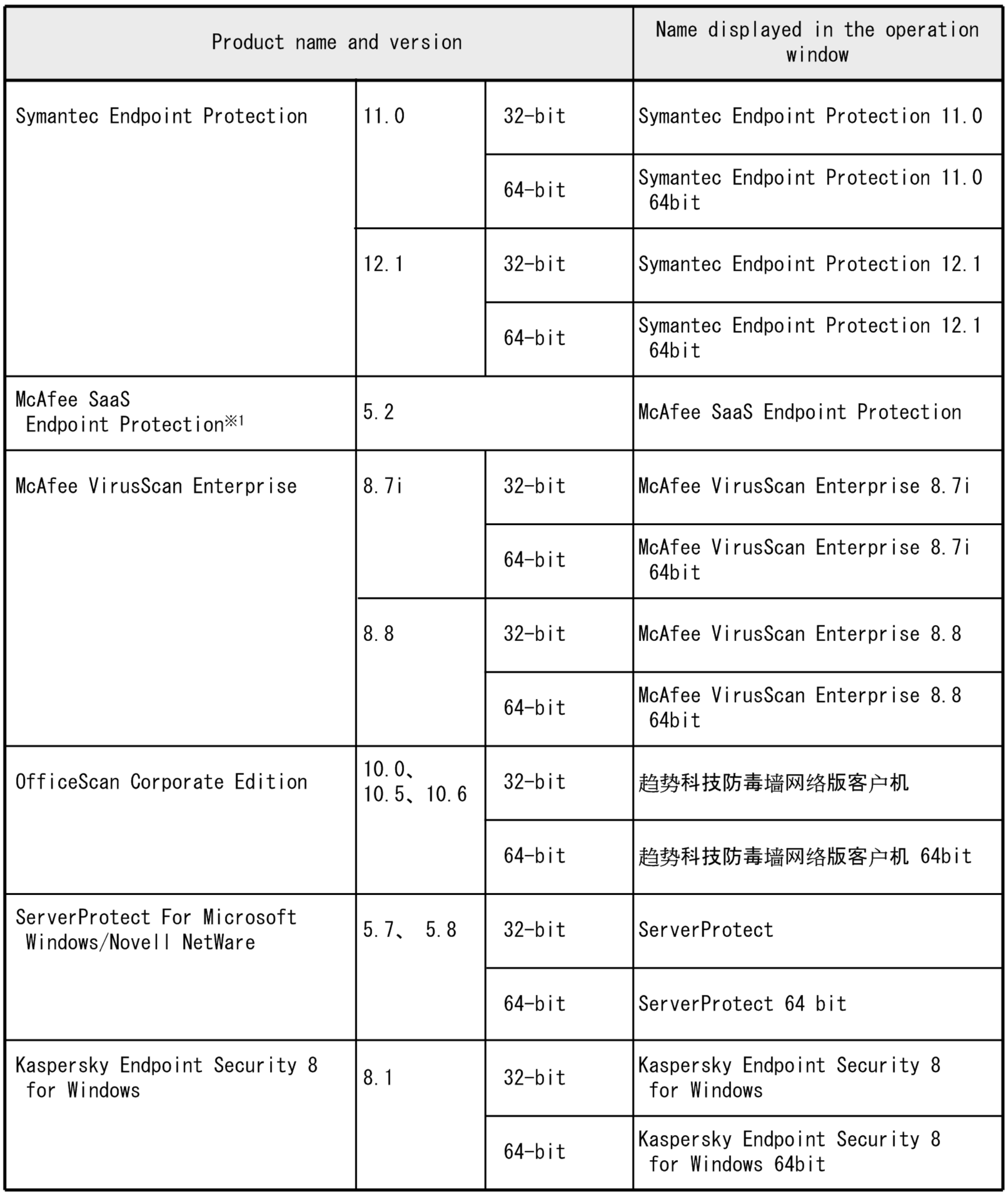
#3: The last scanned date and time cannot be collected.

#4: The version of the virus definition file cannot be collected.

#5: The last scanned date and time can be collected only when Patch 1 or later has been applied.

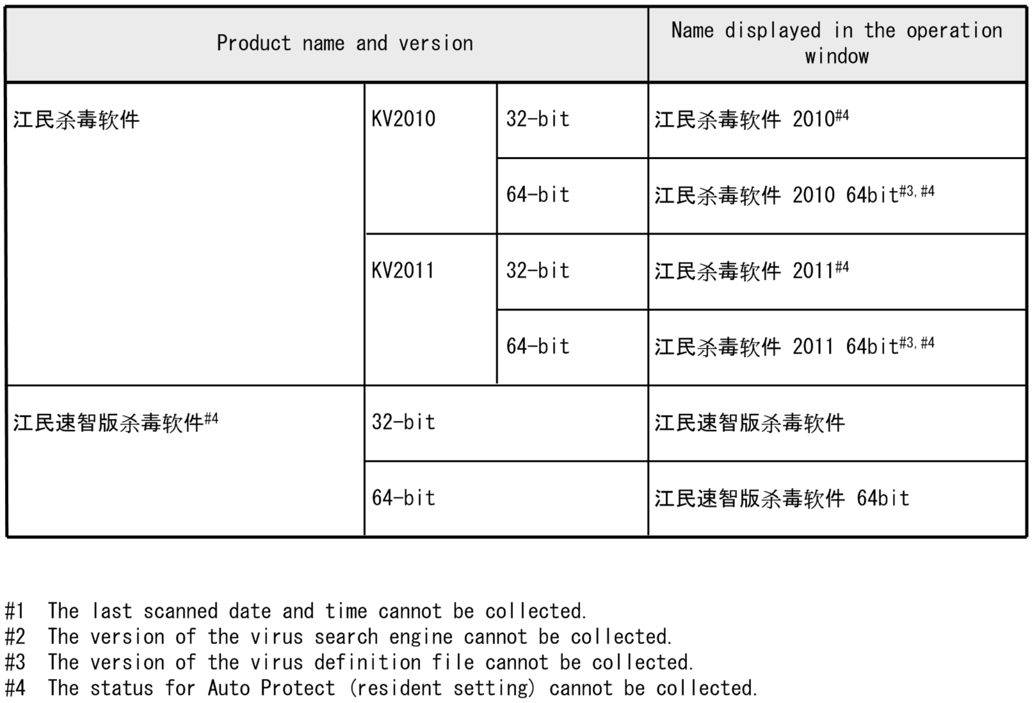
#6: If a complete scan is performed, the last scanned date and time can be collected only when all hard disks, system memory, and startup objects are scanned.

Chinese versions of anti-virus products



Product name and version			Name displayed in the operation window
Symantec Endpoint Protection	11.0	32-bit	Symantec Endpoint Protection 11.0
		64-bit	Symantec Endpoint Protection 11.0 64bit
	12.1	32-bit	Symantec Endpoint Protection 12.1
		64-bit	Symantec Endpoint Protection 12.1 64bit
McAfee SaaS Endpoint Protection※1	5.2		McAfee SaaS Endpoint Protection
McAfee VirusScan Enterprise	8.7i	32-bit	McAfee VirusScan Enterprise 8.7i
		64-bit	McAfee VirusScan Enterprise 8.7i 64bit
	8.8	32-bit	McAfee VirusScan Enterprise 8.8
		64-bit	McAfee VirusScan Enterprise 8.8 64bit
OfficeScan Corporate Edition	10.0、10.5、10.6	32-bit	趋势科技防毒墙网络版客户机
		64-bit	趋势科技防毒墙网络版客户机 64bit
ServerProtect For Microsoft Windows/Novell NetWare	5.7、 5.8	32-bit	ServerProtect
		64-bit	ServerProtect 64 bit
Kaspersky Endpoint Security 8 for Windows	8.1	32-bit	Kaspersky Endpoint Security 8 for Windows
		64-bit	Kaspersky Endpoint Security 8 for Windows 64bit

Product name and version			Name displayed in the operation window
卡巴斯基 网络版 Server	6.0.3#1,#2,#3	Server 32-bit	卡巴斯基反病毒 6.0 Windows 服务器
		Server 64-bit	卡巴斯基反病毒 6.0 Windows 服务器 64bit
		Workstation 32-bit	卡巴斯基反病毒 6.0 Windows 工作站
		Workstation 64-bit	卡巴斯基反病毒 6.0 Windows 工作站 64bit
	6.0.4	Server 32-bit	卡巴斯基反病毒 6.0 Windows 服务器
		Server 64-bit	卡巴斯基反病毒 6.0 Windows 服务器 64bit
		Workstation 32-bit	卡巴斯基反病毒 6.0 Windows 工作站
		Workstation 64-bit	卡巴斯基反病毒 6.0 Windows 工作站 64bit
瑞星杀毒软件网络版#1,#2,#3,#4	2010,2011,2012	32-bit	瑞星杀毒软件网络版
		64-bit	瑞星杀毒软件网络版 64bit
金山毒霸#1,#2,#4	2011	32-bit	金山毒霸 2011
		64-bit	金山毒霸 2011 64bit
	2012	32-bit	金山毒霸 2012
		64-bit	金山毒霸 2012 64bit
新毒霸#1,#2,#4	2013	32-bit	新毒霸 2013
		64-bit	新毒霸 2013 64bit



Product name and version			Name displayed in the operation window
江民杀毒软件	KV2010	32-bit	江民杀毒软件 2010[#4]
		64-bit	江民杀毒软件 2010 64bit[#3,#4]
	KV2011	32-bit	江民杀毒软件 2011[#4]
		64-bit	江民杀毒软件 2011 64bit[#3,#4]
江民速智版杀毒软件[#4]	32-bit		江民速智版杀毒软件
	64-bit		江民速智版杀毒软件 64bit

#1 The last scanned date and time cannot be collected.
#2 The version of the virus search engine cannot be collected.
#3 The version of the virus definition file cannot be collected.
#4 The status for Auto Protect (resident setting) cannot be collected.

Judgment conditions for Auto Protect (resident setting) of anti-virus products

You can collect the status of Auto Protect (resident setting) from most anti-virus products. The status of whether an anti-virus product is resident or non-resident is judged by the setting of the anti-virus product. The following shows the judgment conditions for whether anti-virus products are resident or non-resident.

Japanese versions of anti-virus products

Product name	Condition for judging whether the product is resident or non-resident
Norton AntiVirus	--
Symantec AntiVirus Corporate Edition	The product is resident when **Auto-Protect** を有効にする is on.
Symantec Client Security	
Symantec Endpoint Protection	The product is resident when ファイルシステム **Auto-Protect** を有効にする is on.
McAfee Total Protection Service	--
McAfee SaaS EndpointProtection	The product is resident when オンアクセススキャン is enabled.
McAfee VirusScan Enterprise	The product is resident when システム起動時にオンアクセススキャンを有効にする is on.
ウイルスバスター	The product is resident when リアルタイム検索 is on.
ウイルスバスター 2011 クラウド	The product is resident when ウイルス/スパイウェアの監視 is on.
ウイルスバスター コーポレートエディション	If ウイルス/不正プログラム検索を有効にする (ウィルス検索を有効にする for version 8.0, or リアルタイム検索を有効にする for version 10.0) is set to off in リアルタイム検索の設定 on the management server running ウイルスバスター コーポレートエディション and then the settings are applied to the clients, real-time scan on the clients stops. At this time, the product becomes non-resident.
ウイルスバスター コーポレートエディション アドバンス	If リアルタイム検索を有効にする (ウィルス検索を有効にする for version 8.0) is set to off in リアルタイム検索の設定 on the management server running ウイルスバスター コーポレート

Product name	Condition for judging whether the product is resident or non-resident
ウイルスバスター コーポレートエディション サーバ版	エディション and then the settings are applied to the clients, real-time scan on the clients stops. At this time, the product becomes non-resident.
ウイルスバスター コーポレートエディション サーバ版 アドバンス	
ビジネスセキュリティ	If リアルタイムのウイルス対策/スパイウェア対策を有効にする is set to off in the security settings and the settings are applied to a computer, real-time scan on the computer stops. At this time, the product becomes non-resident.
ServerProtect for Windows NT/ Netware	If リアルタイム検索を有効にする is set to off in リアルタイム検索 on the information server and the settings are applied to general servers, real-time scan on general servers stops. At this time, the product becomes non-resident.
Forefront Client Security	The product is resident when リアルタイム保護を使用する is on.
Kaspersky Open Space Security Server	The product is resident when プロテクションを有効にする is on.
Kaspersky Open Space Security Workstation	The product is resident when プロテクションを有効にする is on.
ESET NOD32 Antivirus	--
Sophos Endpoint Security and Data Protection	The product is resident when このコンピュータでオンアクセス検索を実行する is on.
Sophos Security Suite small business solutions	
Sophos Computer Security small business solutions	
Sophos Anti-Virus small business solutions	
F-Secure Client Security	--

Legend: --: The status of whether the product is resident or non-resident cannot be collected.

English versions of anti-virus products

Product name	Condition for judging whether the product is resident or non-resident
Norton AntiVirus	--
Symantec AntiVirus Corporate Edition	The product is resident when **Enable Auto-Protect** is on.
Symantec Client Security	
Symantec Endpoint Protection	The product is resident when **Enable File System Auto-Protect** is on.
McAfee Total Protection Service	--
McAfee SaaS EndpointProtection	The product is resident when **On-access scanning** is on.
McAfee VirusScan Enterprise	The product is resident when **Enable on-access scanning at system startup** is on.
OfficeScan Corporate Edition	For version 8.0, 10, 10.5, or 10.5Patch1, the product is resident when **Enable virus/malware scan** is on. For version 10.6, if **Enable virus/malware scan** is set to off in **Real-time Scan Settings** on the management server and the settings are applied to client, real-time scan on client stops. At this time, the product becomes non-resident.
PC-cillin	The product is resident when **Protection Against Viruses & Spyware** is on.

Product name	Condition for judging whether the product is resident or non-resident
Titanium Internet Security	The product is resident when **Protection Against Viruses & Spyware** is on.
Worry-Free Business Security-Standard	The product is resident when **Enable real-time Antivirus/Anti-spyware** is on (for version 8.0).
Worry-Free Business Security-Advanced	
OfficeScan Corporate Edition	The product is resident when **Enable virus/malware scan** is on.
ServerProtect for Windows NT/Netware	If **Enable Real-time Scan** is set to off in **Real-time Scan** on the information server and the settings are applied to general servers, real-time scan on general servers stops. At this time, the product becomes non-resident.
Forefront Client Security	The product is resident when **Use real time protection** is on.
Kaspersky Open Space Security Server	The product is resident when **Enable File Anti-Virus** is on (for version 6.0.3) or when **Enable protection** is on (for version 6.0.4).
Kaspersky Open Space Security Workstation	The product is resident when **Enable File Anti-Virus** is on (for version 6.0.3) or when **Enable protection** is on (for version 6.0.4).
Kaspersky Endpoint Security 8 for Windows	The product is resident when **Pause** of **Pause protection and control** is off.
ESET NOD32 Antivirus	--
Sophos Endpoint Security and Data Protection	The product is resident when **Enable on-access scanning for this computer** is on.
Sophos Security Suite small business solutions	
Sophos Computer Security small business solutions	
Sophos Anti-Virus small business solutions	
Sophos Endpoint Protection - Enterprise	
Sophos Endpoint Protection - Advanced	
Sophos Endpoint Protection - Basic	
F-Secure Client Security	--

Legend: --: The status of whether the product is resident or non-resident cannot be collected.

Chinese versions of anti-virus products

Product name	Condition for judging whether the product is resident or non-resident
Symantec Endpoint Protection	The product is resident when 启用文件系统自动防护 is on.
McAfee SaaS Endpoint Protection	The product is resident when 按访问扫描 is on.
McAfee VirusScan Enterprise	The product is resident when 启用在系统启动时进行按访问扫描 is on.
OfficeScan Corporate Edition	For version 8.0, 10, 10.5, or 10.5Patch1, the product is resident when 启用病毒/恶意软件扫描 is on. For version 10.6, if 启用病毒/恶意软件扫描 is set to off in 实时扫描设置 on the management server and the settings are applied to client, real-time scan on client stops. At this time, the product becomes non-resident.
ServerProtect for Microsoft Windows/Novell NetWare	If 启用实时扫描 is set to off in 实时扫描 on the information server and the settings are applied to general servers, real-time scan on general servers stops. At this time, the product becomes non-resident.
Kaspersky Endpoint Security 8 for Windows	The product is resident when 暂停 of 暂停保护和控制 is off.
卡巴斯基 网络版	The product is resident when 启用保护 is on.
瑞星杀毒软件网络版	—
金山毒霸	—
新毒霸	—
江民杀毒软件	—
江民速智版杀毒软件	—

Legend: --: The status of whether the product is resident or non-resident cannot be collected.

(15) Excluding user accounts from security status judgment targets

If multiple user accounts are registered in an OS, the security status is judged for each user account for the following security configuration items:

- Safety of the password
- Password never expires
- Number of days passed since the password was changed
- Password protection for the screen saver
- Waiting time before the screen saver starts

OS user accounts might be automatically created depending on the components of the OS or on certain programs. The security status might not be correctly managed if the security status is also judged for such unused user accounts.

In such a case, you can create a judgment-excluded user settings file so that certain user accounts will not be judged.

Tip

JP1/IT Desktop Management 2 automatically excludes some user accounts that are automatically created, from the judgment targets. If an unknown user account has been judged when you check the security status, create a judgment-excluded user settings file.

(16) Format of a user settings file excluded from security status judgment

Specify the file name as follows: jdn_except_users.dat.

Create a user settings file excluded from security status judgment in the following format:

OS user account name 1

OS user account name 2

Specify a single user account name for each line. To specify multiple user accounts, you can specify them by using multiple lines.

For a user account name, specify a character string not exceeding 20 single-byte characters, which can consist of alphanumeric characters and symbols. Note, however, that the following symbols cannot be used:

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

In addition, you cannot specify a user account name by using only periods (.) or single-byte spaces.

Tip

You can use an asterisk (*) as a wildcard to specify all user account names for which the initial characters match the entered string, for example, HOGE*. You can specify an asterisk (*) only at the end of a character string. User account names consisting only of asterisks (*) are ignored.

2.9.4 Managing a security policy

In the **Security Policies** view of the Security module, create and manage a security policy. This subsection explains security policy management.

Create a security policy.

Create a security policy based on your organization's security principles. You can create multiple security policies. You can create a different security policy for each department or a security policy for computers that require special management.

Assign a security policy to computers.

To keep track of the security status of computers, you need to assign the created security policy to computers or groups.

Edit a security policy.

If the security trends change or your organization's security principles are changed, edit a security policy. Security trends change as the computers and the network environment change. By always incorporating security trends into your organization, you become able to robustly manage the security status.

Delete a security policy.

Delete security policies that are not needed anymore when the management structure has changed or when multiple security policies have been integrated.

(1) Items that can be set for a security policy

The following are the items that can be set for a security policy:

Security Configuration Items

Windows Update

You can judge whether Windows automatic update has been executed properly and whether Windows updates have been installed properly. You can also configure the settings so that countermeasures are automatically enforced when the security status is inadequate.

Antivirus Software

You can judge whether anti-virus products have been properly installed or configured. This item is judged when information necessary for judgment can be collected from the computer.

Software Use

You can judge whether software programs have been properly installed. You can also configure the settings so that countermeasures are automatically enforced when the security status is inadequate.

Windows Services

You can judge whether certain services operate properly. You can also configure the settings so that countermeasures are automatically enforced when the security status is inadequate.

OS Security

You can judge whether the OS security settings (such as OS user accounts, screen saver, and share folders) are adequate. You can also configure the settings so that countermeasures are automatically enforced when the security status is inadequate.

User-Defined Security Settings

You can specify a policy related to the security settings to judge whether the security settings are appropriate based on user-specified conditions.

Other Access Restrictions

You can restrict print operations or the use of devices and software programs. You can also specify so that a user's computer receives a message notifying that the use of the device was restricted.

Operation Logs

You can set the targets for which operation logs are collected and the conditions for operations to be regarded as suspicious.

Common settings for prohibited operations and operation logs

You can set intervals for sending notification of prohibited operations and operation logs to the higher-level system, and the period for which prohibited operations and operation logs are kept on a user's computer.

Action Items

Send User Notification

You can configure the settings so that messages are automatically reported to computers depending on the results of security status judgments.

Network Connection Control

You can configure the settings so that network connection of the computer is automatically controlled depending on the results of security status judgment.

Assigned Groups

Target Group Type

You can set a group of computers to which a security policy is to be assigned. To assign a security policy to individual computers, first create a security policy, and then assign the security policy to the computers from the **Computer Security Status** view in the menu area.

The following table gives details about the items that can be set for a security policy.

Security Configuration Items

Configuration item		Description	Automated countermeasures
Windows Update	Automatic Windows Update	You can judge whether Windows automatic update is enabled. To make sure that the latest Windows updates are installed, we recommend that you enable automatic update. By making sure that Windows automatic update is enabled, you can make sure that the Windows updates are properly installed.	Y[#1]
	All updates are installed	You can judge whether Windows updates have been installed. By checking whether the updates have been installed, you can understand whether the OS status is latest and proper.	Y
	Selected updates are installed		
Antivirus Software	Install	You can judge whether an anti-virus product supported by JP1/IT Desktop Management 2 has been installed. If one of the products set in a security policy has been installed on a computer, the computer is judged to have a supported anti-virus product installed.	--
	Scan Engine Version	You can judge whether the latest version of the anti-virus scan engine is being used. You can set an update time limit, which is the period of time allowed after the latest version is detected and until the scan engine is updated. During the update time limit, even if an older version of the scan engine is used, the security status is judged as adequate.	
	Virus Definition File Version	You can judge whether the most up-to-date virus definition file is being used. You can set an update time limit, which is the period of time allowed after the latest version is detected and until the virus definition file is updated. During the update time limit, even if an older version of the virus definition file is used, the security status is judged as adequate.	
	Auto Protect	You can judge whether the auto protect setting (resident setting) is enabled.	
	Last Scanned Date/Time	You can judge whether the last virus-scan date and time is within the specified number of days (scan time limit).	
Software Use	Mandatory Software	You can judge whether specified software programs have been installed. You can control your environment properly by making sure that the mandatory software programs defined in your organization have been installed. You can specify multiple mandatory software programs.	Y
	Unauthoriz ed Software	You can judge whether prohibited software programs have been installed. By making sure that prohibited software programs, such as file sharing programs that are problematic for security, have not been installed, you can prevent information leakage. You can specify multiple prohibited software programs.	Y

Configuration item		Description	Automated countermeasures
Windows Services[#2]		You can judge whether prohibited services are operating. By checking whether prohibited services are operating in your organization, you can understand whether the computers are being used illegally. You can specify multiple prohibited services. Judgment is made based on whether the specified services are operating.	Y[#3]
OS Security	Guest Account	You can judge whether there is a valid guest account. If there is a guest account, everybody can use the computer. By making sure that no guest account can be used, you can prevent misuse of the computer.	Y
	Password Strength[#4]	You can judge whether there is an account with a vulnerable password. A vulnerable password might be easily decrypted. By making sure that no vulnerable password is set, you can prevent illegal accesses to the computer through decryption of the password.	--
	Password Never Expires[#4]	You can judge whether there is an account with an indefinite password. If the same password is used for a log time, it will become easier to decrypt. By making sure that no indefinite password is set, you can prevent illegal accesses to the computer through decryption of the password.	Y
	Days Since Last Password Change[#4]	You can judge whether the number of days since the last password change exceeds the time limit. If the same password is used for a long time, it will become easier to decrypt. By checking the number of days the password has been used, you can prevent illegal accesses to the computer through decryption of the password.	--
	Auto Logon	You can judge whether auto logon is enabled. If auto logon is enabled, anyone can start up and use the computer. By making sure that auto logon is not enabled, you can prevent illegal use of the computer.	Y
	Power On Password	You can judge whether a power-on password is enabled, and whether the power-on password function is implemented. By making sure that a power-on password is enabled, you can prevent illegal use of the computer.	--
	Password (Screen Saver)[#4]	You can judge whether the screen saver is password protected. If the screen saver is not password protected, the computer might be illegally used while the user is absent. By making sure that the screen saver is password protected, you can prevent illegal use of the computer.	Y[#5]
	Startup Time (Screen Saver)[#4]	You can confirm that the screen saver starts within the specified time. If the password protected screen saver has not yet been started, the computer might be illegally used while the user is absent. By checking the startup time of the screen saver, you can prevent illegal use of the computer.	Y[#5, #6]
	Shared Folder	You can judge whether there are any shared folders. Shared folders can allow illegal access to the computer. By making sure that shared folders are disabled, you can prevent illegal accesses to the computer.	Y
	Administrative Share	You can judge whether administrative share is enabled. If administrative share is enabled, the computer might be illegally accessed. By making sure that administrative share is disabled, you can prevent illegal access to the computer.	Y
	Anonymous Access	You can judge whether anonymous access is enabled with no restrictions. If anonymous access is enabled with no restrictions, the computer might be illegally accessed. By making sure that the anonymous access with no restrictions is disabled, you can prevent illegal accesses to the computer.	Y

Configuration item		Description	Automated countermeasures
OS Security	Windows Firewall [#7, #8]	You can judge whether Windows Firewall is enabled, and whether it is implemented. If Windows Firewall is disabled, the computer might illegally accessed. By making sure that Windows Firewall is enabled, you can prevent illegal accesses to the computer.	Y[#1]
	DCOM	You can judge whether DCOM is disabled. If DCOM is enabled, the computer might be illegally accessed. By making sure that DCOM is disabled, you can prevent illegal accesses to the computer.	Y
	Remote Desktop[#8]	You can judge whether remote desktop is disabled, and whether it is implemented. If remote desktop is enabled, the computer might be illegally accessed. By making sure that remote desktop is disabled, you can prevent illegal accesses to the computer.	Y[#1]
User-Defined Security Settings (System Information)	Host Name	You can specify the host name in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Computer Name	You can specify the computer name in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Description	You can specify the description of the computer in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Model	You can specify the model of the computer in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Computer Manufacturer	You can specify the manufacturer of the computer in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Computer UUID	You can specify the universally unique identifier (UUID) of the computer in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Computer Serial Number	You can specify the computer's serial number in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	CPU	You can specify the CPU in computer information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Total Memory	You can specify the amount of memory in computer information as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Total Free Space	You can specify the amount of free space on the hard disk in computer information as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Number of Drives[#9]	You can specify the number of drives in System Drive information as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--

Configuration item		Description	Automated countermeasures
User-Defined Security Settings (System Information)	Drive Letter	You can specify the drive letter in System Drive information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Total Free Space on Logical Drive	You can specify the amount of free space on the logical drive in System Drive information as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Total Capacity of Logical Drive	You can specify the total capacity of the logical drive in System Drive information as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Logical Drive File System	You can specify the file system for the logical drive in System Drive information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Hard Disk Model	You can specify the model of the hard disk drive in System Drive information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Total Capacity of Hard Disk	You can specify the total capacity of the hard disk drive in System Drive information as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Hard Disk Interface	You can specify the interface for the hard disk drive in System Drive information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	BIOS Name	You can specify the name of the BIOS in BIOS information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	BIOS Manufacturer	You can specify the manufacturer of the BIOS in BIOS information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	BIOS Serial Number	You can specify the serial number of the BIOS in BIOS information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	BIOS Version (BIOS)	You can specify the version of the BIOS in BIOS information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	BIOS Version (SMBIOS)	You can specify the version of the SMBIOS in BIOS information as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	AMT Firmware Version	You can specify the version of the AMT firmware as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Turn Off Monitor (AC)	You can specify, as a judgment target item, the length of time until the monitored power supply (AC) is turned off. This information is contained in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--

Configuration item		Description	Automated countermeasures
User-Defined Security Settings (System Information)	Turn Off Monitor (DC)	You can specify, as a judgment target item, the length of time until the monitored power supply (DC) is turned off. This information is contained in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	System Standby (AC)	You can specify, as a judgment target item, the length of time until the system enters standby (AC) in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	System Standby (DC)	You can specify, as a judgment target item, the length of time until the system enters standby (DC) in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	Hibernation (AC)	You can specify, as a judgment target item, the length of time until the system goes into hibernation (AC) in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	Hibernation (DC)	You can specify, as a judgment target item, the length of time until the system goes into hibernation (DC) in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	Turn Off Hard Disks (AC)	You can specify, as a judgment target item, the length of time until the hard disk is turned off (AC) in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	Turn Off Hard Disks (DC)	You can specify, as a judgment target item, the length of time until the hard disk is turned off (DC) in Power Control information. You can enter a number in the range from 0 to 2,147,483,647 (minutes) for the judgment value.	--
	Last Logged On User Name	You can specify, as a judgment target item, the user name of the last user who logged on in User Details. You can enter 1 to 256 characters for the judgment value.	--
	Last Logged On User's Account Name	You can specify, as a judgment target item, the domain name (or computer name) of the last user who logged on in User Details. You can enter 1 to 256 characters for the judgment value.	--
	Last Logged On User Description	You can specify, as a judgment target item, the description of the last user who logged on in User Details. You can enter 1 to 256 characters for the judgment value.	--
	OS	You can specify the OS in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	OS Service Pack	You can specify the service packs for the OS in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	OS Serial Number	You can specify the serial number of the OS in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--

Configuration item		Description	Automated countermeasures
User-Defined Security Settings (System Information)	OS Owner	You can specify the owner of the OS in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	OS Company Name	You can specify the company name for the OS in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Windows Installer Version	You can specify the version number of Windows Installer in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	IE Version	You can specify the IE version in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	IE Service Pack	You can specify the IE service pack in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Windows Update Agent Version	You can specify the version number of the Windows Update agent in OS Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Network Adapter	You can specify the network adapter in Network Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	MAC Address	You can specify the MAC address in Network Details as a judgment target item. You can enter 1 to 17 characters for the judgment value.	--
	Domain (Workgroup)	You can specify the domain (work group) in Network Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
User-Defined Security Settings (Hardware Information)	Number of Cores#9	You can specify the number of cores in Processor Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Processor	You can specify the processor in Processor Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Memory Capacity	You can specify the amount of memory in Memory Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Memory Slot Capacity	You can specify the amount of memory in a memory slot in Memory Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Virtual Memory Capacity	You can specify the amount of virtual memory in Memory Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Number of Hard Disks#9	You can specify the number of hard disk drives in Hard Disk Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--

Configuration item		Description	Automated countermeasures
User-Defined Security Settings (Hardware Information)	Hard Disk Model	You can specify the model of the hard disk drive in Hard Disk Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Hard Disk Capacity	You can specify the capacity of the hard disk drive in Hard Disk Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Hard Disk Interface	You can specify the interface for the hard disk drive in Hard Disk Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Logical Drive Letter	You can specify the drive letter of the logical drive in Hard Disk Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Total Free Space on Logical Drive	You can specify the amount of free space on the logical drive in Hard Disk Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Total Capacity of Logical Drive	You can specify the total capacity of the logical drive in Hard Disk Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Logical Drive File System	You can specify the file system for the logical drive in Hard Disk Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of CD-ROM Drives[#9]	You can specify the number of CD-ROM drives in CD-ROM Drive Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	CD-ROM Drive Model	You can specify the model of the CD-ROM drive in CD-ROM Drive Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of Removable Drives[#9]	You can specify the number of removable drives in Removable Drive Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Number of Printers[#9]	You can specify the number of printers in Printer Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Printer Name	You can specify the name of the printer in Printer Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Printer Driver	You can specify the printer driver in Printer Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Printer's Shared Name	You can specify the shared name of the printer in Printer Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--

Configuration item		Description	Automated countermeasures
User-Defined Security Settings (Hardware Information)	Printer Server Name	You can specify the name of the printer server in Printer Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Printer Port	You can specify the printer port in Printer Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of Video Controllers #9	You can specify the number of video controllers in Video Controller Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Video Chip	You can specify the name of the video chipset in Video Controller Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	VRAM Capacity of Video Card	You can specify the amount of VRAM on the video card in VRAM Video Controller Details as a judgment target item. You can enter a number in the range from 0 to 9,223,372,036,854,775,807 (bytes) for the judgment value.	--
	Video Driver	You can specify the video driver in Video Controller Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of Sound Cards#9	You can specify the number of sound cards in Sound Card Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Sound Card Name	You can specify the name of the sound card in Sound Card Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Sound Card Manufacturer	You can specify the manufacturer of the sound card in Sound Card Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of Network Adapters#9	You can specify the number of network adapters in Network Adapter Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Network Adapter	You can specify the network adapter in Network Adapter Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of Monitors#9	You can specify the number of monitors in Monitor Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Monitor	You can specify the monitor in Monitor Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
	Number of Keyboards#9	You can specify the number of keyboards in Keyboard Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Keyboard	You can specify the keyboard in Keyboard Details as a judgment target item.	--

Configuration item		Description	Automated countermeasures
User-Defined Security Settings (Hardware Information)	Keyboard	You can enter 1 to 256 characters for the judgment value.	--
	Number of Mouse[#9]	You can specify the number of mouse in Mouse Details as a judgment target item. You can enter a number in the range from 0 to 2,147,483,647 for the judgment value.	--
	Mouse	You can specify the mouse in Mouse Details as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
User-Defined Security Settings (Added Management Item)	Added Management Item (Number)[#9]	You can specify an added management item whose data type is Number as a judgment target item. You can enter a number in the range from -2,147,483,647 to 2,147,483,647 for the judgment value.	--
	Added Management Item (Enumeration)	You can specify an added management item whose data type is Enumeration as a judgment target item. You can select a judgement value from the pull-down menu.	--
	Added Management Item (Text)	You can specify an added management item whose data type is Text as a judgment target item. You can enter 1 to 256 characters for the judgment value.	--
Other Access Restrictions[#2]	Print suppression	You can restrict print operations. You can also set a password to allow printing.	--
	Suppression of the use of USB devices	You can restrict the use of USB devices.	--
	Allow registered USB device usage	You can allow use of only the USB devices whose hardware asset information has been registered.	--
	Suppression of the use of built-in CD/DVD drives	You can restrict the use of built-in CD/DVD drives.	--
	Suppression of the use of built-in FD drives	You can restrict the use of built-in FD drives.	--
	Suppression of the use of IEEE1394 devices	You can restrict the use of IEEE1394 devices.	--
	Suppression of the use of built-in SD cards	You can restrict the use of built-in SD cards.	--
	Suppression of the use	You can restrict the use of Bluetooth devices.	--

Configuration item		Description	Automated countermeasures
Other Access Restrictions#2	of Bluetooth devices	You can restrict the use of Bluetooth devices.	--
	Suppression of the use of imaging devices	You can restrict the use of imaging devices.	--
	Suppression of the use of Windows portable devices	You can restrict the use of Windows portable devices.	--
	Display of suppression message	You can display a message indicating that the use of the device has been suppressed on the user's computer.	--
	Suppression of write operation to removable disks	You can restrict only the write operation to removable disks.	--
	Suppression of write operation to CD/DVD drives	You can restrict only the write operation to CD/DVD drives.	--
	Suppression of write operation to FD drives	You can restrict only the write operation to FD drives.	--
	Suppression of startup of software	You can restrict startup of one or more specified software programs.	--
Operation Logs#2	Target Operations to be Logged	You can set the operations for which operation logs are to be collected.	--
	Send/ Receive E-mail with Attachments	You can set whether sending or receiving email with attachments is regarded as a suspicious operation.	--
	Use Web/FTP Server	You can set whether uploading files onto a Web server or an FTP server is regarded as a suspicious operation.	--
	Copy/Move the File to External Device	You can set whether copying or moving files to external media is regarded as a suspicious operation.	--
	Large Number of Printing Jobs	You can set whether submission of a large number of printing jobs (exceeding a defined value) is regarded as a suspicious operation.	--

Configuration item		Description	Automated countermeasures
Common settings for prohibited operations and operation logs[#2]	Intervals for sending notification of prohibited operations and operation logs to the higher-level system	You can set intervals for sending notification of prohibited operations and operation logs to the higher-level system.[#10]	--
	Period for which prohibited operations and operation logs are kept on the user's computer	You can set a maximum time period for which prohibited operations and operation logs are kept on the user's computer before they are notified to the higher-level system.	--

Legend: Y: Automated countermeasures can be set. --: Automated countermeasures are not supported.

#1: When Active Directory is used, if the computer settings are improperly set by a group policy, automated countermeasures will fail because the computer settings cannot be changed.

#2: Computers managed offline and agentless computers are not supported.

#3: Automated countermeasures may fail because services that do not have the SERVICE_STOP permission or that depend on operating services cannot be stopped.

#4: When multiple user accounts are registered in the OS, this item is judged for each user account.

#5: Automated countermeasures are enforced only for the user accounts logged on to the OS.

#6: Automated countermeasures fail when the screen saver data is not placed in the Windows' `System32` folder.

#7: When the agent OS is Windows Server 2003 without Service Pack, this item is not judged and automated countermeasures cannot be enforced. When the OS is Windows Server 2008 R2 or Windows 7 and multiple network cards are used, automated countermeasures are enforced for all network profiles.

#8: This item is not judged when the agentless OS is Windows Server 2003 without any Service Packs, Windows XP with Service Pack 1, Windows XP without any Service Packs, or Windows 2000.

#9: If it is not possible to determine if the value is unspecified or set to 0, the value is regarded as 0.

#10: Use the default setting of 60 minutes because setting a shorter notification interval might cause too much load on the higher-level system. You can use a shorter notification interval when you want to acquire operation logs earlier, for example, at the time of implementation.

Action Items

Item	Description
Send User Notification	Messages can be automatically sent to the computer when the security status judged to be `Critical`, `Important`, or `Warning`. You can create a notification message. The contents of the violation, as well as the notification message, are reported to the user.
Network Connection Control	You can allow or block the network connection of the computer based on the judgment result of the security status.

#: Action items are executed only when the target computer connects to the management server.

Assigned Groups

Item	Description
Target Group Type	You can specify the configuration of a group (OS, network, department, location, and user-defined) to which a security policy is to be assigned. For the specified group configuration, you can set which group the security policy is to be assigned to.

(2) Notes on setting security policy

Computers managed offline and agentless computers are not subject to automated countermeasures.

(3) Security policies provided by the product

JP1/IT Desktop Management 2 provides the following policies.

Default policy

This security policy is automatically assigned when no security policy is assigned to a managed computer. A support services contract is required to use the default policy.

Recommended security policy

This security policy is used to strengthen the security of an agent-installed computer. The security configuration items and action items that are recommended by JP1/IT Desktop Management 2 are set in the recommended security policy. A support services contract is required to use the recommended security policy.

You can copy and use these policies when you create a new security policy.

The following table shows the values set for the default policy and the recommended security policy.

Configuration item		Violation level	Default policy		Recommended security policy	
			Setting	Automated countermeasures	Setting	Automated countermeasures
Windows Update	Automatic Windows Update	Important	Y	N	Y	Y
	All updates are installed	Important	Y	N	Y	Y
	Selected updates are installed	Important	N	N	N	N

Configuration item		Violation level	Default policy		Recommended security policy	
			Setting	Automated countermeasures	Setting	Automated countermeasures
Antivirus Software	Install	Critical	E	--	E	--
	Scan Engine Version	Critical	E (1 day)	--	E (1 day)	--
	Virus Definition File Version	Critical	E (1 day)	--	E (1 day)	--
	Auto Protect	Critical	E	--	E	--
	Last Scanned Date/Time	Critical	E (7 days)	--	E (7 days)	--
Software Use	Mandatory Software	Critical	N	N	N	N
	Unauthorized Software	Critical	N	N	N	N
Windows Services		Warning	N	N	N	N
OS Security	Guest Account	Important	Y	N	Y	Y
	Password Strength	Warning	Y	--	Y	--
	Password Never Expires	Warning	Y	N	Y	Y
	Days Since Last Password Change	Warning	Y (180 days)	--	Y (180 days)	--
	Auto Logon	Warning	Y	N	Y	Y
	Power On Password	Warning	Y	--	Y	--
	Password (Screen Saver)	Warning	Y	N	Y	Y
	Startup Time (Screen Saver)	Warning	Y (10 minutes)	N	Y (10 minutes)	Y
	Shared Folder	Important	Y	N	Y	Y
	Administrative Share	Important	Y	N	Y	Y
	Anonymous Access	Important	Y	N	Y	Y
	Windows Firewall	Important	Y	N	Y	Y
	DCOM	Important	Y	N	Y	Y
	Remote Desktop	Important	Y	N	Y	Y
User-Defined Security Settings		Critical	N	N	N	N
Other Access Restrictions	Print suppression	--	N	--	N	--

Configuration item		Violation level	Default policy		Recommended security policy	
			Setting	Automated countermeasures	Setting	Automated countermeasures
Other Access Restrictions	Suppression of the use of USB devices	--	N	--	Y	--
	Allow registered USB device usage	--	N	--	Y	--
	Acquire the stored list of files	--	N	--	Y	--
	Suppression of the use of built-in CD/DVD drives	--	N	--	Y	--
	Suppression of the use of built-in FD drives	--	N	--	Y	--
	Suppression of the use of IEEE1394 devices	--	N	--	Y	--
	Suppression of the use of built-in SD cards	--	N	--	Y	--
	Suppression of the use of Bluetooth devices	--	N	--	Y	--
	Suppression of the use of imaging devices	--	N	--	Y	--
	Suppression of the use of Windows portable devices	--	N	--	Y	--
	Display of suppression message (for USB devices)	--	N	--	Y	--
	Display of suppression message (for devices other than USB)	--	N	--	N	--
	Suppression of write operation to removable disks	--	N	--	N	--
	Suppression of write operation	--	N	--	N	--

Configuration item		Violation level	Default policy		Recommended security policy	
			Setting	Automated countermeasures	Setting	Automated countermeasures
Other Access Restrictions	to CD/DVD drives	--	N	--	N	--
	Suppression of write operation to FD drives	--	N	--	N	--
	Suppression of startup of software	--	N	--	Y	--
Operation Logs	Target Operations to be Logged	--	N	--	N	--
	Send/Receive E-mail with Attachments	--	N	--	N	--
	Use Web/FTP Serve	--	N	--	N	--
	Copy/Move the File to External Device	--	N	--	N	--
	Large Number of Printing Jobs	--	N	--	N	--
Common settings for prohibited operations and operation logs	Intervals for sending notification of prohibited operations and operation logs to the higher-level system	--	Y	--	Y	--
	Period for which prohibited operations and operation logs are kept on a user's computer	--	Y	--	Y	--
Action Items	Send User Notification	--	N	--	Y (Critical, Important, Warning)	--

Legend: Y: Enabled. E: Enabled for anti-virus products for which information can be collected. N: Disabled. --: Not supported.

Related Topics:

- (1) Items that can be set for a security policy

(4) Assigning a security policy

To judge security status, you must assign a security policy to a group or a computer. The following describes the ranges to which a security policy can be assigned.

Tip

The default policy is automatically assigned immediately after a computer is set as a management target.

Assigning a security policy:

If you assign a security policy to a computer, that security policy is then applied to the computer. If you assign a security policy to a group, the security policy is applied to all computers that belong to that group and its subordinate groups.

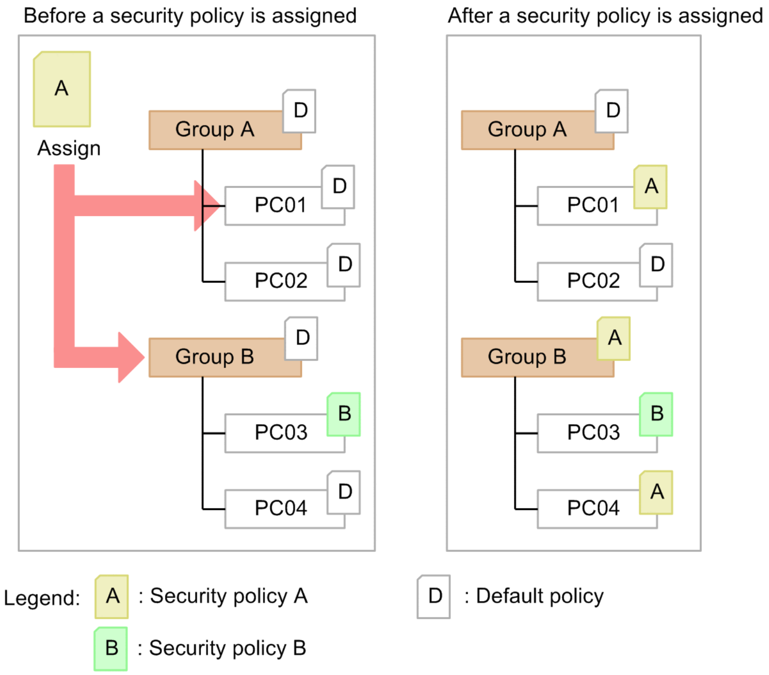
If different security policies are assigned to a computer and the group to which the computer belongs, the security policy assigned to the computer is applied. If a security policy is directly assigned to a group, that security policy is applied to the group. In this case, even if another security policy is assigned to the upper group, the security policy assigned to the upper group is not applied to the subordinate group.

Note that the assigned security policy remains applied even if the computer is switched from online management to offline management.

Important note

A computer might be registered with multiple IP address groups (for example, when multiple network interface cards are used in the computer). If a computer is registered in multiple groups for which different security policies are assigned, the default policy is applied to the computer.

The following figure shows an example of the range of assignment when a security policy is assigned.

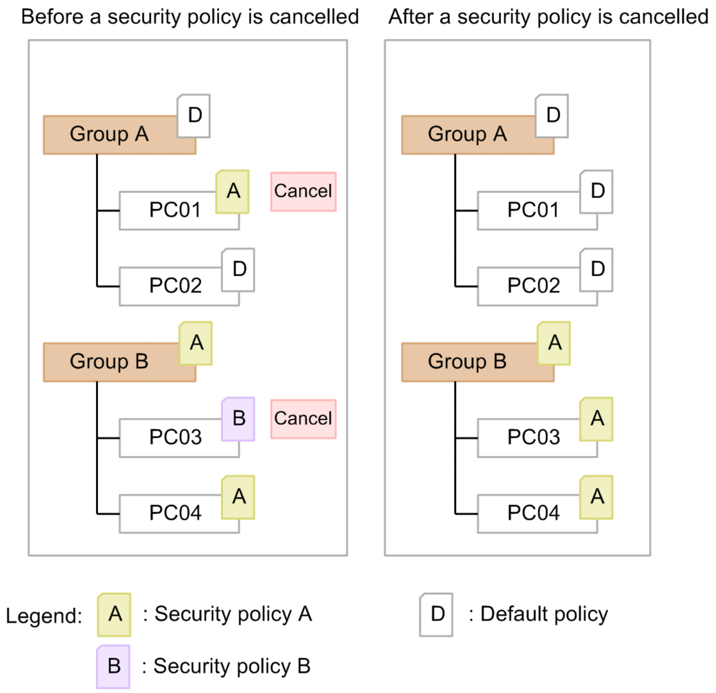


In the above figure, security policy A is assigned to computer PC01 and group B. However, security policy B is applied to computer PC03 in group B because security policy B has been directly assigned to computer PC03.

Cancelling assignment of a security policy:

You can cancel an assigned policy. If a security policy assigned to a group is cancelled, the security policy assigned to the upper group will be applied. If no security policy is assigned to the upper group, the default policy will be assigned.

The following figure shows an example of the range of assignment when a security policy is cancelled.



In the above figure, the security policies assigned to computers PC01 and PC03 are cancelled. The default policy will be applied to PC01 because no security policy is assigned to upper group A. Security policy A, which is assigned to upper group B, will be applied to PC03.

(5) Action items related to security judgment

If a security policy is assigned to a managed computer, the security status will be judged. You can configure the settings for the target computer so that certain actions (such as message notification or network control) are automatically taken depending on the results of the security status judgment.

The following action items can be executed depending on the judgment result of the security status:

Send User Notification

You can create messages to notify the users of the results of security status judgments. If you set the violation level to be notified of and the conditions for notification, you will be able to send the users notification messages only when the violation level is `Critical` (✖) or when the dangerous security status continues for more than a specified number of days. Note that only the computers managed online can receive messages.

For details about how to use notification messages, see (6) Notification messages depending on the security status.

Network Connection Control

You can set how to change the status of a computer's network connection based on the results of a security status judgment. If you set the violation level that is used for determining connection control and the conditions for rejecting connections, you will be able to block network connections of the computers whose violation level is Important (‼), or to control the network connection when the dangerous security status continues for more than a specified number of days.

For details about how to control network connections, see (9) Blocking or allowing network access depending on the judgment result of a security policy.

(6) Notification messages depending on the security status

You can send notification messages to computers whose security status is problematic. Only the computers managed online can receive notification messages. You can report messages in either of the following ways:

- In the **Device List** view (under **Computer Security Status**) of the **Security** module, you can send a message any time you want.
- Automatically send messages that were set in advance, depending on the results of the security policy judgment.

Tip

You can also send notification messages from the **Device List** view (under **Device Inventory**) of the Device module.

If a message is sent to a managed computer from the management server, a pop-up window appears on the user's screen, so the user can view the message. Note that only the latest message can be viewed.

Important note

If notification by a message fails, the message will be re-sent only once. If notification by a message fails twice, the message will no longer be sent.

(7) Contents of an automatically reported message

The following shows example contents of an automatically reported message:

```
Message body
------------------------------------------------------------------------

****** Security settings problem on AAAA ******
** OS Security Settings:△Violation-level
[Details]
BBBB

****** Security settings problem on Computer ******
** Windows Update:△Violation-level
CCCC

[Not Installed Windows Updates]
DDDD

** Antivirus Software:△Violation-level
Installation Status:△Violation-level
Software Version:△Violation-level
Auto Protect:△Violation-level
Virus Definition File Version:△Violation-level
Scan Engine Version:△Violation-level
Last Scanned Date/Time:△Violation-level

** Software Use:△Violation-level
[Installed Unauthorized Software]
EEEE

[Not Installed Mandatory Software]
FFFF

** Unauthorized Windows Service:△Violation-level
[Running Unauthorized Windows Service]
GGGG

** OS Security Settings:△Violation-level
[Details]
HHHH

** User-Defined Security settings:△Violation-level
[Details]
IIII

------------------------------------------------------------------------
```

Legend:

△: Space

Item	Description
Message body	Displays the text specified for the **Message Body** of the **Message Contents** in the **Send User Notification** view (under **Action Items** of **Security Policies**).
Violation level	Displays the following character strings depending on the violation levels corresponding to the judgment results: • Safe: Safe • Warning: Warning • Important: Important • Critical: Critical • Not enough information: Unknown • Error: Unknown • Not performed: Unknown • Out of target: Out of Target
AAAA	Displays the name of the user account that was judged as Critical.
BBBB	Displays the description of the items that were judged as Critical among the items in the **OS Security** view of the user account that was judged as Critical. The following contents are displayed: • Your Password is not strong. • Your Password from Last Password Change expired. • Password (Screen Saver) is disabled. • Startup Time (Screen Saver) is invalid.

Item	Description
CCCC	Displays the message `Automatic Windows Update is disabled.` when Windows automatic update is disabled.
DDDD	Displays the Windows updates that were found not have been installed by the **Windows Update** judgment. The following shows the display formats: • With the article ID: *security-information-ID*(*article-ID*) • Without the article ID: *security-information-ID* • With the service pack name: *product-name*(*service-pack-name*) Note that information that exceeds 5,000 bytes cannot be output. The number of updates that cannot be output is displayed in the form of `Other:` *n*.
EEEE	Displays the names and versions of the prohibited software programs that were found to have been installed by the **Software Use** judgment. The following shows the display formats: • With the version number: *software-name version* • Without the version number: *software-name* Note that information that exceeds 6,000 bytes cannot be output. The number of prohibited software programs that cannot be output is displayed in the form of `Other:` *n*.
FFFF	Displays the names and versions of the mandatory software programs that were found not have been installed by the **Software Use** judgment. • With the software name and version: *software-name version* • With the software name only: *software-name* Note that information that exceeds 6,000 bytes cannot be output. The number of programs that cannot be output is displayed in the form of `Other:` *n*.
GGGG	Displays the service display names of the services that were found to be in use by the **Windows Services** judgment. If information exceeds 6,000 bytes and some services cannot be displayed, the number of the services that cannot be displayed is displayed in the format of `Other:` *n*.
HHHH	Displays descriptions of the items that were judged to be Critical in the judgment of the items in the **OS Security** view. The following contents are displayed: • Enabled Guest Account exists. • Password Never Expires for some accounts. *account name* • Your Password is not strong. *account name* • Your Password from Last Password Change expired. *account name* • Auto Logon is enabled. • Power On Password is disabled or not implemented. • Shared Folder is enabled. • Anonymous Access is enabled. • Windows Firewall is disabled. • Administrative Share is enabled. • DCOM is enabled. • Remote Desktop is enabled. • Password (Screen Saver) is disabled. *account name* • Startup Time (Screen Saver) is invalid. *account name*
IIII	Displays a user-defined item that was determined as Critical as a result of judgment based on the user-defined security settings.

(8) Character strings that can be embedded in automatic notification messages

The following character strings can be embedded in the message body of automatic notification messages.

Character string	Display contents
%judgedate%	The date and time the security status was judged.
%contdays%	The number of days the inadequate status continued.#1
%refusedmsg%	The device has been disconnected. `Your computer will be refused to connect to a network in` *n* `days.`#2

#1: Displayed when **Notification Option** is set in the **Send User Notification** view (under **Action Items** of **Security Policies**).

#2: Displayed when **Disconnect Condition** is set in the **Network Connection Control** view (under **Action Items** of **Security Policies**).

(9) Blocking or allowing network access depending on the judgment result of a security policy

You can block the network access of a computer when the judgment result of a security policy for the computer exceeds the violation level that has been set. If the judgment result returns to a level lower than the set violation level, the network access will be automatically allowed. If you want to block or allow network access of a computer, the network segments to which the target computer belongs must be monitored.

> **Tip**
>
> You can also select the target computer in the **Device List** view (under **Device Inventory**) of the Device module, and then block or allow network access from the **Action** menu. For details, see 2.8.17 Manually controlling network access.

Priority of the network access control

The manual setting takes priority over the automatic network access control.

- When a computer is manually set so that network access is not allowed:

  Network access is not allowed even when the conditions for automatically allowing network access are satisfied.

If some computers must not access the network, manually set those computers so that network access is not allowed.

(10) Countermeasures for security policy violations

When a computer violates a security policy, take actions so that the settings of the computer will be adequate. Using JP1/IT Desktop Management 2, you can enforce automated countermeasures or forced countermeasures in response to a security policy violation.

Automated countermeasures

If you set automated countermeasures for a security policy, the settings of a computer that violated the security policy can be automatically changed to an adequate status. For details, see (11) Automated countermeasures against security policy violations.

Forced countermeasures

You can forcibly enforce countermeasures for each computer that violated a security policy when you want. If you want to enforce forced countermeasures to a computer, an agent for online management must be installed on that computer.

(11) Automated countermeasures against security policy violations

When a computer violates a security policy, you need to check and change the settings of the computer so that the security status becomes adequate. Repeating such jobs requires great care.

If you set automated countermeasures, when a computer violates a security policy, countermeasures are automatically taken so that the security status of the computer becomes adequate. Thus, the administrator can keep the computers in an organization in a safe security status without the need of caring for the settings of individual computers.

Automated countermeasures that can be set for a security policy:

- Enable Windows automatic update.
- When Windows updates included in the mandatory update group have not been installed, forcibly execute Windows automatic update or automatically distribute the updates.
- When mandatory software programs have not been installed, install the software programs.
- When prohibited software programs have been installed, restrict startup of the software programs.
- When prohibited software programs have been installed, uninstall the software programs.
- When prohibited services are running, stop and disable the services.
- Disable the guest account.
- Cancel the setting of a password that never expires.
- Cancel auto logon.
- Set password protection for the screen saver.
- Change the wait time for starting the screen saver when the value exceeds a predefined value.
- Remove shared folders.
- Cancel anonymous access with no restrictions.
- Enable Windows Firewall.
- Remove an administrative share.
- Disable DCOM.
- Disable remote desktop.

Time when countermeasures are automatically enforced

- When a security policy is assigned.
- When a security policy is updated.
- When a group to which managed computers belong is changed.
- When the device information of the managed computers is updated.

Countermeasures are automatically enforced at the above times depending on the security policy settings. Both security configuration and automated countermeasures for services are enforced on the managed computers. As for installation of mandatory software programs and installation of prohibited software programs, the distribution function is executed from the management server.

Important note

For the items below, countermeasures are automatically enforced after a computer to which a security policy is assigned is restarted. After the security policy is applied to the computer, balloon tips are displayed regularly to prompt the user to restart the computer. Whether balloon tips are displayed depends on the specification in the **User notification settings** view for the agent configuration.

- Execute Windows Update
- Anonymous Access
- Windows Firewall #
- Administrative Share
- DCOM
- Remote Desktop

#: Only when the OS on the computer is Windows Server 2008, Windows 7, or Windows Vista.

Related Topics:

- (1) Items that can be set for a security policy

(12) Notes on automated countermeasures against security policy violations

If security countermeasures are automatically enforced or a security policy is applied, you cannot change the settings of the managed computers back to the state before the countermeasures were taken even if you use the JP1/IT Desktop Management 2 functions. For the following items, the JP1/IT Desktop Management 2 functions cannot change the settings back to the state before the countermeasures were taken:

- Windows Update
- Software Use
- Windows Services
- OS Security

2.9.5 Restricting prohibited operations

You can set a security policy so that some computer operations will be restricted. By doing so, you can prevent information leakage.

Restricting printing

You can restrict print operations. This can help you prevent information (for internal use only) from being taken out in printed form.

You can set a password for allowing printing. This will let you restrict the users who are allowed print operations to those that you disclose the password to.

Important note

You cannot restrict output to a printer connected via the Internet. You cannot restrict output to a local printer when using a File port or a LAN Manager port. Also, you might not be able to restrict output to a Windows network shared printer.

When the printing function is used to output a file such as a PDF file, the file might be output even if a message indicating that the printing is restricted appears on the user's computer.

Suppression of Device Usage

You can restrict usage of a device. This prevents information from being taken out via the device. Use of the following devices can be restricted:

- USB devices
- Built-in CD/DVD drives
- Built-in FD drives
- IEEE1394 devices
- Built-in SD cards
- Bluetooth devices
- Imaging devices
- Windows portable devices

You can display a message indicating that use of a device is restricted on the user's computer. If you restrict the use of USB devices, you can also permit the use of some registered USB devices, and acquire a list of files stored on the permitted USB devices.

In addition, you can restrict only the writing operation to the following devices:

- Removable disks
- CD/DVD drives
- FD drives

Write-only restrictions can only be applied to permitted devices.

Tip

The write restrictions are enabled after the computer to which a security policy is assigned restarts. After a security policy is applied to a computer, balloon tips regularly appear, prompting the user to restart the computer. Whether balloon tips are displayed depends on the specification in the **User notification settings** view for the agent configuration.

Restricting startup of software programs

You can block the startup of the software programs that might cause information leakage (for example, file sharing software or messenger software).

You can block the startup of software programs with the following extensions:

- exe
- com
- scr

Note that if the character string made up of the execution file name and the folder name has 260 or more characters, startup of the software program cannot be blocked.

Important note

If a software program finishes its processing immediately after it starts up, startup of the program might not be blocked because it might finish before it is blocked.

Important note

Do not block startup of the execution files related to the OS and JP1/IT Desktop Management 2. If you block startup of such execution files, the OS or JP1/IT Desktop Management 2 might not operate properly.

(1) Devices whose use can be restricted

By setting prohibited operations in a security policy, you can restrict the use of devices on an agent-installed computer.

The following table shows the devices whose use can be restricted, and conditions for the deterrence targets.

Tip

Devices which have been accessed by a user before the security policy settings are enabled are not subject to the restriction.

Devices that can be restricted	Condition for the deterrence targets#1
USB devices	Devices to which data can be stored via USB connection#2. The target devices must satisfy the following two conditions when connected: • The device must be displayed under a USB controller in **Device by type** in the **Device Manager** window. • The device must be displayed under one of the **Disk drives**, **DVD/CD-ROM drives**, or **Floppy disk drives** in the **Device Manager** window. In addition, the enumerator of a device that is displayed under one of the **Disk drives**, **DVD/CD-ROM drives**, or **Floppy disk drives** in the **Device Manager** window must be `USBSTOR`.
Built-in CD/DVD drives	The target devices are CD/DVD drives built in a computer. These drives are displayed under **DVD/CD-ROM drives** in **Device by type** in the **Device Manager** window. The enumerator of the DVD/CD-ROM drive must be `IDE` or `SCSI`.
Built-in FD drives	The target devices are FD drives built in a computer. These drives are displayed under **Floppy disk drives** in **Device by type** in the **Device Manager** window. The enumerator of the floppy disk drive must be `FDC`.
IEEE1394 devices	The target devices are the devices connected to the computer with IEEE1394#3. These drives are displayed under **Disk drives** in **Device by type** in the **Device Manager** window. The enumerator of the disk drive must be `SBP2`.
Built-in SD cards	The target devices are SD cards connected to the computer via a built-in SD card slot#3. A device other than an SD card connected via the SD card slot might be regarded as a built-in SD card and subject to restriction. These drives are displayed under **Disk drives** in **Device by type** in the **Device Manager** window. The enumerator of the disk drive must be `SD` or `RIMMPTSK`. Note that an SD card slot that is built in a computer but uses a USB controller might not be regarded as a built-in SD card.
Bluetooth devices	The target devices are Bluetooth devices connected to the computer via USB. These drives are displayed under Bluetooth in **Device by type** in the **Device Manager** window. The enumerator of the Bluetooth must be `USB`, and the class of the device must be `BTW` or `BTM`.
Imaging devices	The target devices are imaging devices connected to the computer via USB#4. These devices are displayed under **Imaging Devices** in **Device by type** in the **Device Manager** window. The enumerator must be `USB`.
Windows portable devices	The target devices are Windows portable devices connected to the computer#5.

Devices that can be restricted	Condition for the deterrence targets[#1]
Windows portable devices	These devices are displayed under **Portable Devices** in **Device by type** in the **Device Manager** window.

#1: The displayed items might differ depending on the OS settings and other configurations.

#2: The target devices are devices that have one of the following device setup classes:

Class	ClassGuid
CDROM	{4d36e965-e325-11ce-bfc1-08002be10318}
DiskDrive	{4d36e967-e325-11ce-bfc1-08002be10318}
FloppyDisk	{4d36e980-e325-11ce-bfc1-08002be10318}

The *Class* and *ClassGuid* device setup classes are, in Windows 7, the text string displayed by opening the properties of the device from the **Device Manager** window, clicking the **Details** tab, and selecting **Device class** or **Device class guid** from the pulldown menu.

If you cannot find the *Class* and *ClassGuid* device setup classes, ask the developer of the device.

#3: The target devices are devices that have one of the following device setup classes:

Class	ClassGuid
DiskDrive	{4d36e967-e325-11ce-bfc1-08002be10318}

The *Class* and *ClassGuid* device setup classes are, in Windows 7, the text string displayed by opening the properties of the device from the **Device Manager** window, clicking the **Details** tab, and selecting **Device class** or **Device class guid** from the pulldown menu.

If you cannot find the *Class* and *ClassGuid* device setup classes, ask the developer of the device.

#4: The target devices are devices that have one of the following device setup classes:

Class	ClassGuid
Image	{6bdd1fc6-810f-11d0-bec7-08002be2092f}

The *Class* and *ClassGuid* device setup classes are, in Windows 7, the text string displayed by opening the properties of the device from the **Device Manager** window, clicking the **Details** tab, and selecting **Device class** or **Device class guid** from the pulldown menu.

If you cannot find the *Class* and *ClassGuid* device setup classes, ask the developer of the device.

#5: The target devices are devices that have one of the following device setup classes:

Class	ClassGuid
WPD	{eec5ad98-8080-425f-922a-dabf3de3f69a}

The *Class* and *ClassGuid* device setup classes are, in Windows 7, the text string displayed by opening the properties of the device from the **Device Manager** window, clicking the **Details** tab, and selecting **Device class** or **Device class guid** from the pulldown menu.

If you cannot find the *Class* and *ClassGuid* device setup classes, ask the developer of the device.

Related Topics:

- (3) Types of USB devices that can be allowed for use
- (7) Notes on restricting the use of devices

(2) Devices on which only the write operations can be restricted

In prohibited operation settings in the security policy, only write operations can be restricted on an agent-installed computer. You must restart the computer after you change the write restriction security policy.

The following table shows the devices on which only write operations can be restricted, the relevant device type, and conditions for the deterrence targets.

Device	Example applicable device#1	Condition for the deterrence targets#2
Removable disk	• USB-connected hard disk • USB-connected flash memory (such as USB memory device and USB-connected card reader) • IEEE1394-connected hard disk	The target drives include a drive whose drive type is displayed as **Removable Disk** in Windows Explorer, and a drive whose drive type is displayed as **Local Disk** in USB or IEEE1394 connections. The target includes both the built-in drives and USB or IEEE1394-connected drives.
CD/DVD drive	• USB-connected CD/DVD drive • Built-in CD/DVD drive	The target drives are drives that are displayed under **DVD/CD-ROM drives** in **Device by type** in the **Device Manager** window. The target includes both the built-in drives and USB-connected drives.
FD drive	• USB-connected FD drive	The target drives are drives that are displayed under **Floppy disk drives** in **Device by type** in the **Device Manager** window. The target includes both the built-in drives and USB-connected drives.

#1: If an applicable device is recognized by the OS as a different device, the device is treated according to the OS recognition and not subject to the write-operation restriction.

#2: The displayed items may vary depending on the OS settings or other configurations.

Tip

- Write operation to DVD-RAM might not be restricted.
- If a tool tries to access a device under write-operation restriction, the tool might encounter an error, or an event or error dialog box may appear.
- If write-operation restriction is enforced, some devices including encryption-supported USB devices, might not be started or used.

Devices on which write operations can be restricted differ depending on the OS. The following table shows the relationship between the restricted devices and the OSs.

Device	Windows 8.1, Windows 8		Windows Server 2012	Windows 7, Windows Server 2008, Windows Vista	Windows Server 2003	Windows XP (Service Pack 2 or later)
	No edition	Pro, Enterprise				
Removable disk	N	Y #1, #2	Y#1, #2	Y #1	N	S#4

Device	Windows 8.1, Windows 8		Windows Server 2012	Windows 7, Windows Server 2008, Windows Vista	Windows Server 2003	Windows XP (Service Pack 2 or later)
	No edition	Pro, Enterprise				
CD/DVD drive	N	Y #1, #2	Y#1, #2	Y #1	S#3	S#3
FD drive	N	Y #1, #2	Y#1, #2	Y #1	N	N

Legend: Y: Can be restricted. S: Some devices might not be restricted. N: Cannot be restricted.

#1: The Windows service, `Portable Device Enumerator Service`, must be set to `Manual` or `Automatic`.

#2: Writing operation will not be restricted if a USB device is assigned to a memory pool.

#3: Whether the write operation can be restricted or not depends on the writing software. Only software programs that support Windows IMAPI are subject to restriction.

#4: USB devices, including USB-connected hard disks, CD/DVD drives, and FD drives, can be restricted.

When the use of USB devices are restricted

If write restriction for CD/DVD drives, FD drives, or removable disks is set on a computer that restricts the use of USB devices, enabled restriction item and JP1/IT Desktop Management 2 behavior vary depending on the registration status of the connected device. The following table describes the details.

Behavior when USB-connected hard disks, CD/DVD drives, FD drives are connected to a computer that is set to restrict the use of USB devices

Restriction item	Registration status of a connected device (USB device)	Behavior of JP1/IT Desktop Management 2
Write restriction of CD/DVD drive, removable disk, or FD drive	Not registered	Read and write operations are restricted (a restriction event is sent, and a restriction message is displayed).
	Registered	Write operation is restricted.

Related Topics:

- (3) Types of USB devices that can be allowed for use
- (7) Notes on restricting the use of devices

(3) Types of USB devices that can be allowed for use

When the use of USB devices has been restricted by the setting of prohibited operations in a security policy, you can configure the settings so that only USB devices registered as hardware assets are allowed for use.

> **Tip**
>
> The device instance ID (which is acquired when a USB device is registered) is used for identifying a USB device. The device instance ID is an ID set to a USB device. Some USB devices have unique IDs that can be identified individually, and other USB devices have IDs that change depending on the connecting ports or environments.

You can allow the use of the following two types of USB devices:

USB devices that can be allowed for individual devices

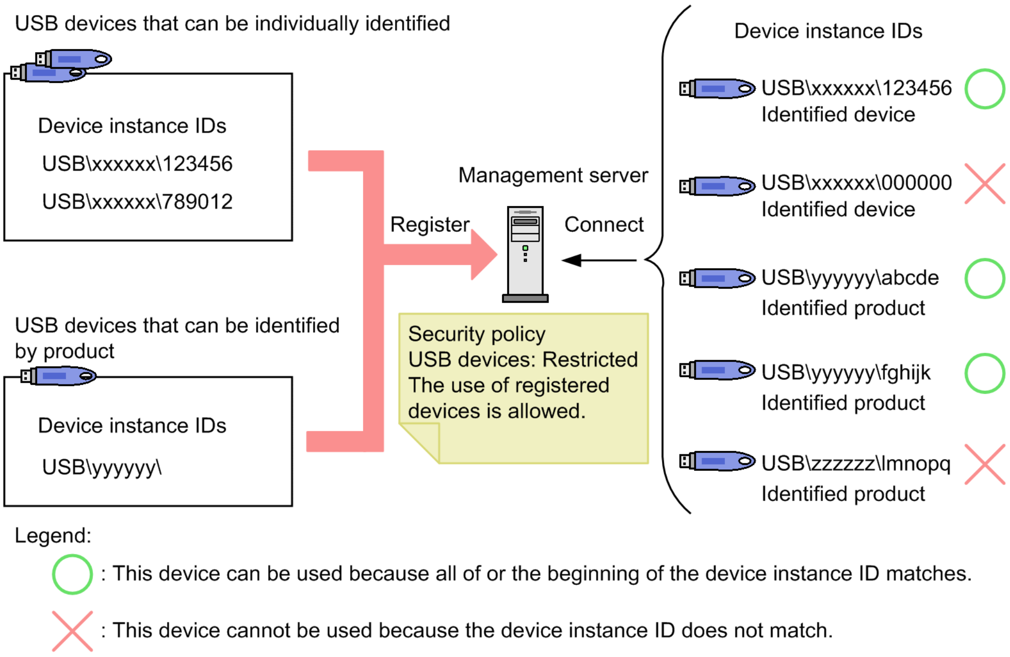
The USB devices that have unique device instance IDs can be allowed for use for individual devices.

Note that, when you display the **Details** tab of the device properties (from the Windows **Device Manager**) and select **Capabilities** from the pull-down menu, the USB devices that have unique IDs are displayed as `CM_DEVCAP_UNIQUEID`.

USB devices that can be allowed for individual products

The USB devices whose device instance IDs change depending on the connecting ports or environments can be registered and allowed for use for individual products. For example, if you have multiple USB memory devices of the same model of the same manufacturer, and if the device instance IDs for those USB memory devices are not unique, registering one of those devices allows the use of all of those devices.

A USB device whose device instance ID may change is identified based on a part of the ID. If the beginning part of the device instance ID for a USB device matches the registered device instance ID (which was specified when another USB device was registered), the two devices are regarded as the same product. Note that for a USB device that can be allowed for use for individual products, a message is displayed when the USB device is registered.



USB devices that can be individually identified
Device instance IDs
USB\xxxxxx\123456
USB\xxxxxx\789012
USB devices that can be identified by product
Device instance IDs
USB\yyyyyy\
Register
Management server
Connect
Security policy
USB devices: Restricted
The use of registered devices is allowed.
Device instance IDs
USB\xxxxxx\123456 Identified device ○
USB\xxxxxx\000000 Identified device ×
USB\yyyyyy\abcde Identified product ○
USB\yyyyyy\fghijk Identified product ○
USB\zzzzzz\lmnopq Identified product ×
Legend:
○ : This device can be used because all of or the beginning of the device instance ID matches.
× : This device cannot be used because the device instance ID does not match.

Important note

Use a computer managed online to register USB devices to be allowed for use. Note that even if the asset information about USB devices is directly registered in the **Hardware Assets** view of the Assets module, the use of those registered devices will not be allowed.

Important note

If you have registered a USB device to be allowed for each product, another device of the same product is treated as the same hardware asset when it is registered. Therefore, if the use of USB devices is restricted in a security policy, the use of USB devices is allowed for individual products.

Important note

When a device has multiple ways for connecting to a computer (for example, connecting interfaces and modes), the device might be identified differently depending on the connection method.

Important note

To allow the use of a USB device that connects to a computer via multiple devices, you must allow the use of all the devices on the connection path.

Important note

When you connect a device with no device instance ID to a computer, the OS generates an arbitrary device instance ID. The device instance ID for such a device changes depending on the connecting computer or port, so the use of the device might not be allowed.

Tip

If you connect a USB device that has already been registered and is individually identified to a computer managed offline, information about the files stored in the USB device is collected. The collected information is displayed on the **Title File List** tab of the **Hardware Assets** view (of the Assets module). Note that the **Title File List** tab is displayed only when the **Device Type** is **USB Device**. However, if acquisition of a list of files is prohibited by the security policy, **Title File List** displays a message that a file list cannot be acquired.

(4) Notes on when prohibited operations are restricted

The following are notes on individual restriction targets when you set a policy for prohibited operations in a security policy.

Related Topics:

- (5) Notes on restricting startup of software
- (6) Notes on restricting printing
- (7) Notes on restricting the use of devices

(5) Notes on restricting startup of software

- The total characters for the file name and folder name of the software program to be restricted must be less than 260 characters.
- If a software program finishes its processing immediately after it starts up, startup of the program might not be blocked because it might finish before it is blocked.
- If the same software program is restricted by JP1/IT Desktop Management 2 and another program, that software program might not be restricted by JP1/IT Desktop Management 2.
- If a target program starts during the approved time and then the system time of the device is changed, the program might not be blocked even outside the approved time.

- If a program is started during an approved time for which it is set, and the computer goes into a sleep or hibernation state, the program will not be restricted after the approved time has passed. The program will be restricted a while after the computer wakes from the sleep or hibernation state.
- If version information for the executable file of the target program is corrupted or contradicted, the program might not be blocked even if the **Original File Name** setting in Windows Explorer matches the **File Name** setting for the program.
- If startup of a program is repeatedly restricted during a short period of time, OS might display the message below. In this case, the user must terminate the program as instructed by the message, and then restart the OS.

```
The application failed to initialize properly (0xc0000142). Click on OK
to terminate the application.
```

(6) Notes on restricting printing

- The table below shows the printers for which printing can be restricted.

Printer type	Printing restriction
Local printer	Y
Network shared printer	Y
Internet printer	N
Virtual printer	Y

Legend:

Y:Printing can be restricted for this type of printer.

N:Printing cannot be restricted for this type of printer.

- In the properties for each printer, **Print** and **Manage Documents** must be allowed for all logged on users.
- When printing is restricted by Hibun, printing cannot be restricted by JP1/IT Desktop Management 2.
- If printing is performed immediately after a printer is added, the printing might not be restricted.
- If printing is performed immediately after you log on to the OS, the printing might not be restricted.
- If a print job is finished before the print operations are notified to the agent, the printing cannot be restricted.
- Depending on the printer, multiple printing restriction logs are collected at a single printing.

For the network shared printer, the following notes are added.

- The table below shows the supported combination of the agent and the print server.

Agent	Print server	Printing restriction
Windows XP/2003	Windows XP/2003	Y
Windows XP/2003	Windows Vista or later	Y
Windows Vista or later	Windows XP/2003	N
Windows Vista or later	Windows Vista or later	Y
Any	Others	N

Legend:

Y:Printing can be restricted for this type of printer.

N:Printing cannot be restricted for this type of printer.

- RPC communication must be possible between the print server and the agent PC. If RPC communication is not possible, the problem might be caused by one of the following:
    - The print server is a server based on the Internet Printing Protocol (IPP).
    - A firewall, proxy or NAT is present between the print server and the agent PC.
    - The agent PC's Windows firewall is enabled and **File and Printer Sharing** is not set to **Exceptions**.
- The agent PC's **File and Printer Sharing for Microsoft Networks** must be enabled.
- The print server must be able to resolve the name of the agent PC.
- If the agent PC is Windows Vista or later, the agent PC and the print server must join the same domain, or the credential of the print server must be registered on the Credential Manager of the agent PC. The agent PC needs to reboot after registering the credential.
- If IPv6 is enabled and rendering of the print job does not work on the client computer, the printing might not be restricted. To operate rendering of print jobs on the client computer, the following settings are required:
    - **Render print jobs on client computers** is enabled.
    - **Enable advanced printing features** is enabled.

(7) Notes on restricting the use of devices

- JP1/IT Desktop Management 2 controls devices according to Windows rules (it cannot control devices that do not comply with Windows rules). We recommend that you check whether the target device can be controlled in advance. For specifications of a device, contact the manufacturer.
- A device might not be identified depending on the OS running on the computer the device is connected to. Therefore, we recommend that you check in advance whether a device can be properly controlled by the OS being used.
- How Windows identifies devices cannot be judged only by the device configuration and the product name. Check the properties in the Windows **Device Manager**.
- Use of a device might not be restricted in the following case, despite the specified security policy:
    - When the device is connected to a computer before the JP1/IT Desktop Management 2 process starts (for example, immediately after the computer has started).
- The device restriction feature cannot be used with other products that restrict the use of devices, for example, Windows group policy or Active Directory policy. If you use the device restriction feature with other device-restricting products, settings in each of the products might not work properly.
- The computer must be restarted in the following cases:
    - When you want to restrict the use of a device that was connected to the computer before the security policy was applied, and the device is not a USB device.
    - When you want to restrict the use of a working device, and the device is not a USB device.
    - If you want to allow the use of a device whose use was restricted by the previous security policy but the restriction was removed by the updated security policy.
    - If you want to restrict the use of a device whose use was not restricted by the previous security policy but the restriction was added by the updated security policy.
- If you change the security policy (to start restricting the use of a device) while file operation logs are collected, file operation logs collected just before the policy change might not be acquired.
- An error might appear in the following situations:
    - When a device with Autoplay enabled is restricted.
    - When a restricted device is accessed by a tool.

    - If you connect a deterrence-target device to a computer for the first time.
    - If a device is restricted during a file operation.
- If a setting on a device performed in other products violates the security policy, change the setting according to the security policy.
- You cannot acquire system information or hardware information from deterrence-target devices.
- If you connect a deterrence-target device to a computer for the first time, the device driver might not be able to be installed. You cannot use the device if the device driver cannot be installed.
- If the device has been connected to the computer before, installation of the device driver might be performed if the device is connected to a different port, or connected by a different user. If the device was connected to the computer before the device was restricted, the restriction of the device is activated after the computer is restarted.
- If a deterrence-target device (whose restriction will be activated after the computer is restarted) is connected to the computer, and you connect another device, a restriction dialog box for the deterrence-target device might reappear, or a warning message might appear.
- If a deterrence-target device is identified by the OS as a different device, the device cannot be restricted. However, if the device was identified by the OS as another deterrence-target device, the device is restricted as the device identified by the OS.
- If you apply a security policy restricting one or more devices to a computer running Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, an error-level event might be recorded in the event logs.
- If you access a deterrence-target device by a tool, an event might be output in the event logs, or an error dialog box might appear.

Notes on restricting the use of USB devices

- When a USB-connected CD/DVD drive is restricted, the tray on the restricted CD/DVD drive might open.
- A USB device that was connected before the restriction-setting security policy was applied is not restricted. In this case, removing the device and then connecting it again activates the restriction.
- A scanner might be identified as an imaging device if it is a USB-connected device.
- If a device is a USB-connected device, it cannot be restricted if it is not identified as a USB device, Bluetooth device, or an imaging device.
- If you connect a deterrence-target USB device to a computer on which AutoPlay is enabled, the AutoPlay might fail, and an error message will be output.
- If AutoPlay is enabled, you cannot restrict use of a USB-connected hard disk drive or FD drive. To restrict the use of these devices, disable the AutoPlay feature.
- If AutoPlay is enabled in Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, use of a USB-connected hard disk drive or FD drive might not be restricted.
- When both the following conditions are met, while copying files to or from a USB-connected hard disk drive or FD drive, use of USB devices cannot be restricted until the file copy operation finishes.
    - The OS of the computer is Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista.
    - You applied a security policy that restricts use of USB devices while a file is being copied.
- When a security policy that excludes a USB device from deterrence targets depending on its **Connection Name** is applied, a USB device that was connected to a computer for the first time might be restricted. This is because the **Connection Name** cannot be acquired. In this case, connect the USB device again.

- If the computer is running Windows 8.1, Windows 8, or Windows Server 2012, any USB devices that are allocated to a memory pool are not restricted.
- If you reconnect a device that was once connected to a computer and restricted by the computer, restriction message display, logs for connection, disconnection, or restriction, or restriction event might not be acquired.

Notes on restricting the use of Bluetooth devices

- If you configure to restrict Bluetooth devices, use of a Bluetooth-connected mouse or keyboard will also be restricted.
- If you connect a Bluetooth device to a computer, a registry of the following Bluetooth device hardware ID is created:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\
  JP1/IT Desktop Management 2 regards a device as a Bluetooth device if the `Class` value of this registry is `Bluetooth`, `BTW`, or `BTM`. You can check the hardware ID from the Device Manager window of the OS.

Notes on restricting the use of Windows portable devices

A USB device, identified as a Windows portable device on a computer on which a Windows portable device is configured as a deterrence target, is restricted as a Windows portable device. (In this case, registered USB devices whose use is allowed and USB devices connected with **USB Device Registration** are also restricted as Windows portable devices.)

2.9.6 Managing Windows updates

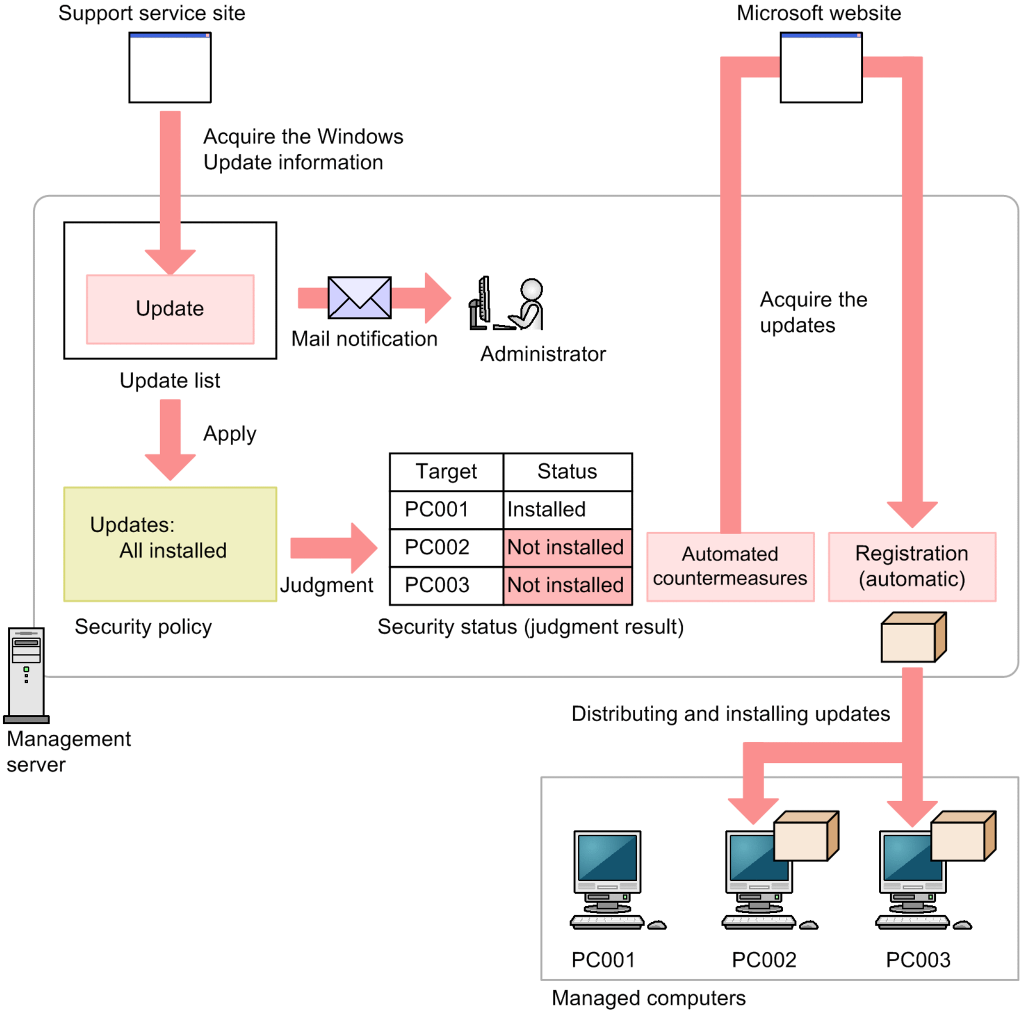
If the OSs running on the computers in your organization are Windows, Windows updates must be installed as necessary to fix errors or security problems. JP1/IT Desktop Management 2 can automatically install Windows updates released from Microsoft according to the security policy.

> **Important note**
>
> The support services contract is required to automatically acquire the latest information about Windows updates and install the updates on your computers.

Using JP1/IT Desktop Management 2, you can reduce the efforts of managing Windows updates by using convenient functions as follows:

- Checking the release of Windows updates
- Automatically distributing and installing Windows updates on computers
- Installing different combinations of Windows updates for individual groups

You can manage Windows updates in the **Windows Update** view of the Security module. The following figure shows the concept of managing Windows updates.



Target	Status
PC001	Installed
PC002	Not installed
PC003	Not installed

After Windows updates are released from Microsoft, information about the updates is automatically acquired from the support service site. At this time, the administrator can be automatically notified by email. After the information about the updates is acquired, the update list is automatically updated.

When **All updates are installed** is set in a security policy, the Windows update information added to the list is applied to the security policy, and the latest status of whether the updates have been installed is judged. If updates have not been installed on some computers, the updates can be automatically distributed and installed on those computers.

By creating update groups, you can change how Windows updates are judged for each security policy. By creating a test group, you can first test whether updates will cause problems on the computers in your organization. Then, you can automatically install only the safe updates.

You can also register and distribute Windows updates manually.

For details on acquiring information from the support services, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

Tip

You can use both the function of automatically distributing Windows updates using a security policy and the Windows automatic update function (Windows Update or Microsoft Update) at the same time. However, you cannot use JP1/IT Desktop Management 2 to control which function is to be used for installing Windows updates. If you want to install all the mandatory updates provided by Microsoft, we recommend that you enable Windows automatic update. If you want to install only the special updates, we recommend that you use the JP1/IT Desktop Management 2 function to distribute the updates.

Creating an update group

When you set **Selected updates are installed** in a security policy, you can use an update group to apply only the Windows updates allowed by the administrator for installation to the security policy. For details about update groups, see (9) Managing update groups.

Related Topics:

- (1) Prerequisites for acquiring and distributing Windows updates
- (3) Types of Windows updates for which information can be automatically acquired
- (2) Notes on acquiring Windows updates
- (6) Checking the status of Windows updates

(1) Prerequisites for acquiring and distributing Windows updates

The following shows the prerequisites for acquiring Windows updates from the Microsoft website based on the Windows update information acquired from the support service site, and for automatically distributing the update to computers.

Prerequisites for automatically acquiring information about Windows updates from the support service site:

- The support services contract is made.
- MSXML 4.0 Service Pack 2 or MSXML 6.0 is installed.
- The management server can connect to the Internet.

Tip

To acquire information about Windows updates from the support service site, the settings for connecting to the support service site are required.

Tip

Even in an environment where the management server cannot connect to the Internet, if another computer can connect to the Internet, you can manually acquire and then register Windows update information from the support service site.

Prerequisites for automatically acquiring Windows updates from the Microsoft website and distributing the updates:

- The management server can connect to the Internet.
- The management server and the distribution-destination computer are connected.
- An agent is installed on the distribution-destination computer.

Tip

To distribute Windows updates to computers, Windows update files are required. In an environment where the management server can connect to the Microsoft website via the Internet, Windows updates are automatically downloaded, and the Windows update files are registered.

Even in an environment where the management server cannot connect to the Internet, if you use another computer that can connect to the Internet to acquire Windows updates (execution files) from the Microsoft website, you can manually register the Windows update files.

(2) Notes on acquiring Windows updates

The following notes give restrictions related to acquiring Windows updates:

- When you distribute acquired Windows updates to other computers, do so after making sure that the updates can be properly distributed and installed on the target computers. Depending on the computer environment, distribution or installation of updates might fail.
- You cannot acquire the following Windows updates:
  - Windows updates provided earlier than January 1 2006 by Microsoft
  - Windows updates provided by Microsoft Security Advisory
  - Windows updates corresponding to the PC-98 series computers
- The files related to the information about Windows updates are stored in *JP1/IT Desktop Management 2-installation-folder*`\mgr\OSPATCH`. Do not change or delete the files in this folder. If you change or delete the files in this folder, correct operation of JP1/IT Desktop Management 2 is not guaranteed.

Related Topics:

- (1) Prerequisites for acquiring and distributing Windows updates

(3) Types of Windows updates for which information can be automatically acquired

By connecting to the support service site, you can acquire information about Windows updates released from Microsoft, and automatically apply the information to security-judgment targets. Also, by setting automated countermeasures in a security policy, you can automatically distribute and install Windows updates to computers.

Information about Windows updates for the following programs can be automatically acquired from the support service site.

Program	Type or version
Windows	Windows 8.1
	Windows 8
	Windows 7
	Windows Server 2012
	Windows Server 2008
	Windows Vista
	Windows Server 2003

Program	Type or version
Windows	Windows XP
	Windows 2000
Internet Explorer	7.0 or later

Information about Windows updates can be acquired only for the updates that satisfy the following conditions:

- The class (the type of Windows update) is `Windows Update`.
- The security number is set (not empty).
- The severity is `Critical` or `Important`.
- There is information about the service pack number of the target OS.

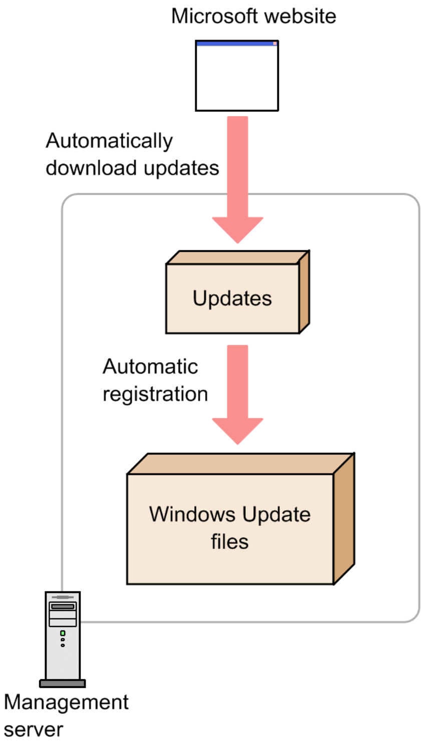
(4) Automatically registering Windows Update files

The Windows updates and installation scripts that are necessary for distribution are automatically downloaded from the Microsoft website and the support service site, and then the Windows Update files are registered. By using this function, the administrator can reduce the efforts of regularly downloading Windows updates because the latest updates can always be acquired and distributed automatically.

Important note

A support services contract is required to automatically download Windows updates and installation scripts.

The following figure shows the flow of automatically registering the Windows Update files.



Note that registered Windows Update files are not added to the **Package List** view of the Distribution (ITDM-compatible) module. Windows Update files can be distributed only by automated countermeasures for a security policy.

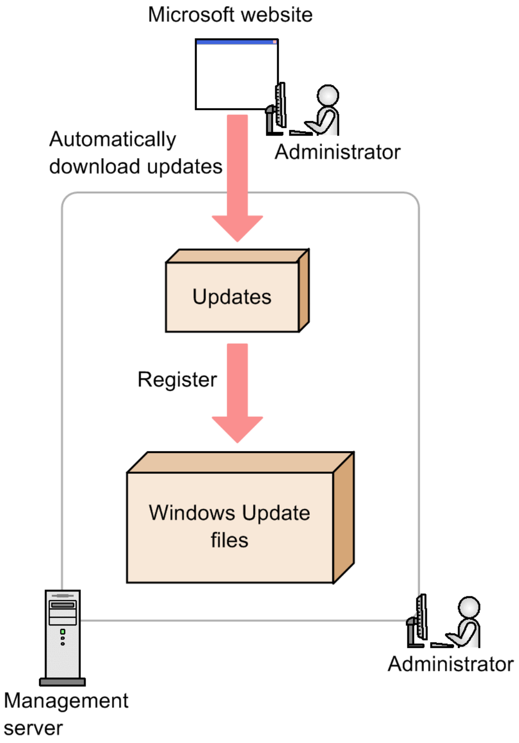
You cannot manually create a task for distributing Windows updates. You can check the executed tasks in the Distribution (ITDM-compatible) module.

(5) Manually registering Windows Update files

By downloading the Windows updates necessary for distribution from the Microsoft website, the administrator can add Windows updates to the management server at any time and register the Windows Update files. The added updates are automatically installed on users' computers. This function is convenient when you want to immediately distribute Windows updates that are important for security without waiting for automated countermeasures of JP1/IT Desktop Management 2.

When manually registering Windows Update files, the administrator must perform all tasks for downloading Windows updates and registering the Windows Update files.

The following figure shows the work flow for manually registering Windows Update files.



Tip

In an environment where the Administrator's computer cannot connect to the Internet (when the update list is updated offline), use another computer that can connect to the Internet to register the Windows Update files.

In this case, on a computer that can connect to the Internet, display the operation window. On the **Windows Update Information** tab of the **Windows Update** view, download the Windows updates from **Execution File Download URL**. After that, from the **Action** menu, select **Register Windows Update File**, and then specify the downloaded updates. Thus, you can register the Windows Update files.

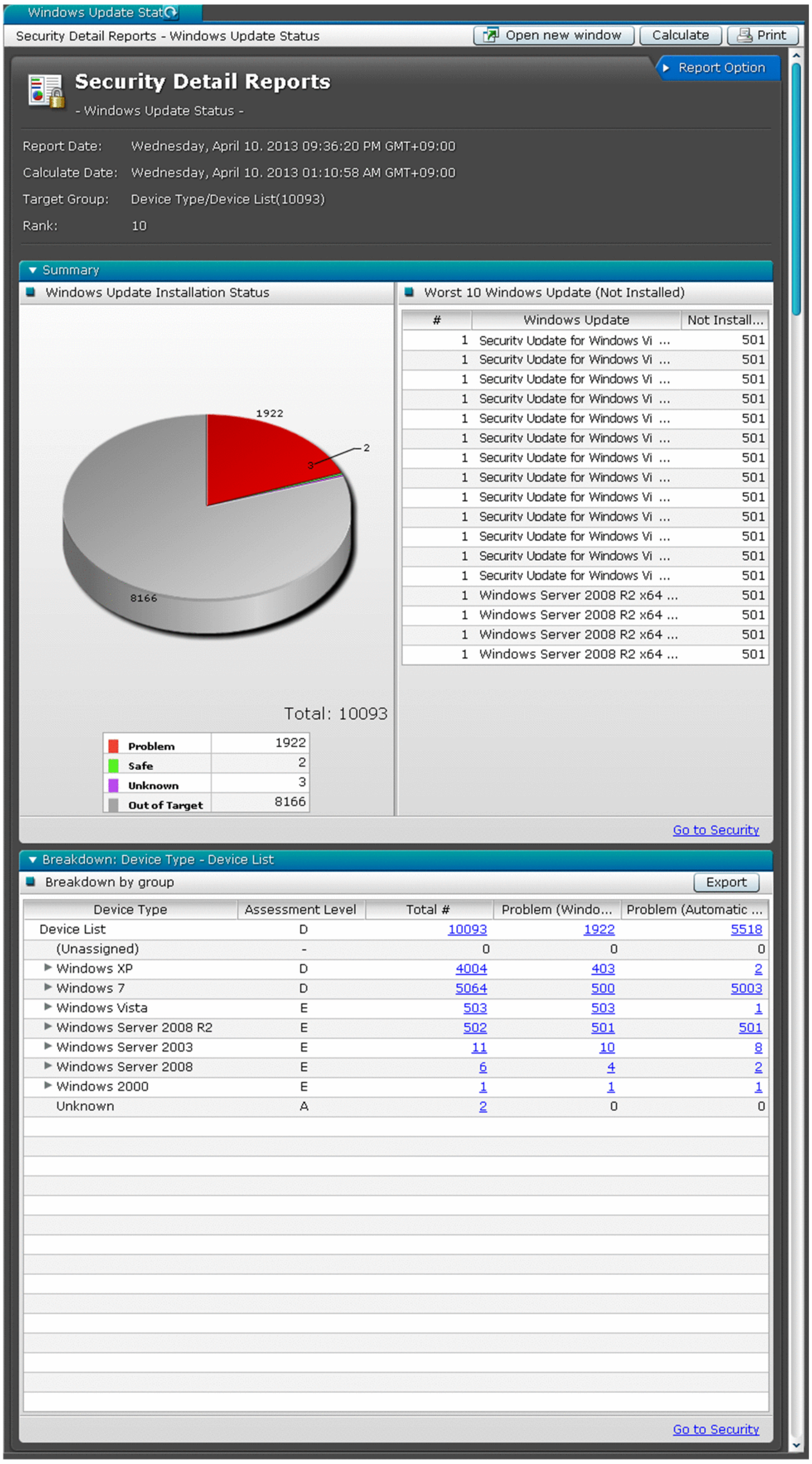
Note that the created Windows Update files are not added to the **Package List** view of the Distribution (ITDM-compatible) module. The Windows Update files can be distributed only by automated countermeasures for a security policy. You cannot manually create a task for distributing Windows updates. You can check the executed tasks in the Distribution (ITDM-compatible) module.

(6) Checking the status of Windows updates

You can check whether Windows updates have been installed in the following ways.

Checking for Windows updates that have not been installed on some computers:

In the **Windows Update Status** report (under **Security Detail Reports**), you can check Windows updates. The Windows updates are listed in the order of the number of computers on which the update has not been installed.



Security Detail Reports

- Windows Update Status -

Report Date: Wednesday, April 10. 2013 09:36:20 PM GMT+09:00

Calculate Date: Wednesday, April 10. 2013 01:10:58 AM GMT+09:00

Target Group: Device Type/Device List(10093)

Rank: 10

Summary

Windows Update Installation Status

Total: 10093

🟥 Problem	1922
🟩 Safe	2
🟪 Unknown	3
⬜ Out of Target	8166

Worst 10 Windows Update (Not Installed)

#	Windows Update	Not Install...
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Security Update for Windows Vi ...	501
1	Windows Server 2008 R2 x64 ...	501
1	Windows Server 2008 R2 x64 ...	501
1	Windows Server 2008 R2 x64 ...	501
1	Windows Server 2008 R2 x64 ...	501

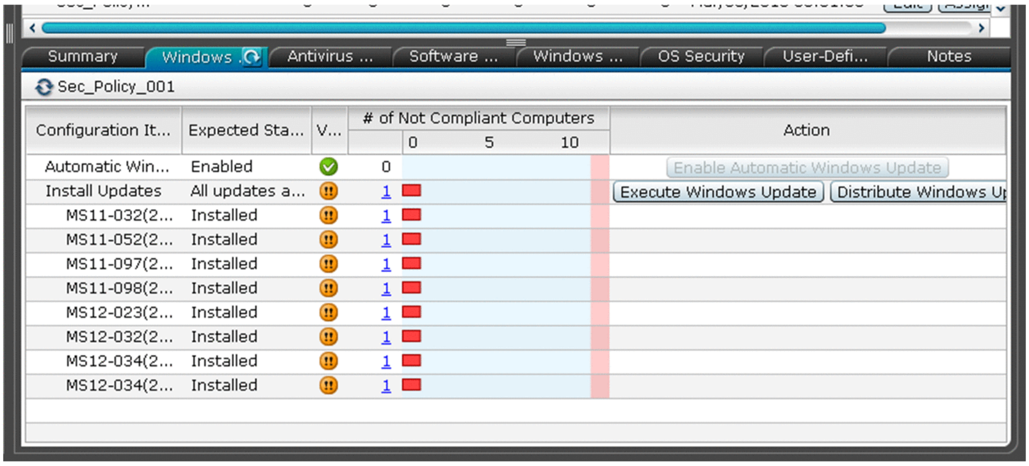
Breakdown: Device Type - Device List

Breakdown by group

Device Type	Assessment Level	Total #	Problem (Windo...	Problem (Automatic ...
Device List	D	10093	1922	5518
(Unassigned)	-	0	0	0
▸ Windows XP	D	4004	403	2
▸ Windows 7	D	5064	500	5003
▸ Windows Vista	E	503	503	1
▸ Windows Server 2008 R2	E	502	501	501
▸ Windows Server 2003	E	11	10	8
▸ Windows Server 2008	E	6	4	2
▸ Windows 2000	E	1	1	1
Unknown	A	2	0	0

Checking the violation level for each security policy:

On the **Windows Update** tab of the **Security Policy List** view (under the Security module), you can check violation levels. If there is a problem related to violation level, there might be computers on which one or more Windows updates have not been installed.

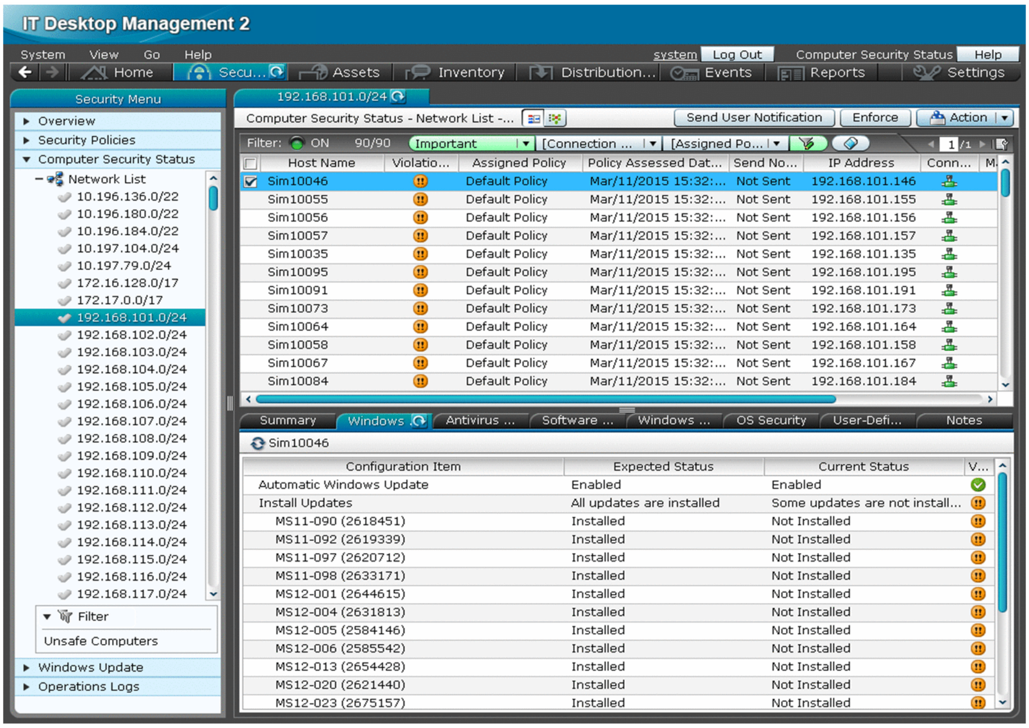


Sec_Policy_001

Configuration It...	Expected Sta...	V...	# of Not Compliant Computers (0 5 10)	Action
Automatic Win...	Enabled	✓	0	Enable Automatic Windows Update
Install Updates	All updates a...	!!	1 🟥	Execute Windows Update | Distribute Windows U
MS11-032(2...	Installed	!!	1 🟥	
MS11-052(2...	Installed	!!	1 🟥	
MS11-097(2...	Installed	!!	1 🟥	
MS11-098(2...	Installed	!!	1 🟥	
MS12-023(2...	Installed	!!	1 🟥	
MS12-032(2...	Installed	!!	1 🟥	
MS12-034(2...	Installed	!!	1 🟥	
MS12-034(2...	Installed	!!	1 🟥	

Checking the status of whether Windows updates have been installed for each device:

On the **Windows Update** tab of the **Computer Security Status** view (under the Security module), you can check the status of whether Windows updates have been installed on each device. If one or more Windows updates have not been installed on a computer, those updates are displayed.



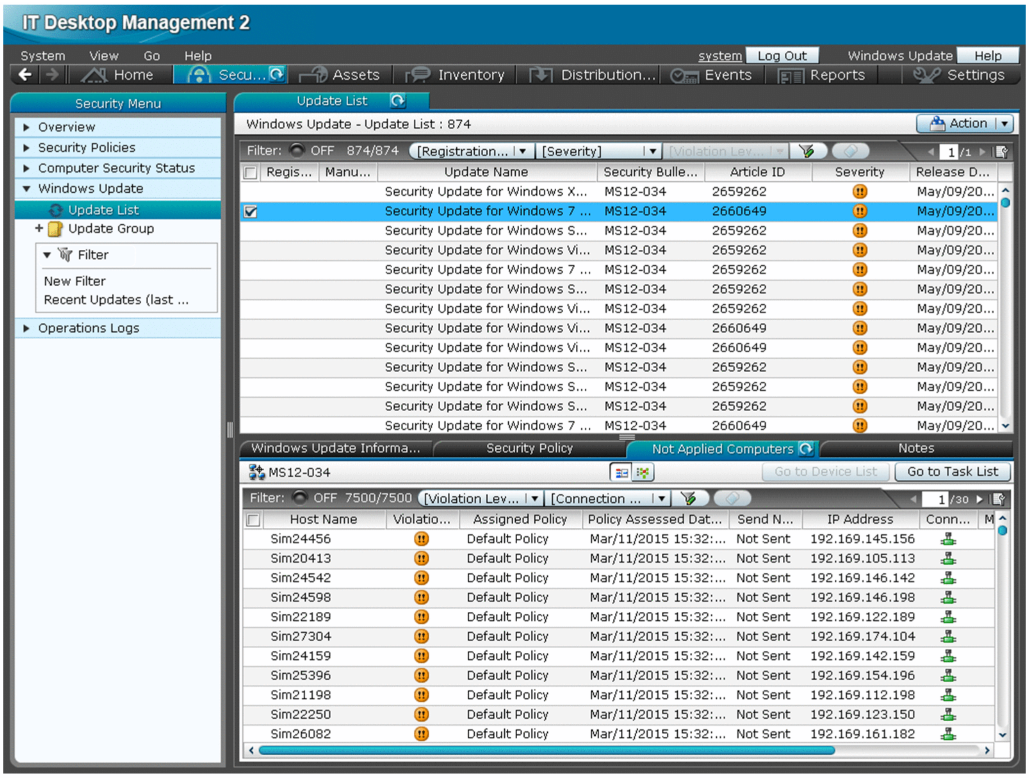
☐	Host Name	Violatio...	Assigned Policy	Policy Assessed Dat...	Send No...	IP Address	Conn...	M.
☑	Sim10046	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.146		
	Sim10055	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.155		
	Sim10056	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.156		
	Sim10057	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.157		
	Sim10035	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.135		
	Sim10095	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.195		
	Sim10091	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.191		
	Sim10073	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.173		
	Sim10064	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.164		
	Sim10058	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.158		
	Sim10067	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.167		
	Sim10084	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.168.101.184		

Sim10046

Configuration Item	Expected Status	Current Status	V...
Automatic Windows Update	Enabled	Enabled	✓
Install Updates	All updates are installed	Some updates are not install...	!!
MS11-090 (2618451)	Installed	Not Installed	!!
MS11-092 (2619339)	Installed	Not Installed	!!
MS11-097 (2620712)	Installed	Not Installed	!!
MS11-098 (2633171)	Installed	Not Installed	!!
MS12-001 (2644615)	Installed	Not Installed	!!
MS12-004 (2631813)	Installed	Not Installed	!!
MS12-005 (2584146)	Installed	Not Installed	!!
MS12-006 (2585542)	Installed	Not Installed	!!
MS12-013 (2654428)	Installed	Not Installed	!!
MS12-020 (2621440)	Installed	Not Installed	!!
MS12-023 (2675157)	Installed	Not Installed	!!

Checking for computers on which Windows updates have not been installed:

On the **Not Applied Computers** tab of the **Update List** view (under the Security module), you can check for computers on which Windows updates have not been installed.



Windows Update - Update List : 874

Filter: OFF 874/874 [Registration... ▾ [Severity] ▾ [Violation Lev... ▾ 1 /1

□	Regis...	Manu...	Update Name	Security Bulle...	Article ID	Severity	Release D...
			Security Update for Windows X...	MS12-034	2659262	!!	May/09/20...
☑			Security Update for Windows 7 ...	MS12-034	2660649	!!	May/09/20...
			Security Update for Windows S...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Vi...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows 7 ...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows S...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Vi...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows Vi...	MS12-034	2660649	!!	May/09/20...
			Security Update for Windows Vi...	MS12-034	2660649	!!	May/09/20...
			Security Update for Windows S...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows S...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows S...	MS12-034	2659262	!!	May/09/20...
			Security Update for Windows 7 ...	MS12-034	2660649	!!	May/09/20...

MS12-034

Filter: OFF 7500/7500 [Violation Lev... ▾ [Connection ... ▾ 1 /30

□	Host Name	Violatio...	Assigned Policy	Policy Assessed Dat...	Send N...	IP Address	Conn...	M
	Sim24456	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.145.156		
	Sim20413	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.105.113		
	Sim24542	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.146.142		
	Sim24598	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.146.198		
	Sim22189	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.122.189		
	Sim27304	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.174.104		
	Sim24159	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.142.159		
	Sim25396	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.154.196		
	Sim21198	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.112.198		
	Sim22250	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.123.150		
	Sim26082	!!	Default Policy	Mar/11/2015 15:32:...	Not Sent	192.169.161.182		

(7) Updating the update list

JP1/IT Desktop Management 2 can automatically update the list of registered old Windows updates by regularly accessing the support service site. This is done based on support contract information or a schedule set by the administrator. This enables the administrator to check whether the latest Windows updates have been installed on all computers, or to check for Windows updates that have not been installed, without the need of performing special operations.

The update list is automatically updated once a day. The time it is updated is the same as the time the setup processing (which is performed immediate after JP1/IT Desktop Management 2 is installed) was completed. The minutes are rounded up to the nearest later hour. For example, if the setup for JP1/IT Desktop Management 2 finishes at 10:30, the update list is updated at 11:00 every day.

Important note

A support services contract and an environment where the management server can connect to the Internet are required.

Important note

The update list is automatically updated about 10 business days after the latest Windows updates are released from Microsoft. This is because it takes about 10 days from the release of Windows updates until the update of the information on the support service site. If you want to immediately add the information about the released Windows updates, the administrator must acquire the Windows updates and the information about Windows updates from the Microsoft website, and then manually add them to the update list.

Related Topics:

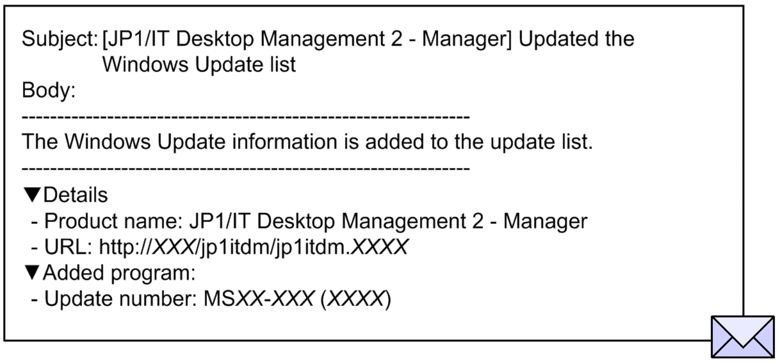
- (3) Types of Windows updates for which information can be automatically acquired
- (5) Manually registering Windows Update files

(8) Mail notification of updating the update list

When the update list is automatically updated, the updated contents can be reported to the administrator by email. In the email, information about the added Windows updates is described. The administrator can understand the details about the added Windows updates just by reading the email.

> **Important note**
>
> The mail server settings and the support service settings are required in advance.

The following is an example email report.



Subject: [JP1/IT Desktop Management 2 - Manager] Updated the
Windows Update list
Body:

The Windows Update information is added to the update list.

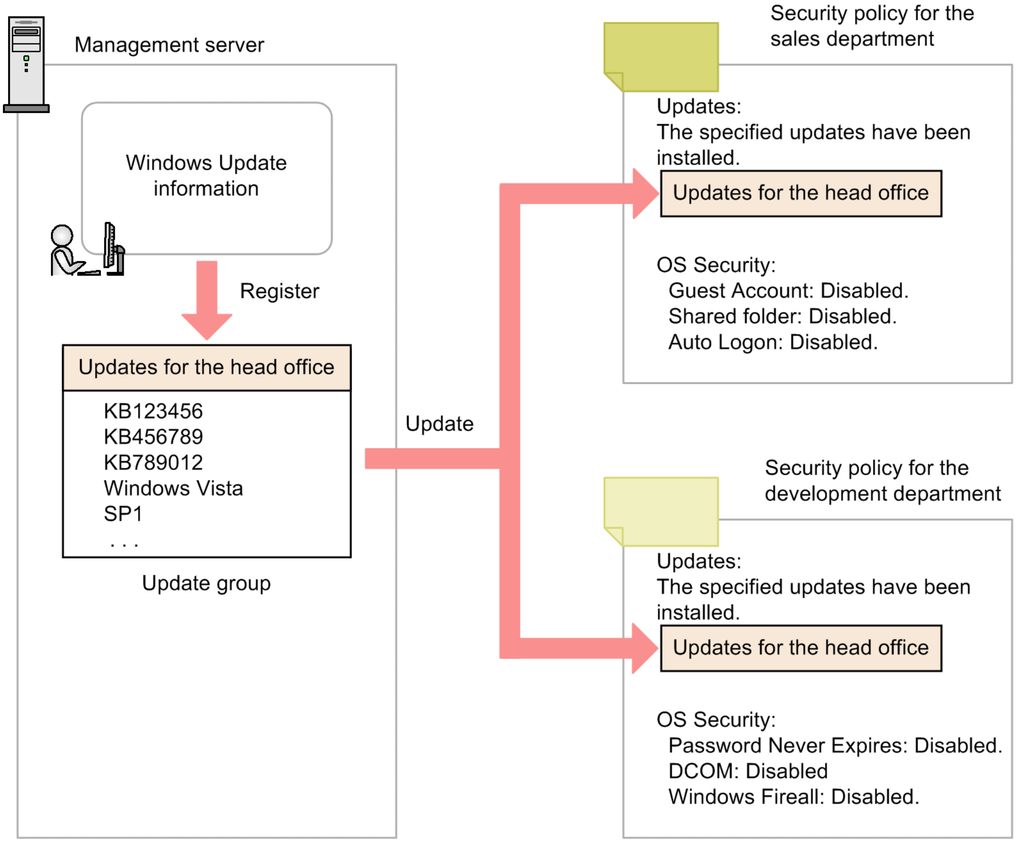
▼Details
 - Product name: JP1/IT Desktop Management 2 - Manager
 - URL: http://*XXX*/jp1itdm/jp1itdm.*XXXX*
▼Added program:
 - Update number: MS*XX*-*XXX* (*XXXX*)

(9) Managing update groups

When you want to judge only whether specific Windows updates have been installed, create an update group that groups the target Windows updates. Since an update group is specified in the security policy, only the Windows updates registered in the group will be judged.

By using an update group, you can centrally manage which Windows updates will be judged by different security policies.

The following figure shows the concept of managing Windows updates to be judged by using an update group.


Management server
Windows Update information
Register
Updates for the head office
KB123456
KB456789
KB789012
Windows Vista SP1
. . .
Update group
Update
Security policy for the sales department
Updates:
The specified updates have been installed.
Updates for the head office
OS Security:
Guest Account: Disabled.
Shared folder: Disabled.
Auto Logon: Disabled.
Security policy for the development department
Updates:
The specified updates have been installed.
Updates for the head office
OS Security:
Password Never Expires: Disabled.
DCOM: Disabled
Windows Fireall: Disabled.

For example, even when different security policies are used for the sales department and the development department, you can configure the settings so that the same Windows updates are installed. By specifying an update group common to the sales department and the development department for the judgment-target Windows updates, you can centrally manage the updates to be installed while using different policies for different departments.

Also, you can use an update group when you want to distribute Windows updates after making sure that installing the updates causes no problems in your organization. Even if you acquire information about Windows updates from the support service, the information is not automatically applied to the update group. By additionally registering Windows updates in the update group, you can add the judgment-target updates without the need of editing a security policy. Therefore, by registering the Windows updates that have already been tested in the update group, only the updates allowed by the administrator can be installed and managed.

(10) Judging the results of distributing Windows updates

Whether a Windows update is successfully distributed is judged by the return value when the update is installed. The following shows the values returned when a Windows update is installed.

Return value	Description
0	Installation successfully finished.
1	Installation failed.
2	The environment is invalid (such as memory shortage or invalid file).
3	An internal error occurred.
4	The installation status of Windows Script Host (WSH) is invalid.
5	An internal error occurred.

2.10 Managing operation logs

You can collect operation logs from a target computer if you set collection of operation logs in a security policy and assign the security policy to the target computer.

To collect operation logs, an agent must be installed on the target computer. Also, to save the collected operation logs on the management server, Setup must be configured on the management server so that operation logs can be collected.

You can change the types of operation logs to be collected in the security policy settings. You can also change the setting of whether to detect suspicious operations in the security policy settings.

The following table shows the categories of suspicious operations and how to confirm them.

Category	Operations selected as suspicious in the security policy	Confirmation methods		
		Security module > **Operation Logs** > **Operation Log List** view	Events module > **Events** > **Event List**	**Suspicious Operations** panel
Suspicious file operations	**Send/Receive E-mail with Attachments**	**Suspicious** column An icon is displayed. **Operation Type (Detail)** column **Send Mail (Attachment File)** is displayed.	In the **Type** column, **Suspicious** is displayed.	**Send E-mail with Attachments** is displayed.
	Use Web/FTP Server	**Suspicious** column An icon is displayed. **Operation Type (Detail)** column **Web Access (Upload)** or **Web Access (Download)** is displayed.	In the **Type** column, **Suspicious** is displayed.	**Use Web/FTP Server** is displayed.
	Copy/Move the File to External Device	**Suspicious** column An icon is displayed. **Operation Type (Detail)** column **Copy file** or **Move file** is displayed.	In the **Type** column, **Suspicious** is displayed.	**Copy/Move the File to External Device** is displayed.
Suspicious print operation	Large Number of Printing Jobs	--	In the **Type** column, **Suspicious** is displayed.	--

Legend: --: Not displayed.

If conditions for suspicious file movement operations are set in the security policy, you can track the history of such operations using the operation logs.

For details about suspicious file movements, see 2.10.3 Investigating suspicious movements of files from systems using operation logs. For details about suspicious print operation, see 2.10.5 Collecting logs for suspicious print operations.

Tip

Collecting all types of operation logs might consume large amount of disk capacity. You can reduce consumption of disk capacity by collecting only the operation logs directly related to information leakage, or by specifying the target operations.

2.10.1 Types of operation logs that can be collected

The table below shows the types of operation logs that can be collected in JP1/IT Desktop Management 2.

Tip

When you configure the settings in a security policy so that suspicious operations can be detected, whether an operation is a suspicious operation is judged based on operation logs. Only a part of operation log types related to suspicious operations are used for such a judgment. If you select **Only operations that divulge information (recommended)** in a policy for operation logs, you can collect only the operation logs related to suspicious operations.

Types of operation logs

Operation Type	Operation Type (Detail)	Description	Behavior when **Only operations that divulge information (recommended)** is selected in a policy for operation logs
Power ON/Shut Down/Log On/Log Off	Power ON	A user started the computer.	Y
	Shut Down	A user shut down the computer.	Y
	Log On	A user logged on to Windows.	Y
	Log Off	A user logged off from Windows.	Y
Program Execution/ Termination	Program Execution	A user started a program.	N
	Program Termination	A user stopped a program.	N
File Operation/ Print Operation	Copy file[#1]	A user copied a file.	C
	Move file[#1]	A user moved a file.	C
	Rename file[#1]	A user renamed a file.	C
	Create file[#1]	A user created a file.	C
	Delete file[#1]	A user deleted a file.	C
	Web Access (Upload)[#2]	A user uploaded a file via a web browser.	C
	Web Access (Download)[#2]	A user downloaded a file via a web browser.	C
	FTP (Send File)[#2]	A user sent a file to an FTP server via a web browser.	C
	FTP (Receive File)[#2]	A user received a file from an FTP server via a web browser.	C
	Send Mail (Attachment File)[#3]	A user sent an email with attachment.	C
	Receive Mail (Attachment File)[#3]	A user received an email with attachment.	C
	Save Attached File[#3]	A user saved a file that was attached to a received email.	C
	Print[#4]	A user submitted a print job.	N

Operation Type	Operation Type (Detail)	Description	Behavior when **Only operations that divulge information (recommended)** is selected in a policy for operation logs
Folder Operation[#1]	Copy folder	A user copied a folder.	N
	Move folder	A user moved a folder.	N
	Rename folder	A user renamed a folder.	N
	Create folder	A user created a folder.	N
	Delete folder	A user deleted a folder.	N
Device operation	Device connection	A user connected a device to the computer.	Y
	Device disconnection	A user disconnected a device from the computer.	Y
	Permitting device connection	A device connection was permitted when usable devices are set for prohibited operations.	Y
Web Access	Web Access[#2]	A user accessed a web service via a web browser.	N
Window Operation	Change active window	A user changed the active window.	N
Deterrence Log	Block Program Activation	Startup of a program was blocked (when prohibited software programs are set).	Y
	Block Printing[#4]	Printing was blocked (when prohibited operations are set).	Y
	Block Device Connections	Use of a device was blocked (when prohibited operations are set).	Y

Legend: Y: Collected. C: Collected when the conditions for determining that the operation is a suspicious file movement are satisfied. N: Not collected.

For details about the conditions for determining that an operation is a suspicious file movement, see 2.10.4 Conditions for determining whether a file is to be monitored for suspicious file movements.

#1

Operation logs can be collected only when the operations are performed using Windows Explorer. Operation logs cannot be collected when the operations are performed from the command prompt or in application programs.

#2

Operation logs can be collected only when Internet Explorer 7, 8, 9, 10, or 11 is used.

#3

Operation logs can be collected when one of the following email clients is used:

- Microsoft Outlook Express 6
- Microsoft Outlook 2002, 2003, 2007, 2010, and 2013
- Windows Mail 6
- Windows Live Mail 2009, 2011, and 2012

#4

Operation logs can be collected when the following types of printers are used:

- Local printers

- Network shared printers
- Virtual printers

> **Important note**
>
> Operation logs cannot be collected for printers connected via the Internet. Also, if the File port is used on a local printer, operation logs for `Block Printing` cannot be collected. When a LAN Manager port is used, operation logs for `Print` and `Block Printing` cannot be collected.

Related Topics:

- (1) Collecting logs for suspicious movements of files from systems
- 2.10.7 Prerequisites and notes on collecting operation logs

(1) Information collected for each type of operation log

The following shows information collected for each type of operation log. For details about the information collected for individual information items, see *Details about the information items to be collected*. The following legend is used for the tables below:

Legend: Y: Collected. M: Might not be collected depending on the device or disk status. N: Not collected.

Power ON/Shut Down/Log On/Log Off

The following table shows the information items to be collected when **Power ON/Shut Down/Log On/Log Off** is the target operation type.

Operation Details	Information to be collected		
	Source	Operation Date/Time#	User Name
Power ON	Y	Y	N
Shut Down	Y	Y	N
Log On	Y	Y	Y
Log Off	Y	Y	Y

#: *Operation Date/Time* information includes **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, and **Time Zone**.

Program Execution/Termination

The table below shows the information items to be collected when **Program Execution/Termination** is the target operation type. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, **Time Zone**, and **User Name** are collected for every operation.

Operation Details	Information to be collected		
	User Name	File Version#	File Name
Program Execution	Y	Y	Y
Program Termination	Y	Y	Y

#: This item is collected only when the program (execution file) has a version number.

File Operation/Print Operation

The table below shows the information items to be collected when **File Operation/Print Operation** is the target operation type. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Browser)**, **Time Zone**, and **User Name** are collected for every operation.

Operation Details	Information to be collected					
	File Created Date/Time	File Last Modified Date/ Time	File size	Original File Drive Type / Original File Created Date/ Time	Original File Name / Drive type	Destination File Name / Drive Type
Copy file	Y	Y	Y	Y	Y	Y
Move file	Y	Y	Y	Y	Y	Y
Rename file	Y	Y	Y	Y	Y	Y
Create file	Y	Y	Y	Y	Y	N
Delete file	Y #1	Y #1	Y #1	Y	Y	N
Web Access (Upload)#2	Y	Y	Y	Y	Y	Y
Web Access (Download)	Y	Y	Y	Y	Y	Y
FTP (Send File)	Y	Y	Y	Y	Y	Y
FTP (Receive File)	Y	Y	Y	Y	Y	Y
Send Mail (Attachment File)	Y	Y	Y	Y	Y	Y
Receive Mail (Attachment File)	N	N	N	Y	Y	Y
Save Attached File	Y	Y	Y	Y	Y	Y
Print#3	N	N	N	N	N	N

#1: It might not be possible to collect **File Created Date/Time**, **File Last Modified Date/Time**, or **File Size** information depending on how the file is deleted.

#2: Information cannot be collected in Internet Explorer 10 or 11.

#3: Only **Printer Name**, **Printed Document Name**, and **Printed Page Count** can be collected.

Folder Operation

The table below shows the information items to be collected when **Folder Operation** is the target operation type. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, **Time Zone**, and **User Name** are collected for every operation.

Operation Details	Information to be collected			
	Original File Name	Source File Drive Type	Destination File Name	Destination File Drive Type
Copy folder	Y	Y	Y	Y
Move folder	Y	Y	Y	Y
Rename folder	Y	Y	Y	Y
Create folder	Y	Y	N	N
Delete folder	Y	Y	N	N

Device connection or disconnection

The table below shows the information items to be collected when **Device connection or disconnection** is the target operation type. Some information might not be collected depending on the device. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, **Time Zone**, and **User Name** are collected for every operation.

Operation Details	Information to be collected						
	Drive Type#1	Drive Name#2	Device Name	Serial #	Device Instance ID	Device Type#3	Device category
Device connection	Y	Y	Y	Y	Y	Y	Y
Device disconnection	M	M	M	M	M	M	M
Permitting device connection	Y	Y	Y	Y	Y	Y	Y

#1: `Others` is output in the case of a built-in FD drive, Bluetooth device, imaging device, or Windows portable device.

#2: Information cannot be collected in the case of a built-in FD drive, Bluetooth device, imaging device, or Windows portable device.

#3: Information can be collected only in the case of a USB device.

Web Access

The table below shows the information items to be collected when **Web Access** is the target operation type. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, **Time Zone**, and **User Name** are collected for every operation.

Operation Details	Information to be collected	
	Web Page Title	URL
Web Access	Y	Y

Window Operation

The table below shows the information items to be collected when **Window Operation** is the target operation type. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, **Time Zone**, and **User Name** are collected for every operation.

Operation Details	Information to be collected			
	Execute Account	File Version#	File Name	Window Title
Window Operation	Y	Y	Y	Y

#: This item is collected only when the execution file has a version number.

Deterrence Log

Deterrence Log includes three types of operations: **Block Program Activation**, **Block Printing**, and **Block Device Connections**. The tables below show information items to be collected when those are the target operations. Note that **Source**, **Operation Date/Time (Browser)**, **Operation Date/Time (Source)**, **Time Zone**, and **User Name** are collected for every operation.

Block Program Activation

Operation Details	Information to be collected				
	Software Name	Software Version	User Name	File Version#	File Name
Block Program Activation	Y	Y	Y	Y	Y

#: This item is collected only when the execution file has a version number.

Block Printing

Operation Details	Information to be collected		
	Printer Name	Printed Document Name	Printed Page Count
Block Printing	Y	Y	N

Block Device Connections

Operation Details	Information to be collected						
	Drive Type#1	Drive Name#2	Device Name	Serial #	Device Instance ID	Device Type#3	Device category
Block Device Connections	Y	Y	Y	Y	Y	Y	Y

#1: `Others` is output in the case of a built-in FD drive, Bluetooth device, imaging device, or Windows portable device.

#2: Information cannot be collected in the case of a built-in FD drive, Bluetooth device, imaging device, or Windows portable device.

#3: Information can be collected only in the case of a USB device.

Details about the information items to be collected

The following table shows the details about the information items to be collected for operation logs.

Item	Description
Source	The fully qualified domain name (FQDN) of the computer on which operation logs were collected. Display example: `dmp530`
Host ID	A unique ID to identify a computer in a system.

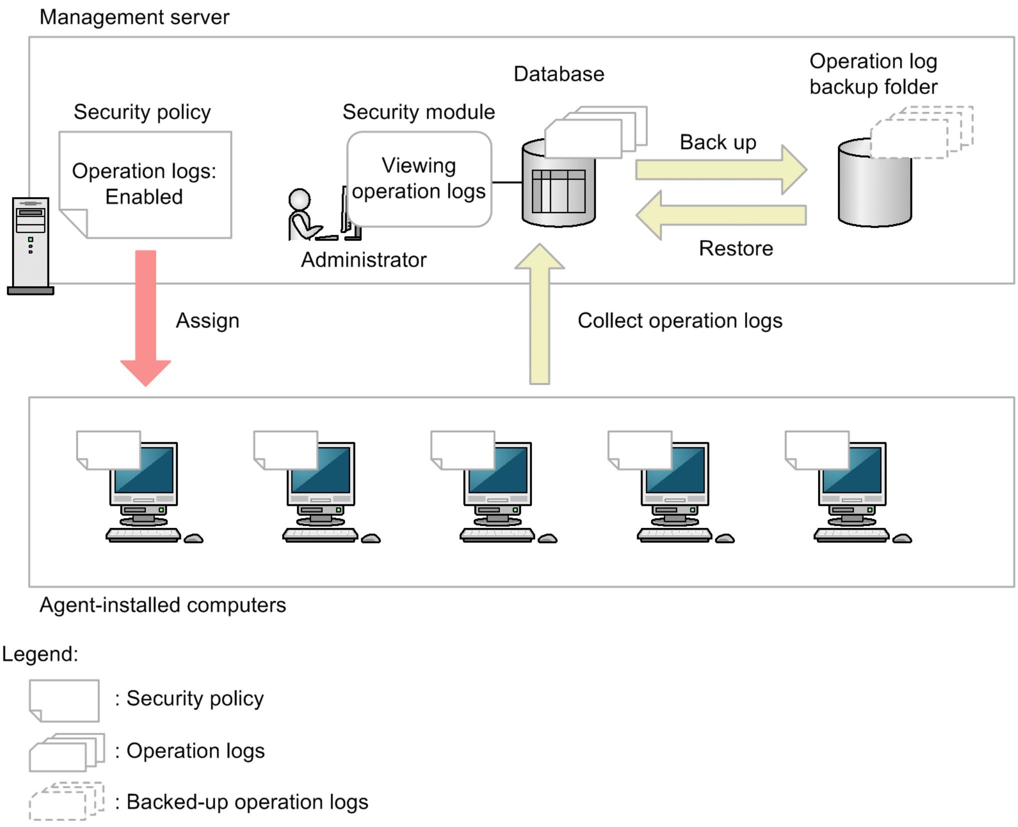
Item	Description
Operation Date/Time (Browser)	Date and time the operation was performed. The displayed value is converted to the local time of the computer on which operation logs are displayed. Display example: `2011/10/01 22:00:01`
Operation Date/Time (Source)	Date and time the operation was performed. The displayed value is converted to the local time of the computer on which operation logs were collected. Display example: `2011/10/02 17:11:51`
Time Zone	Time zone of the computer on which the operation was performed. The difference with UTC is displayed. In the **Log Details** dialog box, this value is displayed in the **Operation Date/Time (Source)** item. Display example: `GMT+09:00`
User Name	Account name of the user who was logged on to the source computer. Display example: `Hostname\user1`
Execute Account	Account name of the user who executed the source program. Display example: `Hostname\user1`
File Version	File version displayed on the **Version** tab of the **Properties** dialog box for the operation-target file. Display example: `1.0.0.111`
File Name	Name of the operation-target file including the file path. Display example: `C:\TEMP\game.exe`
File Created Date/Time	Date and time the operation-target file was created. Display example: `2011/10/01 22:00:01`
File Last Modified Date/Time	Date and time the operation-target file was updated. Display example: `2011/10/02 22:00:01`
File Size	Size of the operation-target file. Display example: `10.2KB`
Original File Drive Type	When a suspicious file operation is detected, this item indicates where the original file was located. • Other • Local Disk • Network Drive • Removable Disk • CD-ROM • RAM Disk • Web • FTP • E-mail Display example: `RAM Disk`
Original File Created Date/Time	Date and time the operation-target file was first detected after collection of operation logs started. Display example: `2011/10/01 22:00:01.159`
Source File Name	Full path to the source file (or folder), or URL of the website to which the file was uploaded or from which the file was received via FTP. For a network drive, the name is indicated in UNC format. If an email with attachment was received, this item indicates the email header. If an attached file was saved, this item indicates the attached file name without a path name. Display example: `\\dmp110\share`
Source File Drive Type	Type of drive in which the source file was stored. • Other • Local Disk • Network Drive • Removable Disk

Item	Description
Source File Drive Type	- CD-ROM - RAM Disk - Web - FTP - E-mail Display example: `Local Disk`
Destination File Name	Full path to the destination file (or folder), or URL of a website to which the file was uploaded or sent via FTP. For a network drive, the name is indicated in UNC format. If an email with attachment was sent, this item indicates the email header. If an email with attachment was received, this item indicates the attached file name without a path name. Display example: `c:\work\program`
Destination File Drive Type	Type of the drive in which the destination file was stored. - Other - Local Disk - Network Drive - Removable Disk - CD-ROM - RAM Disk - Web - FTP - E-mail Display example: `Network Drive`
Printer Name	Name of the printer used for printing. Display example: `printserver01`
Printed Document Name	Name of the printed document. Display example: `FunctionalSpecification.doc`
Printed Page Count	Total number of printed pages. This item is not displayed if it cannot be collected. Display example: `5`
Drive Type	Type of the drive connected to the computer. Information is displayed as a number. - Other - Local Disk - Network Drive - Removable Disk - CD-ROM - RAM Disk - Web - FTP - E-mail Display example: `Network Drive`
Drive Name	Name of the drive connected to the computer. Indicated as `A:` to `Z:`. Display example: `G:`
Device Name	Name of the connected device. Display example: `Hitachi USB` *xxxxx*
Serial #	Serial number of the connected device. Display example: `1234567890ABCD`
Device Type	Type of connected device.

Item	Description
Device Type	Display example: `Disk Drive`
Device category	Type to distinguish a device. Display example: Built-in SD card
Device Instance ID	Device instance ID of the connected device. Display example: `USB\VID_`*xxxx*`&PID_`*xxxx*`\1234567890ABCD`
Web Page Title	Title of the web page the user accessed. Display example: `Hitachi`
URL	URL of the web page the user accessed. Display example: `http://www.hitachi.co.jp/`
Window Title	Caption of the active window. Display example: `game`
Software Name	Name of the software program for which startup was blocked. Displays the name of the blocked software program set in the security policy. Display example: `game`
Software Version	Version of the software program for which startup was blocked. Displays the version of the blocked software program set in the security policy. Display example: `5.1.2600.5512`

2.10.2 Managing operation logs on the management server

Operation logs collected on a computer managed online are stored in an operation log backup folder via the management server. By restoring the operation logs to a database on the management server, you can view the operation logs from the **Operation Logs** view of the Security module.



Storing the operation logs on the management server

The operation logs collected on the management server are stored in an operation log backup folder. If automatic restoration of operation logs is enabled, the operation logs are automatically restored to the operation log database. To view the operation logs stored in the backup folder, restore them from the backup folder to the database.

Operation logs collected on the management server are saved in the database for about one month. The operation logs that are older than about one-month-old are automatically deleted from the database.

Note that if automatic backup of operation logs has been configured in Setup, operation logs are automatically backed up every day. You can view the backup operation logs by temporarily restoring them from the backup folder to the database. After deleting the restored operation logs, you can restore the operation logs for a different time period to the database. This enables you to view past operation logs.

Important note

If operation logs have not been collected on the management server, the **Operation Logs** view is not displayed.

Tip

We recommend that you use high-capacity drives, such as RAID or NAS, for the backup folder because large amounts of data might be stored in the backup folder over a long period of time.

Storing the operation logs on a user's computer

You can store operation logs for a certain amount of time on a user's computer in case the computer fails to connect to the management server. You can specify a time period to keep the operation logs in the security policy. Operation logs that are not sent to the management server are temporarily saved on the computer, and resent to the management server at the time specified by the security policy.

The operation logs can easily become large amounts of data. Therefore, set the time period for which the operation logs are kept after calculating the required disk capacity, based on the following formula:

260 x Time period (days) = Required disk capacity (KB)

Note: The required disk capacity varies depending on the acquired operation log items and user operations.

Important note

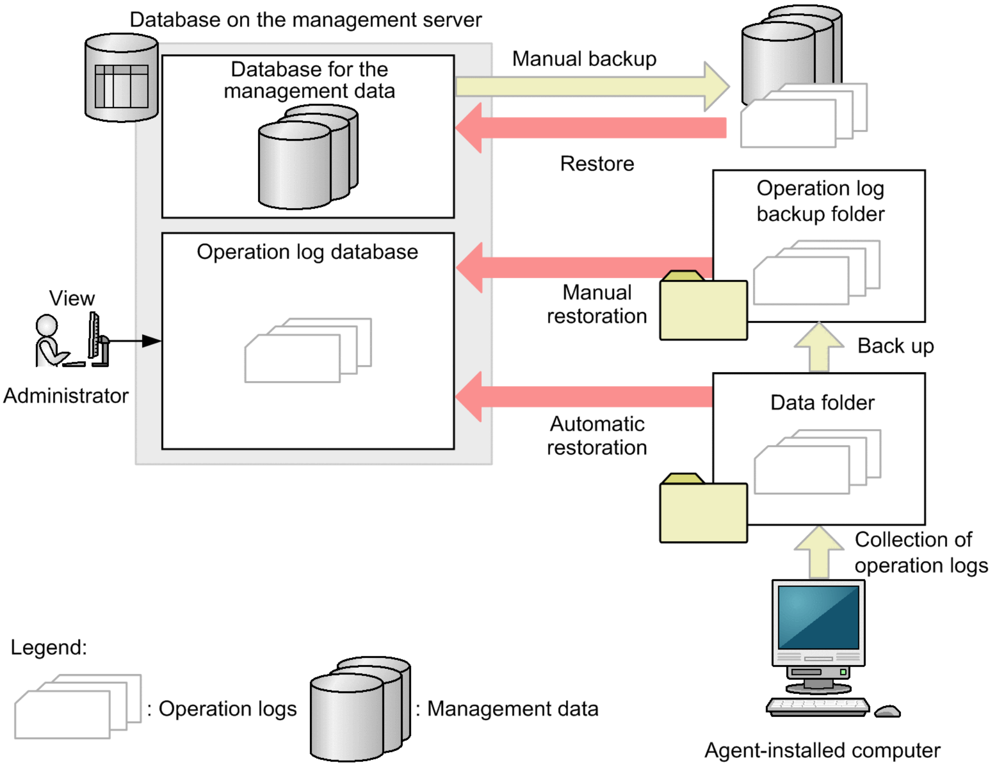
If processing is interrupted while the computer is communicating with the management server, some operation logs might be duplicated because the same data is notified at the next connection.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(1) Backing up and restoring operation logs on the management server

If the management server is configured to back up operation logs, you can collect a history of user operations as operation logs, and save them in an operation log backup folder.



Operation logs are collected from agent-installed computers at an interval specified by the security policy. The collected operation logs are accumulated in a data folder, and then stored in an operation log backup folder. You can also automatically restore collected operation logs to the operation log database.

The operation logs that have been restored to the operation log database can be viewed in the **Operation Logs** view in the Security module. To check past operation logs, restore them to the database, and then view the past operation logs in the **Operation Logs** view. You can clear the data in the database for restoration if you no longer need to view the data.

Note that backing up or restoring databases using Database Manager does not back up or restore the operation log database. You must back up or restore the operation log data manually.

> **Important note**
>
> When the management server has been configured in Setup so that operation logs are not collected, even if you enable collection of operation logs in a security policy, the operation logs collected from a computer are not saved.

> **Important note**
>
> Operation logs collected from a computer are not saved if the operation date and time of the operation logs is before the year 2000, or after more than 7 days from the current time on the management server.

(2) Backing up operation logs on the management server

Operation logs collected from computers are accumulated in a data folder and stored in the operation log backup folder once an hour.

Data to be backed up

Backup files for operation logs grouped by date with each group stored in a date folder, and stored in the **Operations log backup folder** specified during the Setup.The format of the date folder is `OPR_DATA2_`*YYYYMMDD*.

Size required for backup

The following conditions are used as guides to explain how to calculate the size required for backing up operation logs.

- Number of managed computers: 10,000 machines
- Number of occurrences of operation logs per day: 2,000 logs/machine
- Data size of an operation log: 500 bytes
- Compression ratio of a ZIP file: 6.7%

Note: All the above conditions are set as guides.

Size of operation log data

Size of operation log data per machine: 2,000 (logs) x 500 (bytes) = about 1 (MB)

Size of operation log data for 10,000 machines: 1 (MB) x 10,000 (machines) = 10 (GB)

Size of operation log data for 10,000 machines for one month (20 business days): 10 (GB) x 20 (days) = about 200 (GB)

Size of backup file data

Size of backup file data per machine: 1 (MB) x 6.7% = about 67 (KB)

Size of backup file data for 10,000 machines: 67 (KB) x 10,000 (machines) = about 670 (MB)

Size of backup file data for 10,000 machines for one month (20 business days): 670 (MB) x 20 (days) = 13.4 (GB)

Thus, you can calculate the sizes of operation log data and backup file data. Secure the free space for the database and for the backup-destination drive, considering the number of managed computers and the collection period of the operation logs.

Mail notification about free space shortage

You can configure to receive a mail notification when the free space on the backup destination is insufficient. The following are the triggers for mail notification:

Backup fails

If backup fails due to a shortage of the backup-destination drive capacity, a **Critical** error event is displayed in the Events module. In this case, a mail notification is automatically sent if mail notification of such events has been set.

Periodic monitoring detects free space shortage

If free space on the backup-destination drive is insufficient, an error event is displayed in the Events module. In this case, a mail notification is automatically sent if mail notification of such events has been set. Note that you can change the threshold value to output the insufficient free-space event by editing the properties of the configuration file. For properties of the configuration file, see A.5 Lists of properties.

(3) Restoring operation logs to the management server

To view operation logs, you need to restore them to the operation log database. You can restore operation logs automatically or manually.

> **Tip**
>
> The maximum number of days of operation logs that can be restored to the database can be configured in the management server setup. The maximum is 500 days.

Automatic restoration

Operation logs are automatically restored according to the storage period specified in the **Operation Log Settings** in the Settings module.

On average, a managed computer generates 2,000 operation logs per day. Restoring an excessive amount of operation logs might overload the system. To prevent system overload, we recommend that you limit the types of operation logs to be collected, or reduce the number of managed computers.

Use the following formula as a guideline for an operation that does not overload the system:

Number of managed computers x 2,000 logs x Period for storing automatically restored operation logs (days) x $x <$ 300,000,000

x: A coefficient depending on the collected operation log items. Specify the sum of the following items to be collected:

- Start and termination of the programs: 0.26
- File and folder operation: 0.06
- Web access: 0.36
- Window operation: 0.3

This calculation is not necessary for non-bulky operation log types including power-on/shut-down, logon/logoff, file operations via a network, and print operation.

For example, if you want to collect operation logs for web accesses and window operations for 10,000 managed computers, the storage period is as follows:

10,000 computers x 2,000 logs x Period for storing automatically restored operation logs (days) x 0.66 < 300,000,000

Period for storing automatically restored operation logs (days) = 22.7 days ≈ about 1 month (20 business days per month)

Manual restoration

You can restore operation logs by specifying a time period that includes the operation log you want to investigate. You can also specify the target computer you want to restore operations logs from,

> **Important note**
>
> The backup files in the operation log backup folder are stored, based on the time zone on the management server. Therefore, if different time zones are used between the management server and the computer running the web browser, you must use the time zone on the management server when you specify a period for manual restoration of operation logs.

> **Important note**
>
> The data that appears when you place a mouse cursor over a date on the time chart in the **Operation logs** view in the Security module are the status and the number of operation logs. Therefore, if different time zones are used between the management server and the computer running the web browser, the number of operation logs displayed on the tool tip and the number of operation logs filtered by a date might differ.

> **Important note**
>
> Depending on the environment, it might take two or more hours to restore 3 months of operation logs for 200 computers. To reduce the time required for restoration, narrow the scope of restoration.

(4) Periodically exporting operation logs

You can export collected operation logs in a CSV format when you want to save them in a CSV file, or import them to other systems. In the **Operation Log Settings** view in the Settings module, select the **Periodically export operation logs.** check box to export the operation logs to the export folder in the operation log backup folder every hour. The following describes the output information of the CSV file.

Output destination of the CSV file

operation-log-backup-folder`\export`

Output file name

`oplog_`*YYYYMMDD*`_`*NNN*`.csv`

YYYYMMDD: Date on which the periodic export was performed.

NNN: Serial number from 001 to 999. If the number exceeds 999, an event is generated.

The files are output in the order of the operation logs.

File size

A file is 2 GB or less. A file exceeding 2 GB is divided,

Character code

UTF-8

Output format

For details on the output format, see the description of the output format for the exported operation logs in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

> **Important note**
>
> Because an output CSV file is not compressed, enabling periodic export of operation logs requires a large amount of disk space. Compress or back up the CSV files in other disks if necessary. For a guideline on the disk space required when periodically exporting output logs, see 4.5.3 Guidelines for disk space requirements for operation log backup folder.

(5) Additional cache of the operation log database

To increase the search performance of the operation logs, you can set a cache size when you set up the management server. Specify 1 GB for 2,500 managed computers. The additional cache of the operation log database can be set in a 64-bit environment.

(6) Recreating an index of the operation log database

To maintain search performance of operation logs, an index of the operation log database is recreated once a day (between 01:00 and 02:00). This applies to the automatically backed-up operation logs.

An operation log search operation might become slower during recreation of the index of the operation log database. Execute the operation log export command (`ioutils exportoplog`) after the index is recreated.

> **Tip**
>
> You can reduce the time spent on searching for operation logs by filtering the search target devices (for example, by group, location, source, or user name).

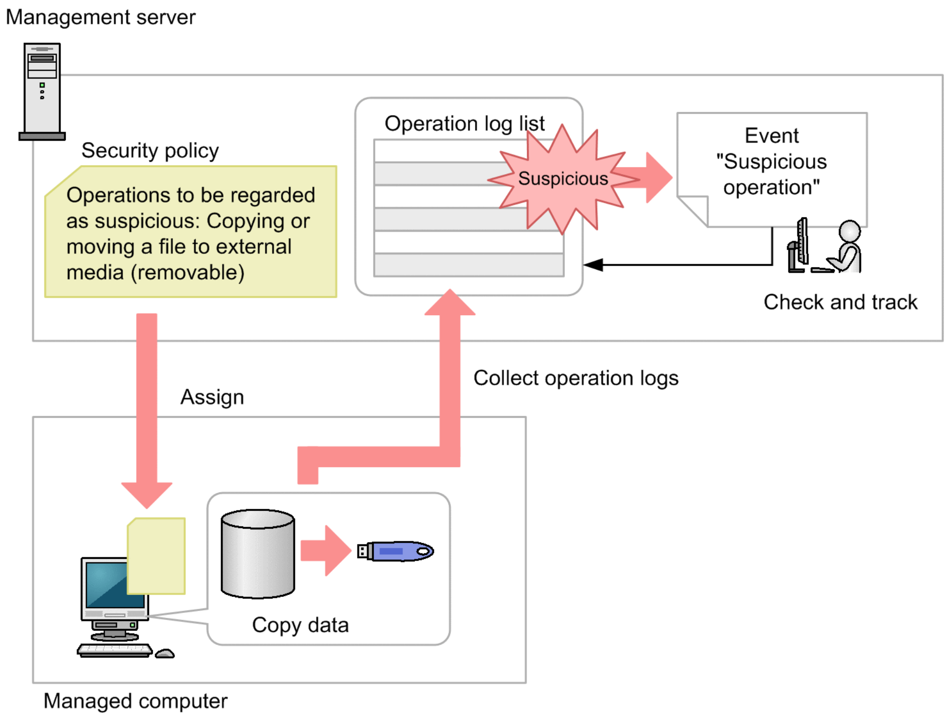
Related Topics:

- A.8 Times at which functions are executed automatically

2.10.3 Investigating suspicious movements of files from systems using operation logs

You can collect computer user's operations as operation logs. Also, by setting the conditions for determining which operations are to be regarded as suspicious in a security policy, suspicious operations that might lead to information leakage can be detected automatically. You can check for operations that might lead to information leakage, and take appropriate actions before the damage expands.

The following figure shows the flow when operation logs are collected for investigation of suspicious operations.



To detect suspicious operations, you need to set the conditions for determining which operations are to be regarded as suspicious in a security policy. Suspicious operations can be detected on a computer to which a security policy that defines these conditions has been applied.

If you detect that a file has moved out of a system, you need to investigate where the file was moved from to prevent confidential information leakage. When a suspicious operation is detected, it is reported as a Suspicious Operations event. You can check the event in the operation log, and track the source of the file that moved out of the system.

Tip

You can export operation logs by executing the `ioutils exportoplog` command. We recommend that you export operation logs when you want to use the contents of operation logs (for example, in documents).

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(1) Collecting logs for suspicious movements of files from systems

JP1/IT Desktop Management 2 can automatically check the contents of operation logs, and monitor suspicious operations that might lead to information leakage due to file movement from a system.

In a security policy, specify the operations that are to be regarded as suspicious and set the conditions for those operations to be regarded as suspicious.

Operations to be regarded as suspicious:

- A monitored file is attached to an email and sent to an email address[#1, #2] set in the policy.
- A monitored file is uploaded to a web server[#1, #2, #3] or an FTP server[#1, #2, #3] that is set in the policy.
- A monitored file is copied or moved to external media.

A file to be monitored satisfies one of the following conditions:

- A file received as an attachment of an email that was sent from an email address[#1, #4] set in the policy
- A file downloaded from a web server[#1, #3, #4]or an FTP server[#1, #3, #4] that is set in the policy
- A file newly created in the organization
- A file that exists since before operation logs were collected

#1: Addresses that partially or completely match the specified address are applicable.

#2: When a monitored file is moved to an address that does not match any of the specified addresses, the operation is determined to be suspicious.

#3: If an IP address is specified, the IP address converted from the host name contained in the address of the downloaded file and an address that partially matches the specified IP address are applicable.

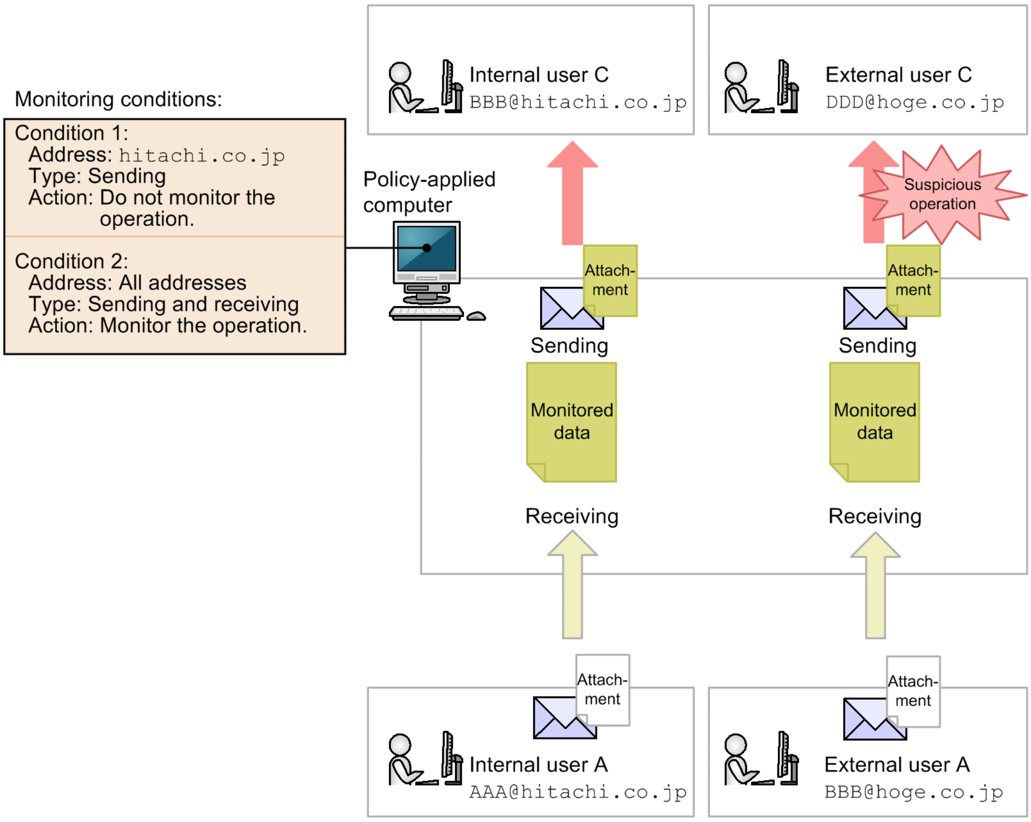
#4: When a file is moved from an address that does not match any of the specified addresses, the file is determined to be monitored.

When a monitored file is acquired, the operation of acquiring the file is not regarded as a suspicious operation. When a monitored file is moved from the system to outside, the operation is regarded as a suspicious operation, and an event is issued.

Example of monitoring emails with attachments

For example, configure the settings as shown in the figure below if you want to perform monitoring as follows:

- Monitor movements of attached files to outside the company.
- Do not monitor movements of attached files within the company (where the address `hitachi.co.jp` is used).



Monitoring conditions:

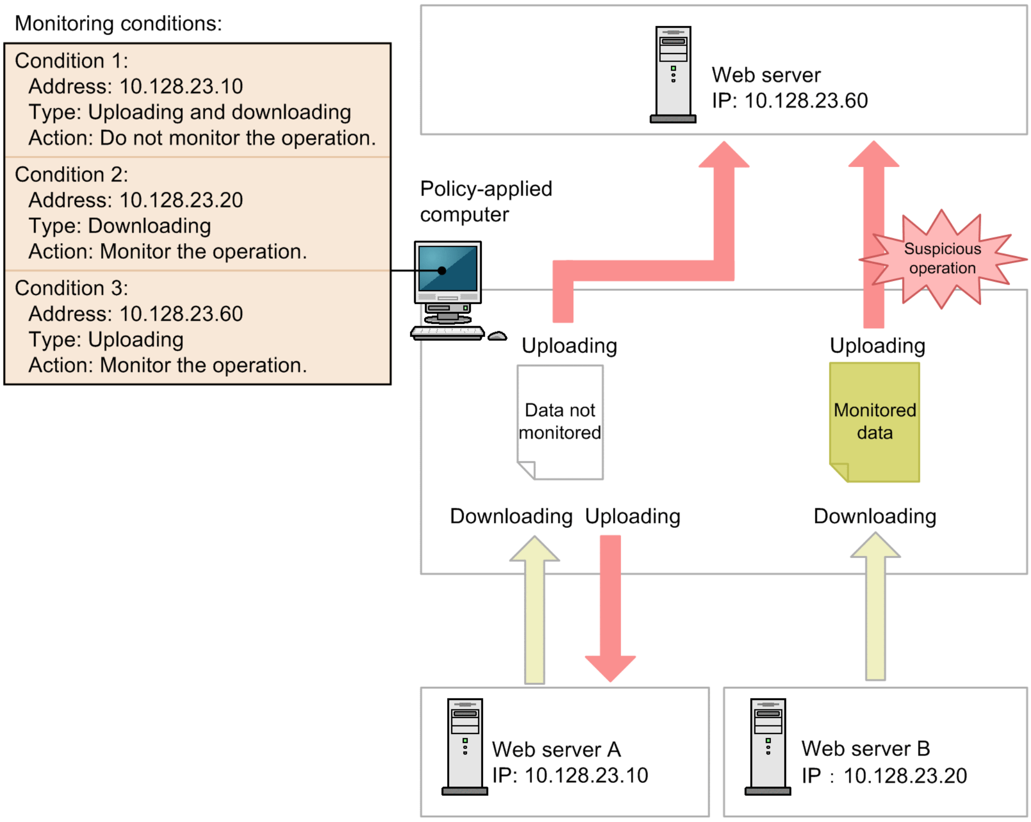
Condition 1:
Address: hitachi.co.jp
Type: Sending
Action: Do not monitor the operation.

Condition 2:
Address: All addresses
Type: Sending and receiving
Action: Monitor the operation.

Example of monitoring a web server or FTP server

For example, configure the settings as shown in the figure below if you want to perform monitoring as follows:

- Do not monitor uploading Web server A's data to outside because the data can be open to the public.
- Monitor uploading Web server B's data to outside because the data is sensitive.



Monitoring conditions:

Condition 1:
Address: 10.128.23.10
Type: Uploading and downloading
Action: Do not monitor the operation.

Condition 2:
Address: 10.128.23.20
Type: Downloading
Action: Monitor the operation.

Condition 3:
Address: 10.128.23.60
Type: Uploading
Action: Monitor the operation.

The products that support monitoring of suspicious operations are the same as the products that support collection of operation logs. For details, see the supported products described in #2, #3, and #4 in 2.10.1 Types of operation logs that can be collected.

Important note

Suspicious operations can be correctly detected only when the file system of the target computer is NTFS. If the file system is not NTFS, the original file information is not set and suspicious operations might not be correctly detected.

2.10.4 Conditions for determining whether a file is to be monitored for suspicious file movements

When files are moved to an agent-installed computer from an external source or are moved from an agent-installed computer to an outside destination, they are checked to determine whether they are monitoring targets for suspicious operations. The following table shows the conditions for these checks.

Determining whether a file moved to a system is to be monitored for suspicious operations

Operation log collection item	Whether a file is to be monitored for suspicious operations
Copy file	C#1
Move file	C#1
Rename file	C#1
Create file	Y
Delete file	C#1
Web Access (Upload)	C#1, #2
Web Access (Download)	C#3
FTP (Send File)	C#1
FTP (Receive File)	C#3
Send Mail (Attachment File)	C#1
Receive Mail (Attachment File)	C#3
Save Attached File	C#1
Print	N

Legend: Y: The file should be monitored. C: The file should be monitored depending on certain conditions. N: The file does not need to be monitored.

#1: The file should be monitored when the drive is a local drive, remote drive, or RAM drive, or when the drive information cannot be collected. The file does not need to be monitored when the drive is a removable drive or CD-ROM drive.

#2: A file uploaded from Internet Explorer 10 or 11 does not need to be monitored.

#3: The file should be monitored when the operation matches the conditions defined for monitoring targets, or when the operation does not match any of the conditions.

Determining whether movement of a file from a system is determined to be a suspicious operation

Operation log collection item	Whether an operation is determined to be a suspicious operation
Copy file	C#1
Move file	C#1
Rename file	N
Create file	C#2
Delete file	N
Web Access (Upload)	C#3, #4, #5
Web Access (Download)	C#6
FTP (Send File)	C#3

Operation log collection item	Whether an operation is determined to be a suspicious operation
FTP (Receive File)	C#6
Send Mail (Attachment File)	C#3
Receive Mail (Attachment File)	N
Save Attached File	C#6
Print	N

Legend: C: An operation is determined to be suspicious depending on a certain condition. N: An operation is not determined to be suspicious.

#1: For the conditions, see the table *Conditions for determining whether an operation is determined to be suspicious when a file is copied or moved from a system* below.

#2: For the conditions, see the table *Conditions for determining whether an operation of moving a file from a system is determined to be suspicious for file creation* below.

#3: An operation is determined to be suspicious when the operation matches one of the conditions defined for determining suspicious operations or when the operation does not match any of the conditions.

#4: In Internet Explorer 10 or 11, all the files are determined to be suspicious.

#5: In Internet Explorer 10 or 11, a check for suspicious operation is performed when a file upload is started. Therefore, a suspicious operation can be detected even when an upload is interrupted by a communication error. For the conditions, see the table *Conditions for determining whether an operation of moving a file from a system is determined to be suspicious for receive operations* below.

#6: For the conditions, see the table *Conditions for determining whether an operation of moving a file from a system is determined to be suspicious for receive operations* below.

Conditions for determining whether an operation is determined to be suspicious when a file is copied or moved from a system

Source	Destination					
	Local drive	Remote drive	Removable drive	CD-ROM drive	RAM drive	Drive information cannot be collected
Local drive	N	N	C#	C#	N	C#
Remote drive	N	N	C#	C#	N	C#
Removable drive	N	N	N	N	N	N
CD-ROM drive	N	N	N	N	N	N
RAM drive	N	N	C#	C#	N	C#
Drive information cannot be collected	N	N	C#	C#	N	C#

Legend: C: An operation is determined to be suspicious depending on a certain condition. N: An operation is not determined to be suspicious.

#: An operation is determined to be suspicious when **Copy/Move the File to External Device** is selected in the security policy.

Conditions for determining whether an operation of moving a file from a system is determined to be suspicious for receive operations

Source	Destination					
	Local drive	Remote drive	Removable drive	CD-ROM drive	RAM drive	Drive information cannot be collected
Any source	N	N	C#	C#	N	C#

Legend: C: An operation is determined to be suspicious depending on a certain condition. N: An operation is not determined to be suspicious.

#: An operation is determined to be suspicious when **Copy/Move the File to External Device** is selected in the security policy.

Conditions for determining whether an operation of moving a file from a system is determined to be suspicious for file creation

Source	Destination					
	Local drive	Remote drive	Removable drive	CD-ROM drive	RAM drive	Drive information cannot be collected
No source	N	N	C#	C#	N	C#

Legend: C: An operation is determined to be suspicious depending on a certain condition. N: An operation is not determined to be suspicious.

#: An operation is determined to be suspicious when **Copy/Move the File to External Device** is selected in the security policy.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

2.10.5 Collecting logs for suspicious print operations

Cases of an excessive number of print jobs can be treated as suspicious operations and collected in logs. To collect logs for suspicious print operations, you need to set the conditions for determining suspicious operations in a security policy. Suspicious print operations are detected for the computers to which this security policy is assigned. For details about the conditions for determining that the number of print jobs is excessive, see 2.10.6 Conditions for checking for large numbers of print jobs.

If suspicious print operations are detected, you need to investigate the relevant user name, the number of print jobs, and the times the print jobs were submitted to prevent confidential information leakage. When suspicious operations are detected, a Suspicious Operations event is reported. Based on this event, check the collected operation logs to determine whether the large number of print jobs is problematic considering information leakage or costs.

2.10.6 Conditions for checking for large numbers of print jobs

JP1/IT Desktop Management 2 can detect operations that might lead to information leakage through printing as suspicious operations. In a security policy, specify the operations that are to be regarded as suspicious operations and set the conditions for regarding those operations as suspicious.

Operations to be regarded as suspicious

- Printing more than a specified number of pages

In print operations that were submitted by a user within one hour, if the total number of print pages exceeds the number of pages set in the security policy, those print operations are detected as suspicious operations. When suspicious operations are detected, the counter for the print pages is cleared. Therefore, if suspicious operations submitted by a user were detected within the previous hour, the count of print pages for the user restarts from the next print operation without including the print operations that were detected as suspicious.

As the number of print pages reported in an event, the total number of print pages in the previous hour is displayed regardless of whether suspicious print operations were detected.

If a computer is shut down, the page count for the print operations performed by a user before the shutdown is cleared and is not included in the total count of the number of print pages for suspicious operations or for an event after the computer restarts.

2.10.7 Prerequisites and notes on collecting operation logs

(1) Notes on collecting operation logs

- Do not enable operation logs on a computer on which 64-bit OS is running and VMWare Server has been installed. If you enable operation logs, the guest OS for VMWare Server might not start.
- If processing is forcibly terminated after operation log data was sent from an agent-installed computer to the management server and before the operation log is deleted from the computer, the same operation log data might be collected twice.

(2) Notes on power-on/shut-down operation logs

- When an agent is overwrite-installed, a computer power-on/shut-down operation log is acquired.
- If the Fast Boot feature is enabled in a computer running Windows 8.1 or Windows 8, a power-on or shut-down operation log might not be acquired when the computer is started or shut down.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(3) Information and notes about operation logs for startup and blockage of programs

- Startup and blocking of programs can be collected in operation logs only when the character string that starts the program (including the file name and the folder name) is less than 260 characters.
- If a software program finishes its processing immediately after it starts up, startup and blocking of the program might not be collected because it might finish before it is blocked by the agent.
- The startup of the programs that have any of the following file name extensions can be blocked:

- exe
- com
- scr

- If a program in the *JP1/IT Desktop Management 2 - Agent-installation-folder*\bin folder cannot be started from the **Start** menu, startup and blocking of the program will not be collected in operation logs.
- Startup and blocking of the following programs in the *JP1/IT Desktop Management 2 - Agent-installation-folder* \bin folder will not be collected in operation logs.
  - cacls.exe
  - cmd.exe
  - conime.exe
  - cscript.exe
  - jdngsendinv.exe
  - jdngsetup.exe
  - netsh.exe
  - regsvr32.exe
  - secedit.exe

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(4) Prerequisites for and notes on collecting web access operation logs

The following describes the prerequisites and notes when operation logs are collected for web accesses.

Prerequisites

- For Internet Explorer, on the **Advanced** tab of the **Internet Options** dialog box, **Enable third-party browser extensions** must be selected. Note that in Internet Explorer installed on Windows Server 2012, Windows Server 2008, and Windows Server 2003, **Enable third-party browser extensions** is not selected by default.
- The add-on for monitoring web accesses that is added to the user's computer must be enabled.
- For Internet Explorer, in **Toolbars and Extensions** (which is displayed when you select **Manage Add-ons** from the **Tools** menu), the JP1/IT Desktop Management 2 - Agent add-on must be enabled.

> **Tip**
>
> An add-on for monitoring web accesses is added to the web browser on the agent-installed computer. This add-on monitors and detects web accesses. This add-on detects web accesses. Uploads, downloads, sending, and receiving of files are monitored and detected by the agent.

Notes

- If you start a web browser when all add-ons are disabled, operation logs of web accesses cannot be collected.
- When you open a file or folder in Internet Explorer, operation logs for the web access can be collected.
- Images on a web page cannot be collected.

- If multiple web accesses are performed within a second, the web accesses might not be collected in the operation logs.
- If 15 or more Internet Explorer programs are running at the same time, web accesses might not be collected in the operation logs.
- If Internet Explorer is started immediately after you log on to the Windows, web accesses might not be collected in the operation logs.
- If the Enhanced Protected Mode is enabled in an environment using Internet Explorer 10 or 11, web access operation logs cannot be collected.
- Even if an error occurs during a web access (for example, due to a communication error or because the accessed URL does not exist), operation logs for the web access might be collected.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(5) Information and notes about operation logs collected for file/folder operations

When a user copies, moves, or deletes a folder, information about the operations for all the files and subfolders in the folder can be collected. Note that when a folder is renamed, information about the operation cannot be collected.

Operation logs are collected for the operations performed using Windows Explorer. Therefore, operations performed at the command prompt or by the `COPY` command cannot be collected.

The following describes information about operation logs and notes when operation logs are collected for file or folder operations.

If a user performs an undo operation (by selecting the **Undo** menu or pressing the **Ctrl** + **Z** keys) immediately after a file or folder operation, any of the operation logs in the following table is collected.

Operation performed before an undo operation	Operation log collected during an undo operation
Copy	Indicates that the copied file or folder has been deleted.
Move	Indicates that the moved file or folder has been moved back to the original location.
Rename	Indicates that the file or folder has been renamed to the original name.
Delete	Indicates that the deleted file or folder has been moved back to the original location

When a file operation is performed, operation logs for file creation or deletion that is not directly related to the user's operations (such as operations in the Windows **Recent Items** folder) might be output. Therefore, operation logs that satisfy all the following conditions are not collected:

- The operation is creating or deleting a file.
- The file path includes either of the following folders:
  - %USERPROFILE%\Recent
  - %APPDATA%\Microsoft\Office\Recent
- The file extension is `.lnk`.

Also, for operations (on files or folders under the agent installation folder) that satisfy all the following conditions, operation logs are not collected:

- The operation is creating, deleting, or renaming a file, or creating, deleting, or renaming a folder.
- The file path includes the following folders (including subfolders):
    - *JP1/IT Desktop Management 2 - Agent-installation-folder*

Notes

- If a user repeatedly copies the same file or folder, information indicating that a file or folder was created might be collected.
- When a user moves a file or folder to the Windows **Recycle Bin**, the information indicating that the file or folder was deleted (not moved) is collected.
- When a user deletes a file or folder in the Windows **Recycle Bin**, the collected file name or folder name might be different from the name before deletion.
- If a user deletes a large number of files in a batch, the history about the deletion of some of those files might not be collected.
- If a user overwrite-copies or moves a large number of files or folders, information about some file operations might not be collected.
- If a user overwrites a file in the destination folder when moving files, or if a user performs an undo operation (by selecting the **Undo** menu or pressing the **Ctrl** + **Z** keys) for file movement, excess information about deleting the source files might be collected, in addition to the information about moving files.
- Information about the operations for compressed folders (in ZIP format) cannot be collected. However, information about some of such operations might be collected depending on the OS or user operations.
- When the use of USB devices is restricted, information about the file operations on a USB-connected device might not be collected.
- Information about operations of Windows portable devices cannot be collected. However, some operation information might be collected, depending on the OS or device.

When the OS is Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, in addition to the above notes, the following notes also apply:

Notes (Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

- All operations
    - Even when an operation on a file or folder is performed by an application program or at the command prompt, operation logs for some operations might be collected.
    - Information about shadow copy operations and restoration operations from backup cannot be collected. However, some information might be collected.
- Copy
    - When a file is overwritten by a copy operation, if **Copy, but keep both files** is selected in the **Confirm File Replace** dialog box, the following pieces of information are collected:

      - Information indicating that the file name after copying became *file-name-before-copying* (*n*) (where *n* indicates a number) is collected.

      - If the source file is deleted after copying, information about file movement might be collected additionally.

      - If the last modified date and time of the source file is the same as the one of the overwritten file, information indicating that the file names were the same before and after copying is collected.

- If the **Confirm Folder Replace** dialog box is displayed multiple times for one copy operation, excess history of copying the folder and files might be collected.
- If a user copies a file or folder whose name includes parentheses (()), information might not be correctly collected.
- If a user selects multiple files or folders whose names include (*n*) (where *n* indicates a number), and overwrite-copies the files or folders, selecting **Copy, but keep both files** in the **Confirm File Replace** dialog box, information might not be correctly collected.
- If a user performs a redo operation (by selecting the **Redo Copy** menu or pressing the **Ctrl** + **Y** keys) after an undo operation, information about the file operation cannot be collected. Note that for a redo operation for a folder, information can be collected as a folder copy operation.
- If a user copies a series of files or folders whose names include (*n*) (where *n* indicates a number), for the second or later copy operation, information is collected as creation of files or folders.
- If a user selects multiple files or folders, or selects a folder that contains multiple files and folders, and then copies them, information about the operations might not be collected.
- When a user cancels copying in the dialog box that confirms whether to perform an overwrite operation, if the latest modified date and time are the same for the source file and the file that has the same name as the source file in the destination folder, information is collected as a copy operation.

- Move
    - When a file is overwritten due to a user's move operation, if the user selects **Move, but keep both files** in the **Move File** dialog box, information indicating that the name of the file after moving became *file-name-before-moving* (*n*) (where *n* indicates a number) is collected. Also, excess information indicating that the file names become the same before moving and after moving is collected.
    - When a user selects multiple files or folders whose names include (*n*) (where *n* indicates a number) and moves the files or folders, if **Move, but keep both files** is selected in the **Confirm File Replace** dialog box, information might not be correctly collected.
    - When a folder is overwritten due to a user's move operation, if the user confirms overwriting by clicking the **Yes** button in the **Confirm Folder Replace** dialog box, the following pieces of information are collected:

      - If files with the same name exist in the source folder and the destination folder, when the folder is merged, only the files are moved and the folders in the source folder are not deleted. At this time, information indicating the folder copy operation is collected.

      - If a user selects **Move and replace** when confirming overwriting of a file, and if the last modified date and time is the same for the source file and the overwritten file, information indicating file copy and delete operations (not a file move operation) is collected.

      - If a user selects **Move, but keep both files** when confirming overwriting of a file, information indicating that the name of the file after moving became *file-name-before-moving* (*n*) (where *n* indicates a number) is collected. If the last modified date and time is the same for the file before moving and the overwritten file, excess information indicating the file copy and delete operations is collected in addition to the information indicating the file move operations. If the last modified date and time is different for the source file and the overwritten file, excess information indicating that the file names became the same for the source file and the destination file is collected.

      - In Windows Vista or a later version of Windows, if a file is moved from a folder that needs elevation of permissions to a drive whose file system is other than NTFS, the type of the original drive might not be collected and the file might not be tracked correctly.
- Rename
    - When a folder is overwritten due to a rename operation performed by a user, the **Confirm Folder Replace** dialog box is displayed. If the user clicks the **Yes** button in this dialog box, the following pieces of information are collected:

    - If a user renames a folder that contains some files, operation logs for creation of the files in the overwritten folder and operation logs for deletion of the files in the source folder are collected. An operation log for deletion of the source folder is not collected. If no files are contained in the source folder, only the operation logs for creation of the subfolders in the new folder are collected.

    - If subfolders with the same name exist in the source folder and in the destination folder, information indicating the creation of the subfolders is collected. At this time, information indicating the deletion of the source folder is not collected.

    - If multiple files or subfolders exist in the source folder, information about some of the file operations might not be collected.

    - Information about operations for the files in the subfolders of the source folder might not be collected.

    - If a user select multiple files or folders, or a folder that contains multiple files and folders and then renames the files and folders in a batch, information about those operations might not be collected.

- Delete
    - If a user performs an undo operation or selects the **Undo** menu after deleting a file, information about the operation of creating the deleted file at the original location, and information about the operation of deleting the file from the Windows **Recycle Bin** are collected. However, for the information about the operation of deleting the file from the Windows **Recycle Bin**, the file name cannot be correctly collected.
    - If a user moves a file from the Windows **Recycle Bin** after deleting the file, information about the operation of moving the deleted file to the original location is collected.
    - Assume that a user select multiple files or folders, or a folder that contains multiple files and folders, delete them, and then select the **Undo** or move the folder or folders from the Windows **Recycle Bin**. In this case, information about those operations might not be collected.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(6) Notes on collecting operation logs for file uploads and downloads

Operations for uploading or downloading files on a web browser can be monitored, and the operation logs for those operations can be collected. The following describes the notes you must keep in mind when collecting operation logs for uploading or downloading files.

Prerequisites

- If your Web browser is Internet Explorer 10 or 11, the **Enable third-party browser extensions** check box must be selected on the **Advanced Settings** tab in **Internet Options**. Note that this check box is cleared by default for Internet Explorer installed in Windows Server 2012, Windows Server 2008, and Windows Server 2003.
- If your Web browser is Internet Explorer 10 or 11, the add-on for upload monitoring that is added to the user's computer must be enabled.

  If you register the add-on for file upload monitoring, a message prompting you to select if you want to enable the add-on appears. If you enable the add-on and restart Internet Explorer, file upload monitoring starts.
- If your Web browser is Internet Explorer 10 or 11, the *JP1/IT Desktop Management 2 - Agent* add-on must be enabled in the list of add-ons displayed by selecting **Tools**, **Manage Add-ons**, and then **Toolbars and Extensions**.

Notes

- For web uploads executed by unusual upload processing (such as SOAP, WebDAV, Flash, Silverlight), operation logs are not collected.

- If the folder for storing the internet temporary files for Internet Explorer is changed, operation logs might be collected even if no web download operation is performed. To collect operation logs correctly, immediately restart Internet Explorer.
- If the Enhanced Protected Mode is enabled in an Internet Explorer 10 or 11 environment, operation logs for file uploads and downloads cannot be collected.
- In Internet Explorer 7, 8, and 9, an operation log is collected when uploading of a file is completed. In Internet Explorer 10 and 11, an operation log is collected when uploading of a file is started. Therefore, in Internet Explorer 10 and 11, an operation log can be acquired even when the uploading operation is interrupted by an error or other cause.
- If a user uploads multiple files simultaneously to an HTML5 upload site by using Internet Explorer 10 or 11, an operation log for only a single file is acquired.
- When a user uploads a file by using Internet Explorer 10 or 11, if encoding differs between the Web page from which data was uploaded and the data sent from the browser to the destination, the file name in the acquired operation log will become garbled. If garbling occurs when, for example, encoding conversion fails, the file name of the operation log will become `unknown`.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(7) Information and notes about operation logs collected when emails are sent and received

Among the emails sent and received by users via email clients, you can collect operation logs for the operations of sending and receiving emails with attachments. The following provide information and notes about when operation logs are collected for the operations of sending and receiving emails.

The following table shows the email clients for which operation logs can be collected.

Email client	Version
Microsoft Outlook Express	6
Microsoft Outlook	2002
	2003
	2007
	2010
	2013
Windows Mail	6
Windows Live Mail	2009, 2011, or 2012

The table below shows the email operations for which operation logs can be collected. Note that when multiple attached files are sent or received, operation logs are collected for individual attached files.

Email operation that can be collected	Protocol
Receive	POP3, APOP, or IMAP4
Send	SMTP or ESMTP

Notes

- If communication is encrypted by SSL/TLS (such as SMTP over SSL or POP3 over SSL), operation logs are not collected.
- If emails are encrypted by S/MIME encryption, PGP encryption, or other encryption methods, operation logs cannot be collected.
- When an email is sent, if multiple files with the same contents are attached to the email, information about the files moved from the system is not correctly collected. For the operation source file name and the drive type, the name of the file last loaded among the attached files with the same contents and the drive type are displayed.
- If an email to which a file with zero bytes is attached is sent, the operation source file name might be different from the name of the file actually sent.
- If emails sent in TNEF format of Microsoft Outlook are sent or received, information about the attached files might not be correctly collected in the operation logs for the operations of sending and receiving emails. Therefore, file tracking or detection of suspicious file movements from the system might not be possible.
- If the number of attached files per email exceeds 200, it might not be possible to collect operation logs.
- If `Content-type` in the MIME header is either of the following, the attachment is not treated as an attached file:
    - application/pkcs7-mime, application/pkcs7-signature, or application/pkcs10 (digital signature)
    - multipart/alternative (such as HTML mails)

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(8) Notes on collecting operation logs when attached files are saved

You can collect operation logs when attached files are saved from an email a user received using a specific mailer to a local disk or another location. Listed below are some notes on operation logs that are collected for the operations of saving attached files.

The following table shows the email clients for which operation logs can be collected.

Email client	Version
Microsoft Outlook Express	6
Microsoft Outlook	2002
	2003
	2007#
	2010#
	2013#
Windows Mail	6
Windows Live Mail	2009, 2011, or 2012

#: If attached files are saved with the network drive specified as the destination, file names that are different from the saved file names will be collected as the destination file names in the operation logs.

Notes

- When an email (to which multiple files with the same contents are attached) is received and the attached files are saved, the name of the file last received among the attached files with the same contents will be displayed as the operation source file name.
- In Windows Vista or a later version of Windows, if either of the following operations is performed in the email client's window, operation logs for saving attached files might not be collected.
  - Select attached files, and drag and drop the files to Windows Explorer or the Desktop.
  - Select files, click **Copy**, and then **Paste** to save the files.
- If attached files are saved from an email that was received before collection of operation logs started, the operation logs for the operations of saving the attached files will not be collected.
- If emails in TNEF format of Microsoft Outlook are received, operation logs for the operations of saving attached files might not be collected correctly.
- If the number of attached files per email exceeds 200, it might not be possible to collect operation logs.
- If `Content-type` in the MIME header is either of the following, the attachment is not treated as an attached file:
  - application/pkcs7-mime, application/pkcs7-signature, or application/pkcs10 (digital signature)
  - multipart/alternative (such as HTML mails)

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(9) Notes on collecting operation logs when files are sent and received

You can collect operation logs when a user accesses an FTP site via a web browser and sends or receives files. For the supported web browsers, see the table of prerequisites in 2.10.1 Types of operation logs that can be collected. The following are notes on when operation logs are collected for the operations of sending and receiving files.

Notes

- If FTP over SSL/TLS is used when files are sent or received, operation logs cannot be collected.
- If the Enhanced Protected Mode is enabled in an Internet Explorer 10 or 11 environment, operation logs for FTP receive operations cannot be acquired.
- The URL is collected as the operation source file name when an operation log for file reception is acquired using Internet Explorer.
- As the destination file information in the operation log for FTP send operations, the IP address of the FTP server is collected.
- If the Enhanced Protected Mode is enabled in an Internet Explorer 10 or 11 environment, operation logs for FTP receptions cannot be collected.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(10) Information about, prerequisites for, and notes on operation logs collected for print operations

You can collect operation logs for print operations. The table below shows the printers for which operation logs for print operations can be collected. Note that only the printers set in the **Devices and Printers** dialog box are supported. Note that the printers displayed in the **Devices and Printers** dialog box can be commonly used by all users.

Printer type	Collection of operation logs for print operations
Local printer	Y
Network shared printer	Y #
Internet printer	N
Virtual printer	Y

Legend: Y: Operation logs can be collected for this type of printer. N: Operation logs cannot be collected for this type of printer.

#: Information about the number of print pages cannot be collected.

Prerequisites

In the properties for each printer, **Print** and **Manage Documents** must be allowed for all logged on users.

For the network shared printer, the following prerequisites are added.

- The table below shows the supported combination of the agent and the print server.

Agent	Print server	Collection of operation logs for print operations
Windows XP/2003	Windows XP/2003	Y
Windows XP/2003	Windows Vista or later	Y
Windows Vista or later	Windows XP/2003	N
Windows Vista or later	Windows Vista or later	Y
Any	Others	N

  Legend: Y: Operation logs can be collected for this type of printer. N: Operation logs cannot be collected for this type of printer.
- RPC communication must be possible between the print server and the agent PC. If RPC communication is not possible, the problem might be caused by one of the following:
  - The print server is a server based on the Internet Printing Protocol (IPP).
  - A firewall, proxy or NAT is present between the print server and the agent PC.
  - The agent PC's Windows firewall is enabled and **File and Printer Sharing** is not set to **Exceptions**.
- The agent PC's **File and Printer Sharing for Microsoft Networks** must be enabled.
- The print server must be able to resolve the name of the agent PC.
- If the agent PC is Windows Vista or later, the agent PC and the print server must join the same domain, or the credential of the print server must be registered on the Credential Manager of the agent PC. The agent PC needs to reboot after registering the credential.

Notes

- If printing is restricted by Hibun, operation logs for print operations cannot be collected.
- If printing is performed immediately after a printer is added, it might not be possible to collect operation logs for print operations.
- If printing is performed immediately after you log on to the OS, it might not be possible to collect operation logs for print operations.

- If a print job is finished before the print operations are notified to the agent, operation logs for print operations cannot be collected.
- Depending on the printer, multiple printing restriction logs are collected at a single printing.

For the network shared printer, the following notes are added.

- If IPv6 is enabled and rendering of the print job does not work on the client computer, the printing might not be restricted. To operate rendering of print jobs on the client computer, the following settings are required:
  - **Render print jobs on client computers** is enabled.
  - **Enable advanced printing features** is enabled.
- When a network shared printer is used, information about the number of print pages cannot be collected. Therefore, the detection of large numbers of print jobs and the report of User Activity (Print) are out of scope.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(11) Notes on collecting logs for device operations

If prohibited operations are set, you can also collect operation logs for device connection suppression and device connection permission.

Logs of inserting or ejecting media (such as CDs, DVDs, SD cards) into or from drives cannot be collected. The following notes are about collecting operation logs of device operations.

Notes

- Console session users are regarded as the target users. If no one is using a console session, no account name can be collected.
- If a device is connected to the computer for the first time, multiple instances of connecting and disconnecting (detaching) information might be acquired for a single connection.
- If you detach a device from a computer running Windows 8.1 or Windows 8 with the Fast Boot feature enabled while the computer is shutting down, a device disconnection operation log is acquired when the computer is restarted.
- Items might be missing in device connection logs, disconnection logs, block device connections logs, and events acquired in a condition where the device is restricted.
- An operation log cannot be acquired if a device is connected before JP1/IT Desktop Management 2 is started (for example, immediately after the computer is turned on).
- If a device with multiple device instance IDs is connected to a computer, multiple operation logs and events are acquired for the single device. However, only one operation log and event might be acquired when the device is disconnected.
- If you connect a device to a computer for the first time, and drive installation is performed, the same operation log and event might be acquired multiple times.
- In a case where a restart of the computer is required to activate a setting, the connection suppression logs, and connection suppression events are acquired when you apply the setting.
- An operation log is also acquired when the device setting is changed by another product, and the system detects connection or disconnection of the device.
- If a USB device is connected, operation logs cannot be acquired for devices that are not identified as a USB device, Bluetooth device, or imaging device.
- Multiple logs might be acquired if you connect a CD/DVD drive that has a CD or DVD inserted.

- In a case where a restart of the computer is required to activate the deterrence of a device, deterrence logs, disconnection logs, and events are not acquired for the deterrence-target device.
- If a log-acquisition-target device is identified by the OS as a different device, operation logs for the device cannot be acquired. However, if the OS identifies it as another log-acquisition-target device, the device is restricted according to the OS identification.
- If you change the deterrence setting on the same device a number of times in a short period of time, connection logs and disconnection logs might not be acquired.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(12) Notes on collecting operation logs for window operations

You can collect operation logs for window OS operations in the following cases:

- When a window starts and becomes active.
- When the active window is switched by a mouse operation or because the **Alt** + **Tab** keys are pressed.
- When a new window starts during window operations and that window becomes active.

The followings are notes on collecting operation logs for window operations.

Notes

- When the OS is Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, operation logs for windows for which user permissions have been elevated cannot be collected.
- If operation logs for window operations are collected immediately after logon, the logon user name might become null.
- For a window that is created by an application and first displayed without a title and then the title is set, the window title is not collected.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

(13) Prerequisite for collecting source information when checking incoming files and notes on suspicious out-movement of files

You can collect information about the input source of a file when the file is moved to an agent-installed computer. The following are a prerequisite for collecting source information when checking incoming files and notes on suspicious out-movement of files.

Prerequisite

- The file system on an agent-installed computer must be NTFS 5.0 or later.

Notes

- When a file is moved or copied to a drive that was formatted by a file system other than NTFS (such as FAT or ReFS), information related to suspicious operations is deleted. (Such information includes the results of checking incoming files. Such results are necessary for the checking of suspicious out-movement of files.) Therefore, if such files are moved or copied to external media, suspicious file movements from the system might not be correctly detected. Correct detection also might not be possible when the data is processed (such as when a file is compressed or uncompressed).

- On an agent-installed computer on which operation log collection is enabled, if a file is moved or copied by Windows Explorer to a drive that was formatted in a file system other than NTFS (such as FAT or ReFS), the Windows' **Confirm Stream Loss** dialog box might be displayed.

Related Topics:

- 2.10.1 Types of operation logs that can be collected

2.11 Managing assets

You can use JP1/IT Desktop Management 2 to centrally manage information about assets, such as devices, software licenses, and contracts that are managed within an organization.

This will help you efficiently manage assets. You can list assets and manage them as though in a ledger. You can also define relationships between assets. By doing this, for example, you can quickly check the contracts that were made for devices or the usage status of software licenses.

There are two ways you can manage asset information: using Asset Console and using the operation window ofJP1/IT Desktop Management 2. For differences between the two methods and details on asset management using Asset Console, see *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Description*.

Note that these two methods cannot be used at the same time. To maintain consistency of the asset information, you need to select whether you will use Asset Console or not when setting up the JP1/IT Desktop Management 2 system.

This section describes how to manage assets using the operation window of JP1/IT Desktop Management 2.

You can use the operation window of JP1/IT Desktop Management 2 to centrally control asset information including devices, software licenses, and contracts that are managed in the organization. You can list assets and manage them as though in a ledger. You can also define relationships between assets. By doing this, for example, you can quickly check the contracts that were made for devices or the usage status of software licenses. This will help you efficiently manage assets. You can also manage devices that do not have IP addresses, such as displays and USB memory devices, in addition to devices with IP addresses. You can also add customer-specific information as extended information.

JP1/IT Desktop Management 2 supports the following asset management tasks:

Managing hardware assets

You can manage information about owned devices, such as computers, servers, printers, network devices, and USB devices, as hardware asset information. As well as being able to manage detailed information about hardware assets, you can check the status of hardware assets within an organization. You can manage the status, for example, by organizing hardware into categories, such as `In Use`, `In Stock`, or `Disposed`.

Managing software licenses

You can manage information about owned software licenses and the usage status of individual software licenses. You can not only manage the total number of licenses, but also check for computers that use licenses without permission (after licenses are assigned to individual computers).

Managing asset contracts

You can register information about contracts for hardware assets and software licenses (such as support contracts, rental contracts, or lease contracts), and manage the information about individual contracts associated with individual assets. You can check contracts for which the expiration date is approaching, which will help you schedule a work plan.

Managing costs for assets

By managing information about contracts regarding hardware assets and software licenses, you can check the costs for those assets. By utilizing this information, you can check for unnecessary costs or estimate the costs necessary for maintaining assets.

This section describes how to use JP1/IT Desktop Management 2 for those tasks. Refer to the description related to your target task.

2.11.1 List of the fields for asset information

The following tables list the fields for asset information. The following legend is used in the tables below:

Legend: --: Not supported.

Tip

You can add customized fields in addition to the fields shown below.

Tip

You can change the data source and type for some fields. For details, see (3) Types of asset fields that can be customized.

Hardware assets

Field	Description	Data source	Type
Asset #	Set the certificate number or use a unique number that is customized for easy management. This field is used as a mapping key when hardware asset information is imported.	System Administrator	Text
Device Name	Set a name for the asset.	System Administrator	Text
Description	Set information identifying the asset. We recommend that you enter information that will be easily identified when the information is displayed in a list.	System Administrator	Text
Files Attached	Register files related to the asset. If you register data such as the certificate of the hardware asset, you can reduce the time and effort when you want to view detailed information about the hardware asset.	System Administrator	--
Contract Vendor Name	Displays the contract vendor name in the associated contract information.	--	--
Contract Date	Displays the contract date in the associated contract information.	--	--
Asset Status	Set the status of the asset. You can set it as **In Stock**, **In Use**, or **Disposed** by default.	System Administrator	Enumeration
Planned Asset Status	Set the new asset status if you plan to change the asset status. You can set it as **In Stock**, **In Use**, or **Disposed** by default.	System Administrator	Enumeration
Planned Date	Set the date you plan to change the asset status (if you plan to change the asset status). If you set a date, an event or report will be sent to notify you that operations are required for that asset when that date is approaching and on that date.	System Administrator	Date
Last Tracked Date	Set the date stocktaking of the asset was performed. You can also set that this management field is automatically updated.	System Administrator	Date
Department[#1]	Set the department that uses the asset.	The following data sources can be specified: • System Administrator • End User • Active Directory	The following data types can be specified: • Text • Enumeration • Hierarchy

Field	Description	Data source	Type
Department[#1]	Set the department that uses the asset.	• Registry	The following data types can be specified: • Text • Enumeration • Hierarchy
Location[#1]	Set the location of the asset.	The following data sources can be specified: • System Administrator • End User • Active Directory • Registry	The following data types can be specified: • Text • Enumeration • Hierarchy
User Name[#1]	Set the name of the person who uses the asset. If the asset is used by more than one person, set the name of a representative.	The following data sources can be specified: • System Administrator • End User • Active Directory • Registry	Text
Account[#1]	Set information (for example, an employee number) that identifies the user (or a representative) of the asset.	The following data sources can be specified: • System Administrator • End User • Active Directory • Registry	Text
E-mail[#1]	Set the email address of the user (or a representative) of the asset.	The following data sources can be specified: • System Administrator • End User • Active Directory • Registry	Text
Phone[#1]	Set the phone number of the user (or a representative) of the asset.	The following data sources can be specified: • System Administrator • End User • Active Directory • Registry	Text
Registered Date/Time	Displays the date and time the asset information was registered.	--	--

Field	Description	Data source	Type
Last Modified Date/Time	Displays the date and time the asset information was last modified.	--	--
Device Type[#2]	Set the device type. You can select **PC**, **Server**, **Storage**, **Network Device**, **Printer**, **Smart Device**, **Peripheral Device** , **USB Device**, **Display**, **Other**, or **Unknown** by default.	System Administrator	Enumeration
Model[#2]	Set the device model.	System Administrator	Text
Manufacturer[#2]	Set the manufacturer of the device.	System Administrator	Enumeration[#3]
Serial #[#2]	Set the serial number (BIOS information) of the device. This field is used as the mapping key when hardware asset information is imported or when the collected device information is automatically registered as hardware asset information.	System Administrator	Text
CPU[#2]	Set the CPU of the device.	System Administrator	Enumeration[#3]
Total Memory[#2]	Set the memory size of the device.	System Administrator	Text
Storage Capacity[#2]	Set the total capacity of the logical disks on the storage media (such as hard disks and SSDs) on the device.	System Administrator	Text
IP Address[#2]	Set the IP address of the device. If the device has multiple IP addresses, set a representative IP address for management. This field is used as a mapping key when hardware asset information is imported or when the collected device information is automatically registered as hardware asset information.	System Administrator	Text
Subnet Mask[#2]	Set the subnet mask of the device.	System Administrator	Text
MAC Address[#2]	Set the MAC address of the device. If the device has multiple MAC addresses, set a representative MAC address for management. This field is used as a mapping key when hardware asset information is imported or when the collected device information is automatically registered as hardware asset information.	System Administrator	Text
Host Name[#2]	Set the computer name or host name of the device. This field is used as a mapping key when hardware asset information is imported or when the collected device information is automatically registered as hardware asset information.	System Administrator	Text
OS[#2]	Set the OS installed on the device.	System Administrator	Enumeration[#3]
Device Instance ID	Displays the unique ID of a USB device only when **Device Type** is **USB Device**.	--	--
Free Storage Capacity	Set the total free capacity of the logical disks on the storage media (such as hard disks and SSDs) on the device.	System Administrator	Text
Display Type	Set the display type. You can select **CRT**, **Liquid Crystal Display**, **Plasma Display**, **Video Projector**, or **Other**.	System Administrator	Enumeration
Display Size	Set the display size.	System Administrator	Number
Display Graphic Mode	Set the resolution of the display from the following values: **VGA(640 by 480)**, **SVGA(800 by 600)**, **XGA(1024 by 768)**, **WXGA(1280 by 800)**, **SXGA(1280 by 1024)**, **WSXGA+(1680 by**	System Administrator	Enumeration

Field	Description	Data source	Type
Display Graphic Mode	**1050)**, **UXGA(1600 by 1200)**, **FHD(1920 by 1080)**, **WUXGA(1920 by 1200)**, **QXGA(2048 by 1536)**or **Other**	System Administrator	Enumeration
UDID	Set the ID assigned to an Apple smart device.	System Administrator	Text
IMEI	Set the ID assigned to a mobile communication device. This field is used as a mapping key when hardware asset information is imported or when the collected device information is automatically registered as hardware asset information.	System Administrator	Text
IMSI	Set the ID assigned to the subscriber of a mobile communication device (the ID assigned to the SIM card of a smart device).	System Administrator	Text
ICCID	Set the ID assigned to the SIM card of an Apple smart device.	System Administrator	Text
Carrier	Set the carrier that provides communication service for a smart device.	System Administrator	Text
Contract phone number	Set the phone number of a contracted smart device. This field is used as a mapping key when hardware asset information is imported or when the collected device information is automatically registered as hardware asset information.	System Administrator	Text

#1: On an agent-installed computer, a value for this field can be entered from the **End User Form** view.

#2: When hardware asset information is associated with device information, if device information is modified, the corresponding hardware asset information is also modified.

#3: Options are automatically generated based on the collected device information.

Software licenses

Field	Description	Data source	Type
License #	Set a number that uniquely identifies the software license. Use the software license certificate number, or use a unique number that is customized for easy management. This field is used as the mapping key when software license information is imported.	System Administrator	Text
License Name	Set a name for the software license that can be used for management in a list. We recommend that you use a name that clearly shows the contents of the license.	System Administrator	Text
License Type	Set the software license type.	System Administrator	Enumeration
Total Licenses	Set the total number of software licenses that you purchased.	System Administrator	Number
License Total	Displays the number of owned software licenses. For upgrade licenses and downgrade licenses, the number of licenses after upgrade or downgrade is automatically calculated.	--	--
Assigned License Total	Displays the number of licenses that have been assigned to computers.	--	--
Remaining License Total	Displays the number of software licenses resulting from the subtraction of **Assigned License Total** from **License Total**. If the value becomes minus, a license violation might occur due to a software license shortage.	--	--

Field	Description	Data source	Type
Upgrade Source Name	When you are entering asset information for an upgrade license, set the upgrade-source software license.	--	--
Description	Set information identifying the software license. We recommend that you enter information that will be easily identified when the information is displayed in a list.	System Administrator	Text
Files Attached	Register files related to the software license. If you register the certificate of the software license or other data as electronic data, you can reduce the time and effort when you want to view detailed information about the software license.	System Administrator	--
Contract Vendor Name	Displays the contract vendor name in the associated contract information.	--	--
Contract Date	Displays the contract date in the associated contract information.	--	--
License Status	Set the status of the software license. You can select **In Use** or **Expired** by default.	System Administrator	Enumeration
Planned License Status	Set the new status of the software license if you plan to change the status of the software license. You can select **In Use** or **Expired** by default.	System Administrator	Enumeration
Planned Date	Set the date you plan to change the status of the software license (if you plan to change the status of the software license). If you set a date, an event will be sent to notify you that operations are required for that software license when that date is approaching and on that date.	System Administrator	Date
Last Tracked Date	Set the date stocktaking of the software license was performed.	System Administrator	Date
Department	Sets the department that owns the software licenses. You have to set this item only when you want to manage software licenses by department.	System Administrator	The following data types can be specified: • Text • Enumeration • Hierarchy
Managed Software Name	Set the name of the software that corresponds to the software license.	System Administrator	--
Manufacturer	Displays the manufacturer of the managed software associated with the contract.	--	--
Registered Date/Time	Displays the date and time the software license information was registered.	--	--
Last Modified Date/Time	Displays the date and time the software license information was last modified.	--	--

Managed software

Field	Description	Data source	Type
Managed Software Name	Set a name used to manage the software program. For example, when different versions of software programs `Software HOGE 1.0` and `Software HOGE 2.0` are specified in **Installed Software**, if you register the name `Software HOGE` in this field, those software programs can be managed as one type of software program. This field is used as a mapping key when managed software information is imported.	System Administrator	Text and Enumeration#
Description	Set information identifying the software program. We recommend that you describe the software program or enter the relationship with the installed software information.	System Administrator	Text

Field	Description	Data source	Type
License Type	Displays the license type in the associated software license information.	--	--
License Total	Displays the number of licenses in the associated software license information.	--	--
Number of Used Licenses	Displays the total number of devices on which the managed software program has been installed.	--	--
Remaining License Total	Displays the number of software licenses resulting from the subtraction of **Number of Used Licenses** from **License Total**. If the value becomes minus, a license violation might occur due to a software license shortage.	--	--
Assigned License Total	Displays the number of licenses that have been assigned to computers. If **Number of Used Licenses** is greater than **Assigned License Total**, users might have installed software programs without notice.	--	--
Manufacturer	Displays the manufacturer of the software program.	System Administrator	Text and Enumeration#
Registered Date/ Time	Displays the date and time the managed software information was registered.	--	--
Last Modified Date/Time	Displays the date and time the managed software information was last modified.	--	--

#: Options are automatically generated based on the collected software information.

Contracts

Field	Description	Data source	Type
Contract #	Set the contract number or a unique number that is customized for easy management. This field is used as a mapping key when contract information is imported.	System Administrator	Text
Contract Name	Set the name used to manage the contract. We recommend that you use a name that clearly shows the contents of the contract.	System Administrator	Text
Contract Type	Set the contract type. You can select **Fixed**, **Lease**, **Rent**, **Maintenance**, or **Support** by default.	System Administrator	Enumeration
Contract Term	Set the period of time of the contract. As the expiration date approaches, email notification will be regularly sent to the administrator.	System Administrator	Date
Description	Set information for identifying the contract. We recommend that you enter information that will be easily identified when the information is displayed in a list.	System Administrator	Text
Files Attached	Register files related to the contract. If you register data such as the certificate of the contract, viewing detailed information about the contract is quicker and easier.	System Administrator	--

Field	Description	Data source	Type
Contract Vendor Name	Set information about the contract vendor. Contact information enables you to easily contact the vendor when you renew the contract, ask for a quotation, or ask for troubleshooting.	System Administrator	Enumeration
Contract Date	Set the date the contract was made. Register the contract date written in the contract document.	System Administrator	Date
Payment Mode	Set how to pay the costs specified in the contract.	System Administrator	Enumeration
Monthly Cost ($)	Set the monthly cost of the contract.	System Administrator	Number
Total Cost ($)	Set the total cost of the contract.	System Administrator	Number
Contract Status	Set the status of the contract. You can select from **Active**, **Canceled**, or **Expired** by default. If the value for this field has not changed to **Expired** or **Canceled** even after the expiration date for the contract passed, the contract is treated as expired.	System Administrator	Enumeration
Department	Sets the department that owns the assets associated with the contract. You have to set this item only when you want to manage contracts by department.	System Administrator	The following data types can be specified: • Text • Enumeration • Hierarchy
Registered Date/Time	Displays the date and time the contract information was registered.	--	--
Last Modified Date/Time	Displays the date and time the contract information was last modified.	--	--

Related Topics:

- 2.11.7 Importing asset information
- (2) Data sources for asset fields
- (1) Data types for asset fields

(1) Data types for asset fields

For asset fields, the data types below are used. The following legend is used in the tables below:

Legend: Y: Can be input. N: Cannot be input.

Number

This data type is used to input only a number (-2,147,483,647 to 2,147,483,647). If you want to manage a numerical value related to an asset, select this data type. Note that space characters input at the end are ignored.

Date

This data type is used to input a date. If you want to manage a date related to an asset, select this data type.

Enumeration

This data type is used to select a value from options. If you select this data type, you need to create the options. Each option can be a character string with 256 or less characters. If you want to manage information for which the input values must be restricted, select this data type.

Text

This data type is used to specify a character string with 256 or less characters. If you want to manage information for which any input value is allowed, select this data type. You can also restrict the characters that can be input. Note that space characters entered at the end are ignored.

Hierarchy

This data type can be used only for **Department** and **Location** under **Common Fields (Assets and Device Inventory)**. You can set hierarchical options for up to 40 hierarchies. For each option, you can specify a character string with 256 or less characters excluding slashes (`/`). The hierarchical structure edited here will be also used in the menu area in the Assets and Device modules.

Note that when you specify a hierarchical option, the total path to the option (including the path of the upper options) must be specified with 512 or less characters. In this case, a delimiter (which is counted as one character) must be placed at the beginning of the path, at the end of the path, and between options respectively. For example, if you create options in three hierarchies as **Tokyo - Sales - Section1**, the number of characters for the path is 22 (`/Tokyo/Sales/Section1/`).

Tip

For **Department** and **Location**, you can also enter hierarchical information in Enumeration or Text type. In this case, delimit options by using a slash (`/`): for example, `/HeadOffice/Development/Section2/`. You can omit slashes at the beginning and at the end of the character string. This character string (hierarchical information) must have 512 or less characters. When you omit the slashes at the beginning and at the end of the character string, the character string must have 510 or less characters.

Restrictions on characters that can be set for Text type data

The table below describes the types of restrictions on characters that can be set for Text type data. You can also set customized restrictions other than the restrictions shown below.

General restrictions on characters

Characters	Restrictions on characters						
	Every characters	Alphabetic only	Alphanumeric only	Single-byte characters	Double-byte alphabetic only	Double-byte alphanumeric only	Double-byte numbers only
Alphabetic (uppercase)	Y	Y	Y	Y	N	N	N
Alphabetic (lowercase)	Y	Y	Y	Y	N	N	N
Numbers	Y	N	Y	Y	N	N	N
Periods	Y	N	N	Y	N	N	N
Hyphens	Y	N	N	Y	N	N	N
Plus signs	Y	N	N	Y	N	N	N
At marks	Y	N	N	Y	N	N	N
Blanks	Y	N	N	Y	N	N	N

Characters	Restrictions on characters						
	Every characters	Alphabetic only	Alphanumeric only	Single-byte characters	Double-byte alphabetic only	Double-byte alphanumeric only	Double-byte numbers only
Other signs	Y	N	N	Y	N	N	N
Single-byte kana characters	Y	N	N	Y	N	N	N
Double-byte alphabetic (uppercase)	Y	N	N	N	Y	Y	N
Double-byte alphabetic (lowercase)	Y	N	N	N	Y	Y	N
Double-byte numbers	Y	N	N	N	N	Y	Y
Double-byte spaces	Y	N	N	N	N	N	N
Characters other than alphanumeric	Y	N	N	N	N	N	N

Restrictions on characters for people's names

Characters	Restrictions on characters		
	Name 1	Name 2 (using double-byte characters, delimited by a double-byte space)	Name 3 (using double-byte characters, without spaces)
Alphabetic (uppercase)	Y	N	N
Alphabetic (lowercase)	Y	N	N
Numbers	Y	N	N
Periods	Y	N	N
Hyphens	Y	N	N
Plus signs	Y	N	N
At marks	Y	N	N
Blanks	Y	N	N
Other signs	Y	N	N
Single-byte kana characters	Y	N	N
Double-byte alphabetic (uppercase)	N	Y	Y
Double-byte alphabetic (lowercase)	N	Y	Y
Double-byte numbers	N	Y	Y
Double-byte spaces	N	Y	N

Characters	Restrictions on characters		
	Name 1	Name 2 (using double-byte characters, delimited by a double-byte space)	Name 3 (using double-byte characters, without spaces)
Characters other than alphanumeric	Y	Y	Y

Restrictions on characters for phone numbers and email addresses

Characters	Restrictions on characters			
	Phone number 1 (delimited by a hyphen)	Phone number 2 (for international telephone, delimited by a hyphen)	Phone number 3 (without hyphens)	Email address
Alphabetic (uppercase)	N	N	N	Y
Alphabetic (lowercase)	N	N	N	Y
Numbers	Y	Y	Y	Y
Periods	N	N	N	Y
Hyphens	Y	Y	N	Y
Plus signs	N	Y	N	Y
At marks	N	N	N	Y
Spaces	N	N	N	N
Other signs	N	N	N	Y
Single-byte kana characters	N	N	N	N
Double-byte alphabetic (uppercase)	N	N	N	N
Double-byte alphabetic (lowercase)	N	N	N	N
Double-byte numbers	N	N	N	N
Double-byte blanks	N	N	N	N
Characters other than alphanumeric	N	N	N	N

Related Topics:

- 2.11.1 List of the fields for asset information
- (3) Types of asset fields that can be customized

(2) Data sources for asset fields

For asset fields that can be customized, you can set the following four data sources:

System Administrator

The system administrator directly enters information in the operation window, or inputs information by importing a CSV file.

End User

Displays the **End User Form** view on agent-installed computers, and acquires information input by users.

Users need to perform some operations, but this can reduce the workload for the administrator by removing the need to investigate user-specific information and input the information. When this method is used, departments and locations are grouped depending on the acquired information, so you can automate grouping tasks.

Active Directory

When JP1/IT Desktop Management 2 is linking with Active Directory, information managed as computer properties by Active Directory is acquired.

You can utilize the information managed by Active Directory to manage devices and assets.

Registry

Information about the specified registry items is collected. You can manage information that depends on the user environments.

Important note

Only information of Text data type can be acquired from Active Directory.

Related Topics:

- (3) Types of asset fields that can be customized

(3) Types of asset fields that can be customized

The following describes the types of asset fields, data types, and data sources that can be set in the **Asset Field Definitions** view (under **Assets**) of the Settings module.

Types of asset fields

Common Fields (Assets and Device Inventory)

Sets the fields common to the hardware asset information in the Assets module and the device inventory in the Device module. The asset fields under **Common Fields (Assets and Device Inventory)** have already been set by the system. So, you cannot add or delete them.

Custom Fields (Hardware Assets)

Sets the fields in the hardware asset information in the Assets module. You cannot delete the following asset fields:

- **Asset Status** and **Device Type** that have already been set by the system
- An asset field that is specified as a condition for automatically maintaining host groups and IDs managed by Remote Installation Manager

If a custom field value is set as the following conditions, the value cannot be edited or deleted,

- Filter condition
- Automatic maintenance condition for host groups and IDs

Custom Fields (Software License)

Sets the fields in the software license information in the Assets module. **License Status** and **License Type** have already been set by the system. So, you cannot delete them.

Custom Fields (Contracts)

Sets the fields in the contract information in the Assets module. **Contract Status** and **Contract Type** have already been set by the system. So, you cannot delete them.

Editable fields differ depending on the asset field. The following table describes the editable fields.

Asset field		Field name	Data source	Description	Data type
Common Fields (Assets and Device Inventory)#	Department	N	Y	Y	Y
	Location	N	Y	Y	Y
	User Name	N	Y	Y	*1
	Account	N	Y	Y	*1
	E-mail	N	Y	Y	*1
	Phone	N	Y	Y	*1
System-specific asset fields#	Asset Status	N	N	N	*2
	Device Type	N	N	N	*2
	License Status	N	N	N	*2
	License Type	N	N	N	*2
	Contract Status	N	N	N	*2
	Contract Type	N	N	N	*2
Custom asset fields		Y	*3	Y	Y

Legend:

Y: Can be edited.

*1: The data type is fixed to the **Text** type, but characters that can be input can be edited.

*2: The data type is fixed to the **Enumeration** type, but options can be added.

*3: For the custom fields in software license information and contract information, the data source is fixed to **System Administrator**.

N: Cannot be edited.

#: These fields have already been set by the system, so you cannot delete them.

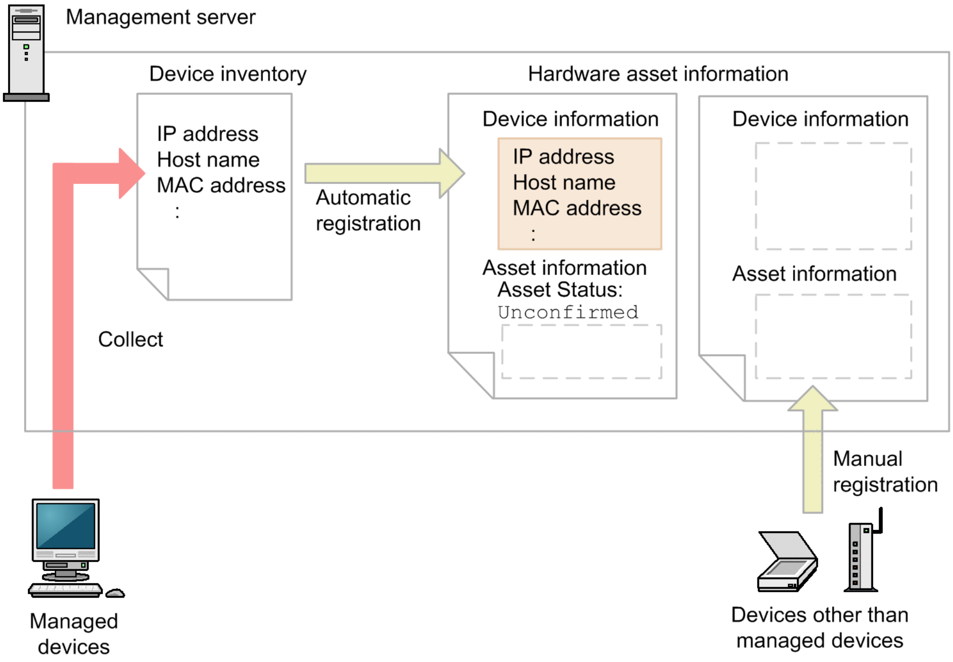
Related Topics:

- 2.11.1 List of the fields for asset information
- (1) Data types for asset fields
- (2) Data sources for asset fields

2.11.2 Managing hardware asset information

In the **Hardware Assets** view of the Assets module, you can register and manage hardware asset information.

When devices are set to be managed, information collected from those devices is displayed in the **Device Inventory** view of the Device module. Information about those devices is also registered automatically as new hardware asset information in the **Hardware Asset** view of the Assets module. The following figure shows the flow when hardware asset information is registered.



For hardware asset information that was automatically registered, **Asset Status** becomes `Unconfirmed`, and only the information items collected from devices are registered. Therefore, information items that are not automatically collected from devices, such as **Asset #**, **Asset Status** (for example, **In Use** or **In Stock**), and user information, must be registered in hardware asset information later.

Tip

When device inventory is updated, the information items (collected from devices) in hardware asset information is also updated.

If hardware assets have already been managed on a management ledger, you can import the information to JP1/IT Desktop Management 2. If no management ledger has been used, maintain the automatically registered hardware asset information.

If you want to manage hardware asset information about devices other than the managed devices, newly register hardware asset information for those devices.

Note that you need to maintain hardware asset information depending on the operation.

You can manage hardware asset information by associating it with other types of hardware information, or by setting the corresponding contract information.

Related Topics:

- (6) Managing hardware asset information associated with other information
- 2.11.1 List of the fields for asset information

(1) Associating devices and hardware assets

In hardware asset management, device information and hardware asset information are associated with each other. If a device is set to be managed, hardware asset information is automatically registered and associated with the device information. However, if a device is not set to be managed, or if hardware asset information only is registered, the device information and hardware asset information might not be associated.

The following table describes the details about association of devices and hardware assets corresponding to each trigger.

Trigger	Description
An agent-installed device connects to the management server.	Device information of the target device is registered, and hardware asset information is automatically registered at the same time. The hardware asset information is associated with the device information.
A device is discovered during device search (when the settings are configured so that a discovered computer is automatically set as a managed device).	Device information of the target device is registered, and hardware asset information is automatically registered at the same time. The hardware asset information is associated with the device information. Note that if **Device Type** is other than **PC**, device information and hardware asset information are not registered because the device is not automatically set as a managed device. Therefore, association of device information and hardware asset information is not performed.
A device is discovered during device search (when the settings are configured so that a discovered computer is not automatically set as a managed device).	Device information and hardware asset information are not registered.
Hardware assets are imported using a CSV file.	Hardware asset information is registered, but device information is not registered. Therefore, association of device information and hardware information is not performed. However, if device information and hardware asset information have already been associated, the imported hardware asset information remains associated with device information.
A USB device is registered.	Hardware asset information is registered for a device for which **Device Type** is **USB Device**, but device information is not registered. Therefore, association of device information and hardware information is not performed.
A hardware asset is manually added in the Assets module.	Hardware asset information is registered, but device information is not registered. Therefore, association of device information and hardware asset information is not performed. However, if device information and hardware asset information have already been associated, the imported hardware asset information remains associated with device information.

When a device and a hardware asset have been associated, the association might be released if the status of device information or hardware asset information is changed or information is deleted.

The following table describes how association changes for each trigger when a device and a hardware asset have been associated.

Trigger	Description
Asset Status of a hardware asset is changed to **Disposed**.	**Device Inventory** in hardware asset information is deleted, and association is released. Also, the target device is deleted from the device list in the Device module. Note that if an agent has been installed on the target device, the device will become a managed device again when the next device search is performed. In this case, if **Asset Status** is set to **Disposed** in hardware asset information, the same hardware asset information will be registered doubly. Therefore, when you set **Asset Status** to **Disposed**, we recommend that you disconnect the target device from the network or uninstall the agent. If **Asset Status** is set to other than **Disposed** in hardware asset information, the association will be registered again.
A target device is deleted in the **Managed Nodes** view of the Settings module.	**Device Inventory** in hardware asset information is deleted, and association is released. Also, the target device is deleted from the device list in the Device module. The behavior when an agent-installed device becomes a managed device again is the same as the behavior when **Asset Status** is set to **Disposed** in hardware asset information.
A target device is set to **Ignored** in the **Managed Nodes** view of the Settings module.	The target device is deleted from the device list in the Device module. **Device Inventory** in hardware asset information is not deleted. Note that when an agent has been installed on the target device, if you manually set the device to be managed again, the target device is registered again in the device list.

Trigger	Description
A hardware asset is deleted.	Hardware assets can be deleted only when **Asset Status** is **Unconfirmed** or **Disposed**. The following are behaviors of the device when a hardware asset is deleted: When **Asset Status** is **Unconfirmed**: The target device is deleted from the **Device Inventory** view of the Device module. When **Asset Status** is **Disposed**: The target device has already been deleted from the **Device Inventory** view of the Device module.

(2) Identifying related devices and hardware assets

When a device is set to be a managed device, hardware asset information is automatically registered and associated with device information. If hardware asset information corresponding to the managed device has already been registered, related registered device information is identified. If device information and hardware asset information that are related with each other are identified, they will be associated.

For identification of related device information and hardware asset information, one of the items in the following table is used.

Priority	Item compared during identification
1	IMEI#1
2	Serial ##2
3	Host Name
4	MAC Address
5	Contract phone number#1
6	IP Address

#1: Used when managing a smart device by linking with an MDM system.

#2: Serial number of BIOS information

During identification, the values of the higher priority items are compared first. If the values for an item with a higher priority have not been acquired or are invalid, the values for the item with the next higher priority are compared.

If the values for an item match, a relationship between device information and hardware asset information is identified, and device information related to the hardware asset information is added. If the values for the items do not match, new hardware asset information is registered.

Important note

When only device information has been registered, even if corresponding hardware asset information is registered later, the relationship between device information and hardware asset information is not identified. In that case, manually associate them.

(3) Collecting information entered by users

If agents have been installed on managed computers, you can display the **End User Form** view on users' computers, and have hardware asset information automatically updated by information entered by users.

By collecting information entered by users, the system administrator can reduce the time and effort for maintaining hardware asset information. For example, if users enter the latest information regularly, even after a large number of people move to different departments, the system administrator can understand user information without any need for special activities to gain the information.

The following fields can be entered by users:

- Department
- Location
- User Name
- Account
- E-mail
- Phone
- Custom fields that are optionally added

To collect user information, you need to set (in advance) asset fields to be entered by users in the **Asset Field Definitions** view (under **Assets**) of the Settings module. To display the **End User Form** view, the display of the user input window must be specified in the **User notification settings** view for the agent configuration.

In the **Asset Field Definitions** (under **Assets**) of the Settings module, the system administrator can also specify the time to allow users to start entering information. The **End User Form** view can be displayed after the settings of multiple fields have changed. So, this view is useful for updating information in accordance with personnel changes at the beginning of a fiscal year.

> **Important note**
>
> If the agent whose version is 10-01 or earlier is installed on users' computers, even if the entry start date and time is specified, the **End User Form** view appears each time a field setting changes. To specify the entry start date and time, install an agent whose version is 10-10 or later on the users' computers.

The **End User Form** view can be displayed on a regular basis on users' computers that are managed online. To do so, specify the display of the user input window in the **User notification settings** view for the agent configuration. At this time, do not specify the entry start date and time in the **Asset Field Definitions** view of the Settings module. If you specify the entry start date and time, the **End User Form** view will not be displayed on a regular basis. For offline-managed computers, the **End User Form** view can be displayed when the `getinv.vbs` command is executed to collect device information.

Before the specified entry start time is reached, selecting Windows **Start**, **All Programs**, **JP1_IT Desktop Management 2 - Agent**, and then **End User Form** on the user's computer only causes a message to appear. At this time, user information cannot be entered. The **End User Form** view is not displayed on offline-managed computers when the `getinv.vbs` command is executed.

(4) Managing the asset status

In hardware asset information, you can set the asset status, which indicates whether the asset is in use, in stock, or in other statuses. By setting the asset status, you will be able to check the usage status of assets, as well as check a list of owned assets. You can also check disposed assets, as well as owned assets.

There are following asset statuses:

Unconfirmed

Asset information has been registered, but it is not managed as an asset. This asset status is set for the hardware asset information automatically registered when a device is set to be managed. If there is an asset whose status is **Unconfirmed**, check the actual hardware and set the asset information including the asset status.

In Stock

The asset is not used.

In Use

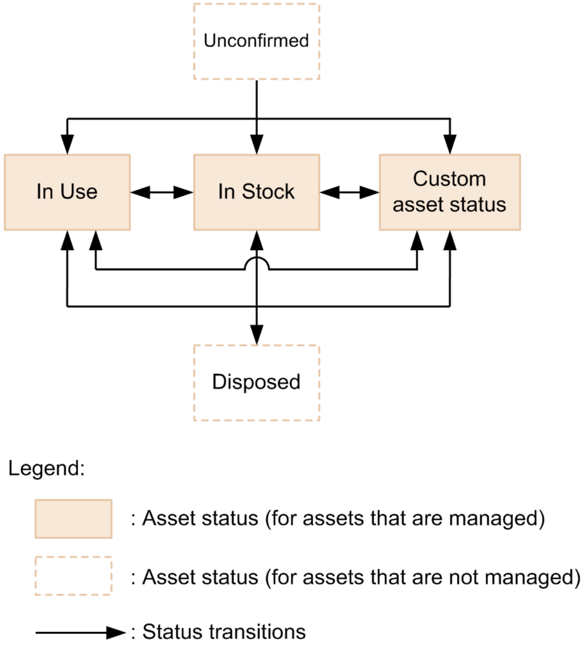
The asset is in use.

Disposed

The asset has been disposed of.

The administrator can add custom asset statuses other than above (no more than 100 items excluding the default asset statuses).

The following figure shows the transition of asset statuses.


Unconfirmed
In Use
In Stock
Custom asset status
Disposed
Legend:
: Asset status (for assets that are managed)
: Asset status (for assets that are not managed)
: Status transitions

To check the usage status, change the asset status according to actual operations. Change the status of assets for which management is no longer needed, to **Disposed**. Note that you can also change **Disposed** back to **In Use**, **In Stock**, or a custom asset status.

Managing the planned asset status

You can set asset statuses that are planned to change in the future. By setting planned asset statuses, you can check the planned tasks for asset management.

For example, for an asset with **In Stock** status, if you set the planned asset status to **Disposed** and set a date for that plan, you can check the date planned for disposal of the asset.

The specifiable types of the planned asset status are the same as for asset status.

Note that planned asset status is not automatically changed when the planned date expires. The administrator must manually change the asset status around the planned date after making sure that the status of the actual hardware asset has changed. If you change the asset status to the one set for the planned asset status, the values set for the planned asset status and the planned date are cleared.

Tip

If you register a planned asset status, the relevant asset can be checked on a summary report.

(5) Updating the tracked date

You can update **Tracked Date** for hardware asset information and software license information. By updating **Tracked Date**, you can check whether all assets have been tracked.

Updating the tracked date manually:

Select information about an asset for which **Tracked Date** is to be updated, and then update **Tracked Date**. We recommend that you use this method to individually track a small number of assets around you.

Updating the tracked dates in a batch based on a CSV file:

Use a CSV file containing **Asset #** or **License #** information to update **Tracked Date** in a batch. **Tracked Date** for the individual assets will become the same. We recommend that you use this method to track assets by using a bar code reader. Output a list of **Asset #** or **License #** read by a bar code reader to a CSV file.

Setting automatic update of the tracked date:

You can set the tracked date in hardware asset information to be automatically updated. JP1/IT Desktop Management 2 checks the existence of devices by monitoring network connection of devices, users' input on devices, and notification of device information acquired from computers managed offline. If the devices are confirmed to exist, the tracked date is automatically updated. We recommend that you use this method to reduce the time and effort of tracking assets.

Important note

Even if **Update Tracked Date (on receiving End User Form)** is selected in the **Update Tracked Date (Automatically)** dialog box, the tracked date in hardware asset information is updated automatically if **Update Device Details** is selected from the **Action** menu. This menu appears in the **Device List** view (under **Device Inventory**) of the Device module.

Tip

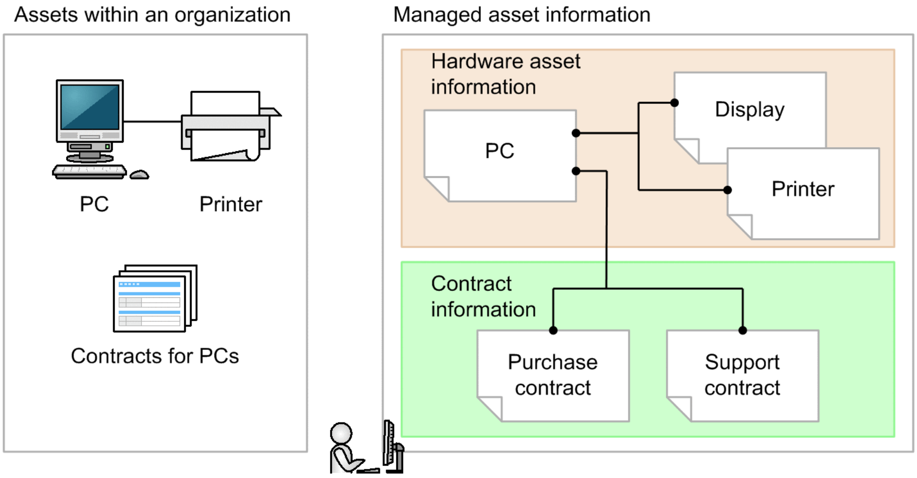
You can also import hardware asset information and software license information, and then update **Tracked Date** in a batch. In this case, you can set different dates for **Tracked Date** for individual assets.

(6) Managing hardware asset information associated with other information

You can manage information about a hardware asset by associating it with other hardware assets, or you can set the contract information corresponding to a hardware asset.

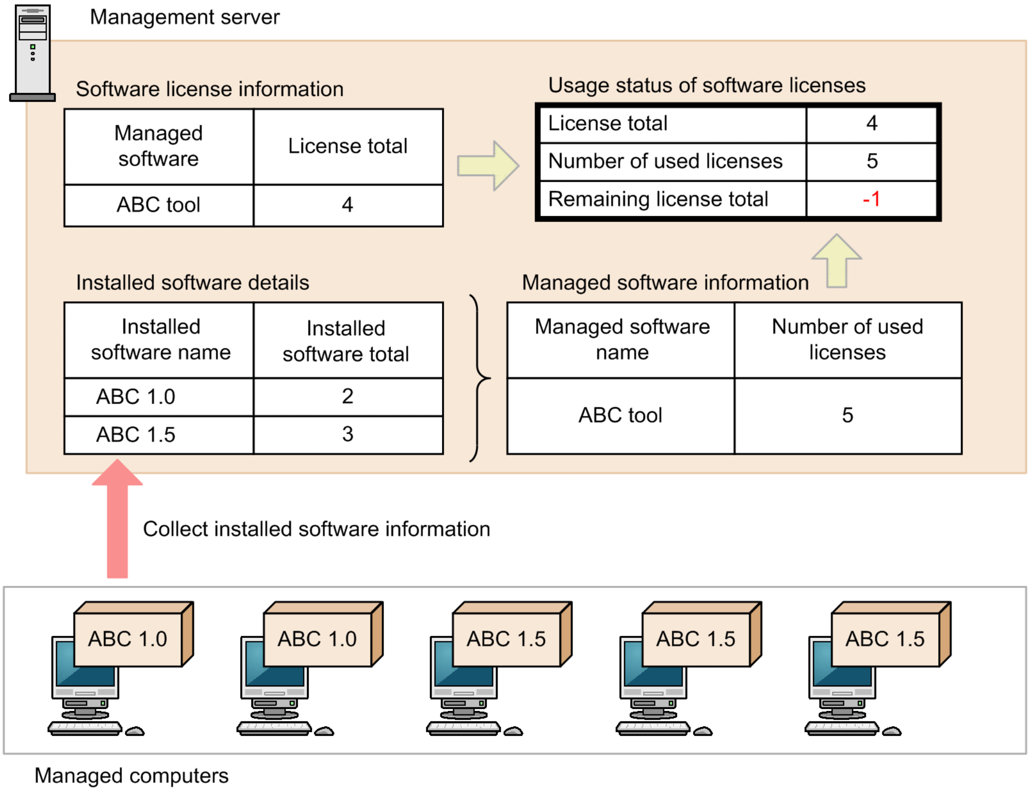
By associating information about a hardware asset with other hardware assets, you can manage a computer, display, and peripheral devices as a set.

By setting the contract corresponding to a hardware asset, you will be able to check the contract that was made for a computer. Also, you will be able to use a report to check the operational costs necessary for a hardware asset.



2.11.3 Checking the usage status of software licenses

Before starting software license management, you need to register managed software information and software license information in JP1/IT Desktop Management 2. Registering such information will enable you to check the usage status of software licenses. The following figure shows an overview of viewing the number of software licenses to check whether there is an excess or shortage of software licenses.


Management server
Software license information
Usage status of software licenses
Installed software details
Managed software information
Collect installed software information
ABC 1.0
ABC 1.0
ABC 1.5
ABC 1.5
ABC 1.5
Managed computers

Managed software	License total
ABC tool	4

License total	4
Number of used licenses	5
Remaining license total	-1

Installed software name	Installed software total
ABC 1.0	2
ABC 1.5	3

Managed software name	Number of used licenses
ABC tool	5

For software license information, set information about the owned software licenses and the corresponding software names (managed software names). For software license information, you can also register the computers to which the software licenses are assigned (that is, use of the software is allowed). Use the **Software Licenses** view of the Asset module to set software license information.

For managed software information, specify information about the software programs for which the number of used licenses is to be counted. You can also specify information about multiple software programs as one type of software programs. This will count the number of installed software programs for each managed software program. Use the **Managed Software** view of the Asset module to specify the managed software information.

When software license information and managed software information are registered, you can collectively check the usage status of software licenses for each managed software program in the **Software License Status** view of the Asset module. For example, checking the number of computers with software licenses assigned (number of assigned licenses) allows you to find the computers on which software has been installed without permission. You can also find the computers for which the use of software is allowed but no software is installed. In addition, the total number of owned licenses and the number of remaining licenses are counted for each managed software program. So, you can check whether there is an excess or shortage of software licenses. The usage status of software licenses can be output to a CSV file by exporting the software license status list in the **Software License Status** view.

The **Software License Status** view allows you to check the usage status of software licenses by department. The following provides examples of managed software names, values specified in software license information, and usage status of software licenses, and shows the values displayed in the **Software License Status** view as an example of specifications.

Specification examples of managed software names and software license information, and usage status of software licenses

Managed software name	Software license information			Usage of software licenses	
	Department	Total number of owned licenses	Number of assigned licenses	Number of installed programs	Department to which the computer with programs installed belongs
ABC software	General affairs department	10	10	12	General affairs department
	Sales department	10	10	10	Sales department
	Development department	5	10	5	Development department
	Development department/Division A	5	10	3	Development department/Division A
	Development department/Division B	5	3	3	Development department/Division B
	--	--	--	3	Development department/Division C
	--	--	--	1	Personnel department
XYZ software	--	20	2	1	Development department/Division A

Managed software name	Software license information			Usage of software licenses	
	Department	Total number of owned licenses	Number of assigned licenses	Number of installed programs	Department to which the computer with programs installed belongs
XYZ software	--	20	2	1	Development department/Division B

Legend: --: Not specified

Information displayed in the Software License Status view

Managed Software Name	Department	License Total	Number of Used Licenses	Remaining License Total	Assigned License Total	Description
ABC software	(Total of All Departments)[#1]	35	37	-2	43	The total values of all departments (General affairs, Sales, Development, and Personnel departments) are displayed.
	General affairs department	10	12	-2	10	The values only for the General affairs department are displayed.
	Sales department	10	10	0	10	The values only for the Sales department are displayed.
	Development department[#2]	15	14	1	23	The values only for the Development department (total values of Development department, Development department/Division A, Development department/Division B, and Development department/Division C) are displayed.
	Development department/Division A[#2]	5	3	2	10	The values only for Development department/Division A are displayed.
	Development department/Division B[#2]	5	3	2	3	The values only for Development department/Division B are displayed.
	Development department/Division C[#2]	--	3	--	0	The values only for Development department/Division C are displayed. If an upper-level department (Development department) is set for department information in software license information but a local department (Development department/Division C) is not set, a hyphen (-) appears for **License Total** and **Remaining License Total**.
	Personnel department	0	1	-1	0	The values only for the Personnel department are displayed.

Managed Software Name	Department	License Total	Number of Used Licenses	Remaining License Total	Assigned License Total	Description
ABC software	Personnel department	0	1	-1	0	If neither a local department (Personnel department) nor an upper-level department is set for department information in software license information, `0` appears for **License Total** and **Assigned License Total**. A negative value appears for **Remaining License Total**.
XYZ software	(Total of All Departments)[#1]	20	2	18	2	The total values of all departments (General affairs, Sales, Development, and Personnel departments) are displayed. The values of **License Total** and **Assigned License Total** for the software programs for which a department is not specified in software license information are also added.
	Development department[#2]	--	2	--	2	The values only for the Development department (total values of Development department, Development department/Division A, and Development department/ Division B) are displayed. If a department is not set for software license information, a hyphen (-) appears for **License Total** and **Remaining License Total**.
	Development department/ Division A[#2]	--	1	--	1	The values only for Development department/Division A are displayed. If a department is not set for software license information, a hyphen (-) appears for **License Total** and **Remaining License Total**.
	Development department/ Division B[#2]	--	1	--	1	The values only for Development department/Division B are displayed. If a department is not set for software license information, a hyphen (-) appears for **License Total** and **Remaining License Total**.

Legend: --: Not applicable

Note: Clicking **Software License Status List** in the menu area displays all fields in the table.

#1: This field is displayed if **(Total of All Departments)** is clicked in the menu area.

#2: This field is displayed if **Development Department** is clicked in the menu area.

Important note

From JP1/IT Desktop Management 10-01, the way of counting the number of used licenses has changed. Therefore, if you upgrade JP1/IT Desktop Management from version 09-50, the number of used licenses might be different.

For the number of used licenses, the number of installed software programs corresponding to the managed software programs is displayed. In version 09-50, if multiple software programs corresponding to a managed software program have been installed on a computer, all of those software programs are counted for licenses. In version 10-01 or later, if multiple software programs corresponding to a managed software product have been installed on a computer, they are counted so that only one license is consumed.

(1) Managing managed software information

In the **Managed Software** view of the Assets module, you can register and manage managed software information.

You can register managed software information manually or by importing a CSV file created for managed software information.

If the corresponding software programs are added or changed, maintain managed software information to keep the latest status.

Note that you can update managed software information in a batch by exporting it and then importing an edited CSV file. You can also delete managed software information for which management is no longer needed.

When managed software information is registered, you can check the usage status of software licenses for each managed software in the **Software License Status** view of the Asset module.

(2) Managing license status

In software license information, you can set **License Status**, which indicates whether the license is in use, expired, or in other statuses. By setting **License Status**, you will be able to check the expired software licenses, as well as a list of owned licenses.

There are following types of license statuses:

In Use

The software license is in use.

Expired

The software license has expired.

The administrator can add other custom license statuses (no more than 100 license statuses excluding the default license statuses).

Managing planned license statuses

You can set license statuses that are planned to change in the future. Setting planned license statuses will enable you to check planned license management tasks. The specifiable fields for planned license status are the same as for license status.

For example, for a software license with **In Use** status, if you set the planned license status to **Expired** and set the planned date, you will be able to check the date the software license will expire.

The planned license status types are the same as those of license status.

Note that the planned license status is not automatically changed when the planned date expires. The administrator must manually change the license status around the planned date. If you change the license status to the one set for the planned license status, the values set for the planned license status and the planned date are cleared.

(3) Managing software license information

In the **Software License** view of the Assets module, you can register and manage information about the total number of owned licenses, corresponding contract information, departments, and other information.

For software licenses that are determined to be managed, maintain software license information to keep the status current. For example, you should maintain information about changes to the software to which the licenses are assigned, disposal of software, and addition or deletion of relevant contracts.

You can register software license information manually or by importing a CSV file that was created by editing exported software license information.

You can also delete software license information for which management is no longer needed.

Related Topics:

- (5) Managing assignment of software licenses

(4) Updating the tracked date

You can update **Tracked Date** for hardware asset information and software license information. By updating **Tracked Date**, you can check whether all assets have been tracked.

Updating the tracked date manually:

Select information about an asset for which **Tracked Date** is to be updated, and then update **Tracked Date**. We recommend that you use this method to individually track a small number of assets around you.

Updating the tracked dates in a batch based on a CSV file:

Use a CSV file containing **Asset #** or **License #** information to update **Tracked Date** in a batch. **Tracked Date** for the individual assets will become the same. We recommend that you use this method to track assets by using a bar code reader. Output a list of **Asset #** or **License #** read by a bar code reader to a CSV file.

Setting automatic update of the tracked date:

You can set the tracked date in hardware asset information to be automatically updated. JP1/IT Desktop Management 2 checks the existence of devices by monitoring network connection of devices, users' input on devices, and notification of device information acquired from computers managed offline. If the devices are confirmed to exist, the tracked date is automatically updated. We recommend that you use this method to reduce the time and effort of tracking assets.

Important note

Even if **Update Tracked Date (on receiving End User Form)** is selected in the **Update Tracked Date (Automatically)** dialog box, the tracked date in hardware asset information is updated automatically if **Update Device Details** is selected from the **Action** menu. This menu appears in the **Device List** view (under **Device Inventory**) of the Device module.

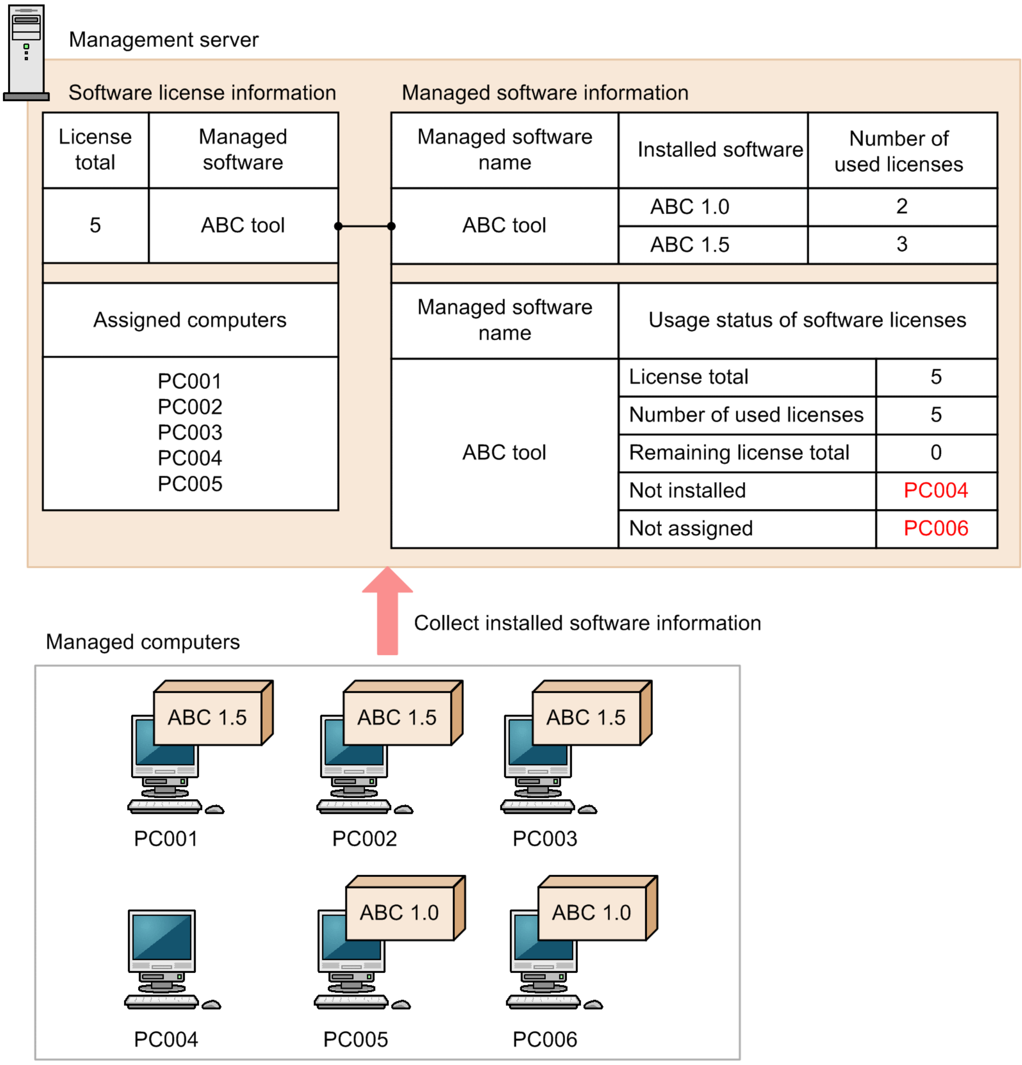
Tip

You can also import hardware asset information and software license information, and then update **Tracked Date** in a batch. In this case, you can set different dates for **Tracked Date** for individual assets.

(5) Managing assignment of software licenses

If you manage computers by assigning software licenses to them, you will be able to check for computers on which software has been installed without permission. You will also be able to check for software licenses that are not used even though their use is permitted.

To realize this, in software license information, specify the computers to which software licenses are to be assigned. Then, when you register managed software information, associate the software license information with it. As a result, information about computers on which software programs have been installed and information about computers to which software licenses are assigned can be compared. This will enable you to confirm whether software licenses are being used as assigned. The following figure shows how software licenses are assigned and managed.



Software license information

License total	Managed software
5	ABC tool

Assigned computers
PC001 PC002 PC003 PC004 PC005

Managed software information

Managed software name	Installed software	Number of used licenses
ABC tool	ABC 1.0	2
	ABC 1.5	3

Managed software name	Usage status of software licenses	
ABC tool	License total	5
	Number of used licenses	5
	Remaining license total	0
	Not installed	PC004
	Not assigned	PC006

You can check whether software is used as assigned on the **Installed Computers** and **Licensed Computers** tabs in the **Managed Software** view of the Assets module.

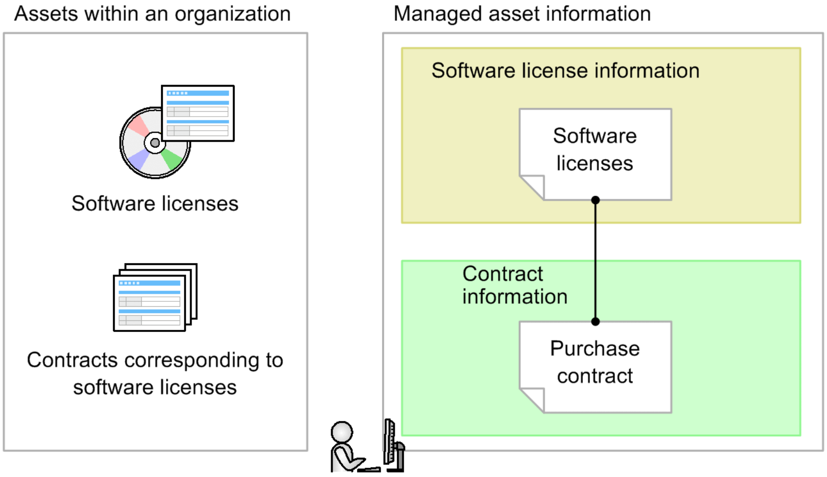
The **Installed Computers** tab displays the computers on which software programs specified in managed software information have been installed. If you select the **Show Only Computers Not Licensed** check box on this page to display the computers to which software licenses have not been assigned, you can check for computers on which software programs have been installed without permission.

The **Licensed Computers** tab displays the computers to which software licenses have been assigned. To check for unused software licenses, select the **Show Only Computers Not Installed** check box. This will display the computers that software licenses have been assigned to but the software has not been installed on.

(6) Managing software license information and the associated contract information

For software license information, you can set the corresponding contract information.

Setting contracts corresponding to the software licenses will enable you to check which contract was made for a software license. Also, you will be able to check the operational costs for software licenses using reports.


Assets within an organization
Software licenses
Contracts corresponding to software licenses
Managed asset information
Software license information
Software licenses
Contract information
Purchase contract

Multiple software licenses can be associated with one contract.

(7) Managing upgrade and downgrade licenses

You can register and manage license information about software upgrades and downgrades.

When you manage upgrade and downgrade licenses, the way of registering the software license information differs from the usual way.

When registering upgrade licenses:

When you upgrade software, in **Upgrade Source Name**, register information about the upgrade-source software licenses.

For example, if you own 10 licenses for `Software A version 2` and purchased 7 upgrade licenses for `Software A version 3`, when registering software license information about `Software A version 3`, specify the software license information about `Software A version 2` in **Upgrade Source Name**. As the result, the number of licenses for `Software A version 2` is automatically changed from 10 to 3 (so that the number of licenses is not counted redundantly), and you will be able to manage the correct number of licenses after the upgrade.

When registering downgrade licenses:

When you downgrade software, register the downgrade-destination managed software information as information about software licenses that can be downgraded.

For example, when you own 5 licenses for `Software A version 2` and 10 licenses for `Software A version 3`, if you downgrade 6 licenses from `Software A version 3` to `Software A version 2`, as the software license information about `Software A version 3`, register 4 usual software licenses and 6 downgrade licenses separately. As information about downgrade software licenses, specify the managed software information about `Software A version 2`. As the result, the number of owned `Software A version 3` licenses becomes 4, and the number of owned `Software A version 2` licenses becomes 11 (including the downgrade licenses). Then, you will be able to manage the correct number of licenses after downgrade.

2.11.4 Managing contract information

In the **Contracts** view of the Assets module, you can register and manage contract information.

You can register contract information by manually adding information about individual contracts or by importing a CSV file containing the contract information.

Maintain contract information to keep the status up to date. This is especially important when a contract is expired or cancelled, when a related asset is changed, or when a contract term is extended.

Note that you can also update information about contracts in a batch by exporting information about contracts and importing an edited CSV file.

You can also delete contract information for which management is no longer needed.

(1) Managing contract status

For contract information, you can set **Contract Status**, which indicates whether a contract is valid (within the contract term) or invalid (contract term has ended). Setting **Contract Status** will let you display a list showing the statuses of the contracts that are entered into. You can also display contracts that have ended, as well as the contracts that are within the contract term.

There are following types of contract statuses:

Active

Indicates that the contract is within the contract term. If a contract for which the contract term has expired has this status, the contract is treated as an expired contract.

Canceled

Indicates that the contract was terminated. Set this status if a contract is cancelled during the contract term.

Expired

Indicates that the contract period has ended.

The administrator can add custom contract statuses (no more than 100 statuses excluding the default contract statuses).

Tip

If you register the contract statuses and contract terms, you can check the contracts for which the expiration date is approaching on a summary report.

(2) Checking the costs for hardware assets and software licenses

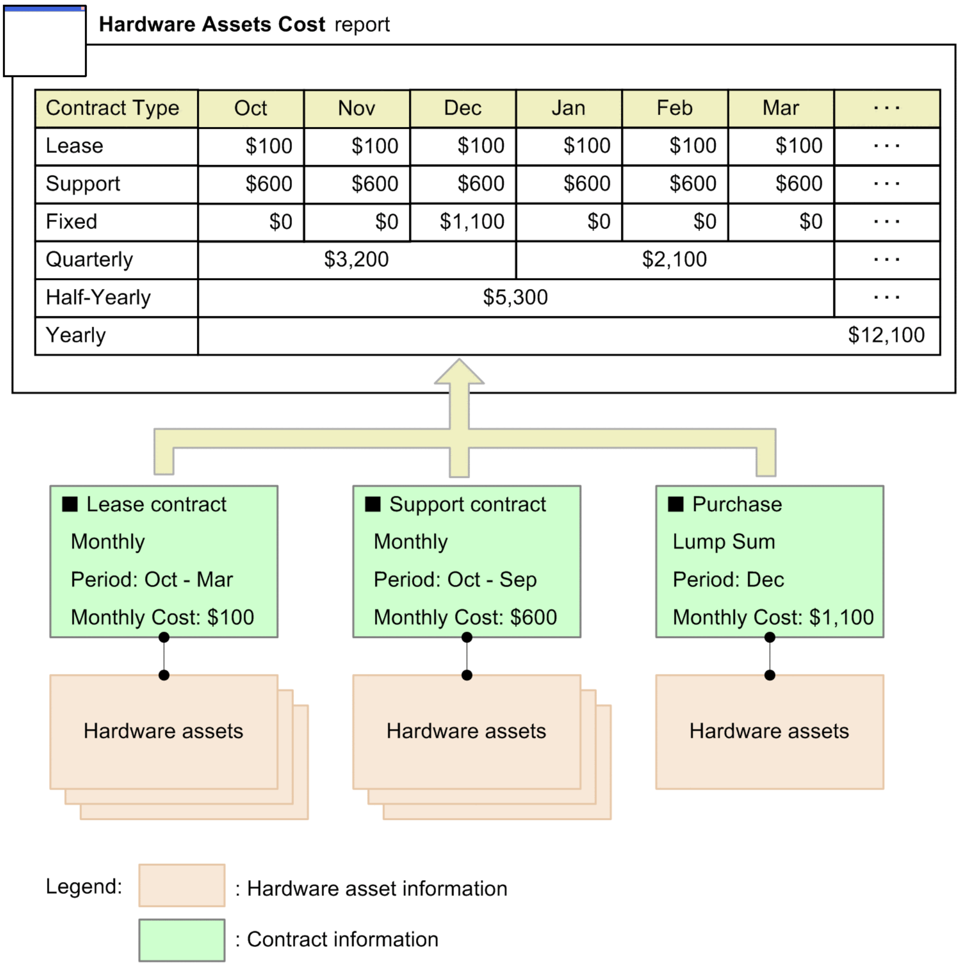
You can check the operational costs for hardware assets or software licenses in reports. You can check the costs for assets, using the following reports under **Asset Detail Reports**:

- **Hardware Assets Cost** report
- **Software License Cost** report

With these reports, you can check the monthly, quarterly, half-yearly, and yearly contract costs for each contract type.

Note that, to check the costs, you must set the costs in contract information and associate it with hardware asset information or software license information.

The following shows the concept of checking the costs for which contract information is associated.



Hardware Assets Cost report

Contract Type	Oct	Nov	Dec	Jan	Feb	Mar	...
Lease	$100	$100	$100	$100	$100	$100	...
Support	$600	$600	$600	$600	$600	$600	...
Fixed	$0	$0	$1,100	$0	$0	$0	...
Quarterly	$3,200			$2,100			...
Half-Yearly	$5,300						...
Yearly	$12,100						

■ Lease contract
Monthly
Period: Oct - Mar
Monthly Cost: $100

■ Support contract
Monthly
Period: Oct - Sep
Monthly Cost: $600

■ Purchase
Lump Sum
Period: Dec
Monthly Cost: $1,100

Legend: ▭ : Hardware asset information
🟩 : Contract information

In the above figure, for the lease contract associated with hardware assets, monthly payment is set for the contract term from October to March. Therefore, for the six months of the contract period, $100 is booked monthly. In the same way, for the support contract, $600 is booked monthly for the twelve months of the contract period. For purchase, the lump sum is set, so $1,100 is booked in December.

The monthly amount is summed up based on these calculated amounts, and the amount is booked quarterly, half-yearly, and yearly.

> **Tip**
>
> The amount is summed up for each contract, and does not depend on the number of hardware assets associated with contract information.

(3) Calculating the costs for hardware assets

If you associate contract information and hardware asset information, the contract costs are calculated. The costs for hardware assets are displayed on the **Hardware Assets Cost** report (under **Asset Detail Reports**) of the Reports module.

The following describes how to calculate the contract costs.

Costs for each contract type

The total costs for individual months are calculated for each contract type. Based on those costs, quarterly, half-yearly, and yearly costs are calculated. The costs for each month is calculated based on the value in **Monthly Cost** for monthly payment, or on the value in **Total Cost** for lump sum. A year starts with the month set in the **Duration and Start Date** view (under **Reports**) of the Settings module. The costs for twelve months are displayed on the **Hardware Assets Cost** report (including the date the report is displayed).

The costs are calculated for each contract type based on the conditions below.

The costs for a contract with contract type *XXX* are calculated below. *XXX* is one of the following:

- Lease
- Rent
- Maintenance
- Support
- Fixed
- Custom contract types added by the administrator

Method of payment	Calculation
Monthly	Sums up **Monthly Cost** for the contracts that satisfy all of the following conditions: • **Contract Type** is *XXX*. • **Payment Mode** is **Monthly**. • Hardware asset information is associated with **Hardware Assets (Contract)**. • The specified month includes the date the costs occurred. Note that the costs for the **Monthly** payment occur every month for the period from the start date to the end date of the contract specified in **Contract Term**. For example, if **Contract Term** is 2011/4/10 to 2011/6/10, the costs occur on 2011/4/10, 2011/5/10, and 2011/6/10. Therefore, if the specified month is April in 2011, May in 2011, or June in 2011, the costs are displayed.
Lump Sum	Sums up **Total Cost** for the contracts that satisfy all of the following conditions: • **Contract Type** is *XXX*. • **Payment Mode** is **Lump Sum**.

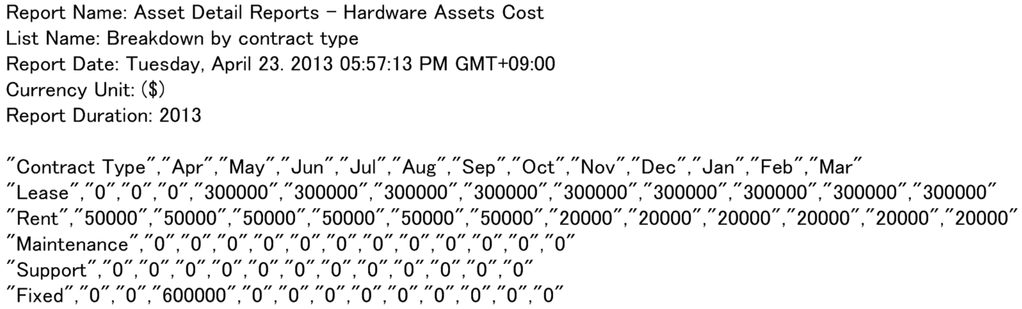
Method of payment	Calculation
Lump Sum	• Hardware asset information is associated with **Hardware Assets (Contract)**. • The specified month includes the date the costs occurred. Note that the costs for a **Lump Sum** payment occur on the **Contract Date**.

Export

You can output the costs summed up for hardware assets to a CSV file. The format of an output CSV file is as follows:

- For **Report Name**, **List Name**, **Report Date**, **Currency Unit**, and **Report Duration**, text strings are output without double quotation marks (`"`).
- For the fields other than above, data is output with double quotation marks (`"`).
- For a blank column, only a comma (`,`) is output as a delimiter.

The following is an example of a CSV file.



```
Report Name: Asset Detail Reports - Hardware Assets Cost
List Name: Breakdown by contract type
Report Date: Tuesday, April 23. 2013 05:57:13 PM GMT+09:00
Currency Unit: ($)
Report Duration: 2013

"Contract Type","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec","Jan","Feb","Mar"
"Lease","0","0","0","300000","300000","300000","300000","300000","300000","300000","300000","300000"
"Rent","50000","50000","50000","50000","50000","50000","20000","20000","20000","20000","20000","20000"
"Maintenance","0","0","0","0","0","0","0","0","0","0","0","0"
"Support","0","0","0","0","0","0","0","0","0","0","0","0"
"Fixed","0","0","600000","0","0","0","0","0","0","0","0","0"
```

Note that data is output for customized contract types, in addition to the default contract types.

(4) Calculating the costs for software licenses

If you associate contract information and software license information, the contract costs are calculated. The costs for software licenses are displayed on the **Software License Cost** report (under **Asset Detail Reports**) of the Reports module.

The following describes how the contract costs are calculated.

Costs for each contract type

The total costs for individual months are calculated for each contract type. Based on **Monthly Cost** or **Total Cost** for individual months, quarterly, half-yearly, and yearly costs are calculated. A year starts with the month set in the **Duration and Start Date** view (under **Reports**) of the Settings module. The costs for twelve months are displayed on the **Software License Cost** report (including the date the report is displayed).

The costs are calculated for each contract type based on the conditions below.

The costs for a contract with contract type *XXX* are calculated below. *XXX* is one of the following:

- Lease
- Rent
- Maintenance
- Support
- Fixed

- Custom contract types added by the administrator

Method of payment	Calculation
Monthly	Sums up **Monthly Cost** for the contracts that satisfy all of the following conditions: • **Contract Type** is *XXX*. • **Payment Mode** is **Monthly**. • Software license information is associated with **Software Licenses (Contract)**. • The specified month includes the date the costs occurred. Note that the costs for the **Monthly** payment occur at every month for the period from the start date to the end date of the contract specified in **Contract Term**. For example, if **Contract Term** is 2011/4/10 to 2011/6/10, the costs occur on 2011/4/10, 2011/5/10, and 2011/6/10. Therefore, if the specified month is April in 2011, May in 2011, or June in 2011, the costs are displayed.
Lump Sum	Sums up **Total Cost** for the contracts that satisfy all of the following conditions: • **Contract Type** is *XXX*. • **Payment Mode** is **Lump Sum**. • Software license information is associated with **Software Licenses (Contract)**. • The specified month includes the date the costs occurred. Note that the costs for the **Lump Sum** payment occur on the **Contract Date**.

Export

You can output the costs summed up for software licenses to a CSV file. The format of an output CSV file is as follows:

- For **Report Name**, **List Name**, **Report Date**, **Currency Unit**, and **Report Duration**, text strings are output without double quotation marks (`"`).
- For the fields other than above, data is output with double quotation marks (`"`).
- For a blank column, only a comma (`,`) is output as a delimiter.

The following is an example of a CSV file.

```
Report Name: Asset Detail Reports - Software License Cost
List Name: Breakdown by contract type
Report Date: Tuesday, April 23. 2013 06:01:59 PM GMT+09:00
Currency Unit: ($)
Report Duration: 2013

″Contract Type″,″Apr″,″May″,″Jun″,″Jul″,″Aug″,″Sep″,″Oct″,″Nov″,″Dec″,″Jan″,″Feb″,″Mar″
″Lease″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″
″Rent″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″
″Maintenance″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″
″Support″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″,″0″
″Fixed″,″50000″,″50000″,″50000″,″50000″,″50000″,″50000″,″50000″,″50000″,″50000″,″50000″,″0″,″0″
```

Note that data is output for customized contract types, in addition to the default contract types.

(5) Notification of expired contracts

Based on the contract end dates set in **Contract Term** in contract information, you can send email notifications of expired contracts.

The function of sending summary reports is used for notification of expired contracts. You can set the summary report notification destinations in the **Summary Report Notifications** view (under **Reports**) of the Settings module.

The number of expired contracts is reported by email. A contract is determined to be expired based on the following conditions:

- **Contract Status** is other than **Expired** or **Canceled**.
- The date of notification is later than the contract end date.

If you want to know the details about expired contracts, click the link in the email body. Clicking the link displays the Reports module. In the **Summary Reports** view of the Reports module, click the link for an expired contract. You are moved to the Assets module, and here you can check the details about the relevant contract.

> **Tip**
>
> You can also check contract terms on the **Expired Contracts (next 3 months)** panel.

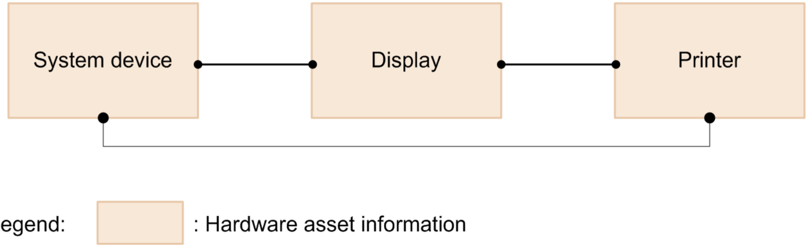
2.11.5 Associating asset information

You can associate and manage multiple assets. By associating assets with one another, for example, you can check the peripheral devices connected with each computer, or check the costs for the support contracts for software licenses.

Associating information about hardware assets

You can associate and manage multiple hardware assets. By doing so, you can manage multiple assets as a set.

The following is an example when multiple hardware assets are associated.



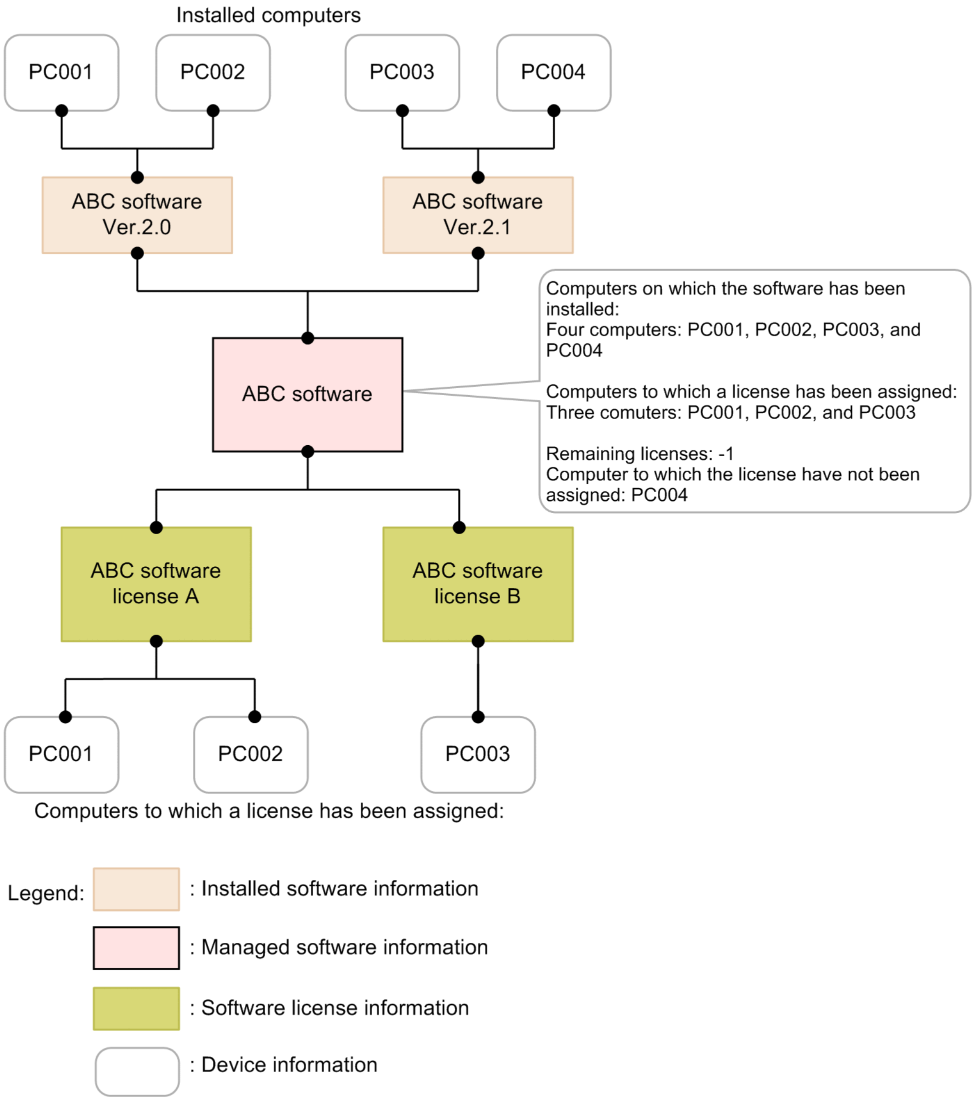
Associating information about software licenses and information about managed software programs

When you manage the usage status of software licenses, you can associate and manage software licenses and managed software programs.

By associating managed software information with the installed software information collected from devices, you can check the number of used licenses for the managed software programs. You can also associate a managed software program with multiple installed software programs. By doing so, you can manage the software licenses whose volume licenses and versions are different for each managed software program.

For software license information, you can associate the device to which the software license is assigned. By doing so, you will be able to check whether software licenses are being used as assigned, based on the information about the installed software summed up as managed software information.

The following is an example when software licenses are assigned to devices to manage the usage status.



Computers on which the software has been installed:
Four computers: PC001, PC002, PC003, and PC004

Computers to which a license has been assigned:
Three comuters: PC001, PC002, and PC003

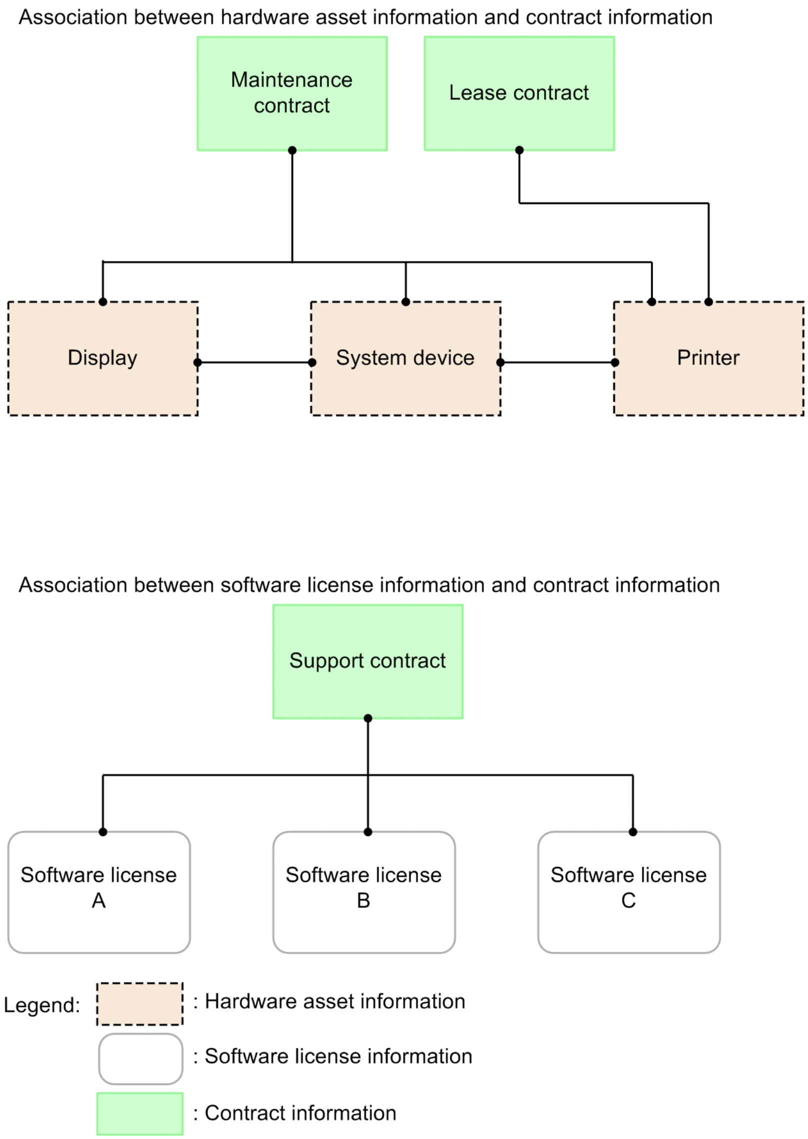
Remaining licenses: -1
Computer to which the license have not been assigned: PC004

Associating contract information

You can associate contract information with hardware asset information or software license information for management. For example, if you associate maintenance contract information with hardware asset information about computers, you can quickly check the maintenance contract information required when a computer fails, and take countermeasures.

If you set the costs for contract information, you can check the costs for hardware assets or software licenses.

The following is an example when contract information is associated with hardware asset information and software license information.


Association between hardware asset information and contract information
Maintenance contract
Lease contract
Display
System device
Printer
Association between software license information and contract information
Support contract
Software license A
Software license B
Software license C
Legend:
: Hardware asset information
: Software license information
: Contract information

As for hardware asset information, multiple contracts can be associated with multiple hardware assets according to the contract type.

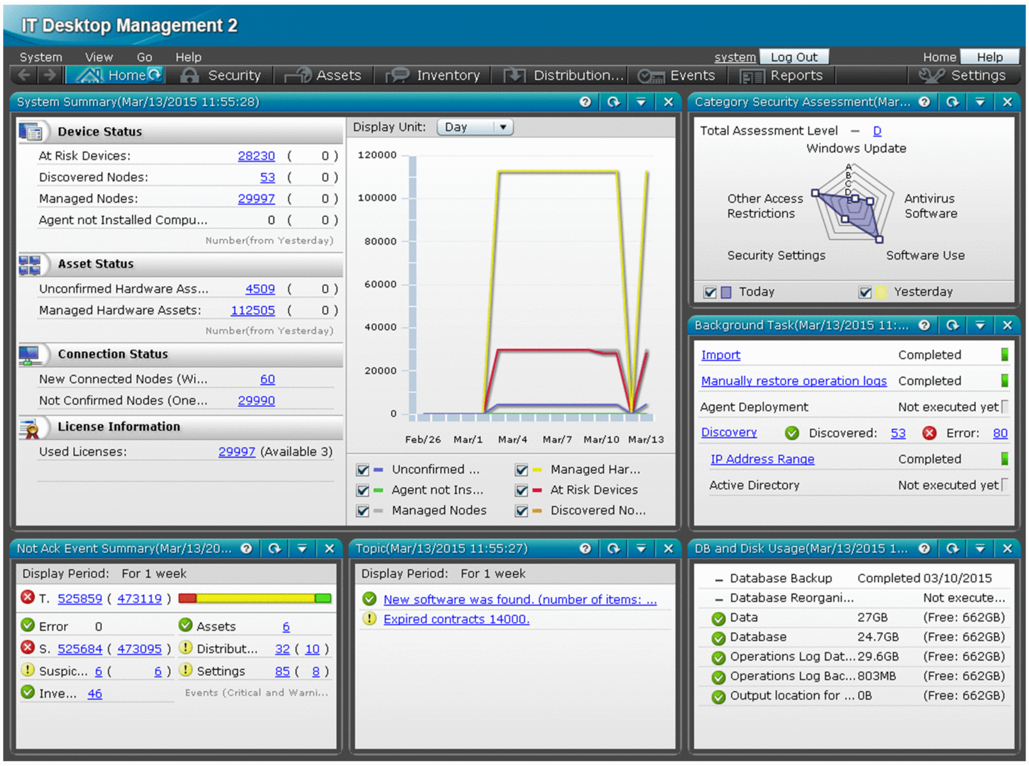
As for software license information, one contract can be associated with multiple software licenses because contracts are managed for each software license.

2.11.6 Checking asset information

Checking on the panels in the Home module

In **Unconfirmed Hardware Assets** on the **System Summary** panel of the Home module, you can check the number of hardware assets with the **Unconfirmed** asset status (the number of hardware assets that are newly registered and for which information has not been input). Clicking the link on the number displays the **Hardware Assets** view of the Assets module, where you can check hardware asset information.

Note that, in **Managed Hardware Assets**, you can check the total number of hardware assets whose asset status is other than **Unconfirmed**.


IT Desktop Management 2
System View Go Help
system Log Out Home Help
Home Security Assets Inventory Distribution... Events Reports Settings

System Summary(Mar/13/2015 11:55:28)

Device Status

At Risk Devices:	28230	(0)
Discovered Nodes:	53	(0)
Managed Nodes:	29997	(0)
Agent not Installed Compu...	0	(0)

Number(from Yesterday)

Asset Status

Unconfirmed Hardware Ass...	4509	(0)
Managed Hardware Assets:	112505	(0)

Number(from Yesterday)

Connection Status

New Connected Nodes (Wi...	60
Not Confirmed Nodes (One...	29990

License Information

Used Licenses: 29997 (Available 3)

Display Unit: Day

Category Security Assessment(Mar...

Total Assessment Level — D

Background Task(Mar/13/2015 11:...

Import	Completed
Manually restore operation logs	Completed
Agent Deployment	Not executed yet
Discovery	✓ Discovered: 53 ☒ Error: 80
IP Address Range	Completed
Active Directory	Not executed yet

Not Ack Event Summary(Mar/13/20...

Display Period: For 1 week

☒ T. 525859 (473119)			
✓ Error 0	✓ Assets 6		
☒ S. 525684 (473095)	! Distribut... 32 (10)		
! Suspic... 6 (6)	! Settings 85 (8)		
✓ Inve... 46	Events (Critical and Warni...		

Topic(Mar/13/2015 11:55:27)

Display Period: For 1 week

✓ New software was found. (number of items: ...

! Expired contracts 14000.

DB and Disk Usage(Mar/13/2015 1...

– Database Backup	Completed 03/10/2015	
– Database Reorgani...	Not execute...	
✓ Data	27GB	(Free: 662GB)
✓ Database	24.7GB	(Free: 662GB)
✓ Operations Log Dat...	29.6GB	(Free: 662GB)
✓ Operations Log Bac...	803MB	(Free: 662GB)
✓ Output location for ...	0B	(Free: 662GB)

Checking in the Assets module

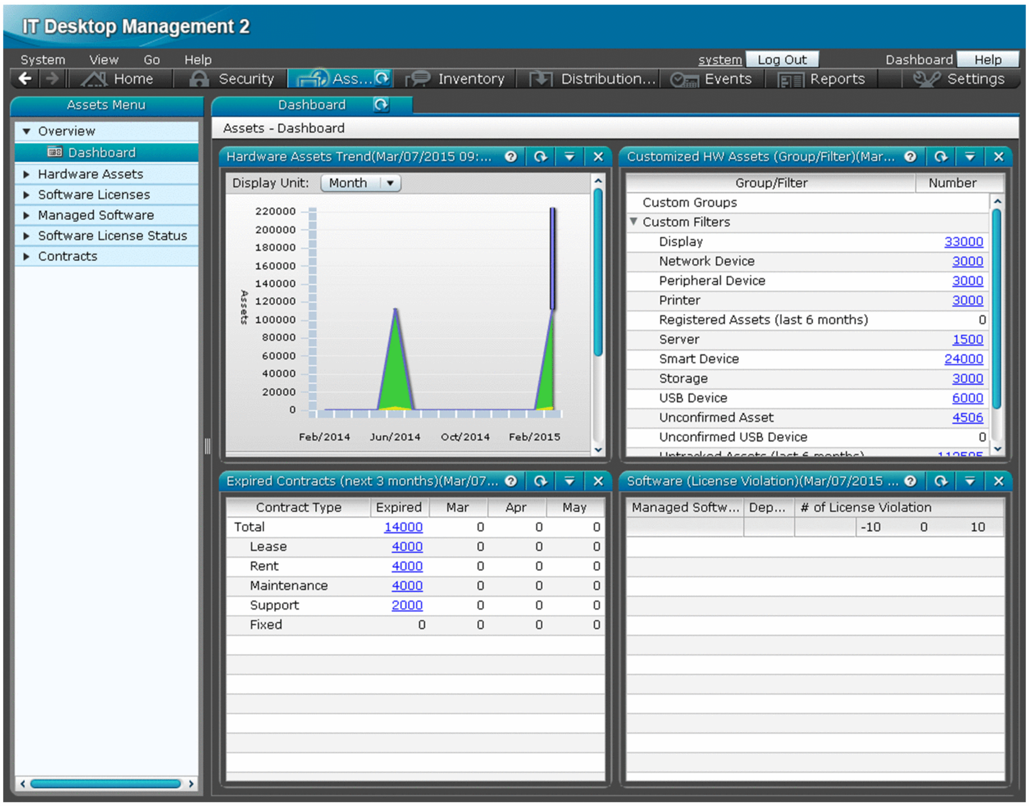
You can check the asset statuses in the **Overview** view, **Hardware Asset** view, **Software Licenses** view, **Managed Software** view, **Software License Status** view, and **Contracts** view of the Assets module. You can use the Assets module as an asset ledger by registering asset information within an organization.

Tip

In the views other than the **Overview** view, you can use filters to extract and view the items that satisfy the filter conditions. You can also use the filters provided by this product in the menu area. For details about how to use filters, see 2.17 Using filters.

Checking in the **Overview** view

You can check an overview of the assets. Clicking a link on a panel displays the view for details, so you can use the **Overview** view as a portal for asset management.



Group/Filter	Number
Custom Groups	
Custom Filters	
Display	33000
Network Device	3000
Peripheral Device	3000
Printer	3000
Registered Assets (last 6 months)	0
Server	1500
Smart Device	24000
Storage	3000
USB Device	6000
Unconfirmed Asset	4506
Unconfirmed USB Device	0

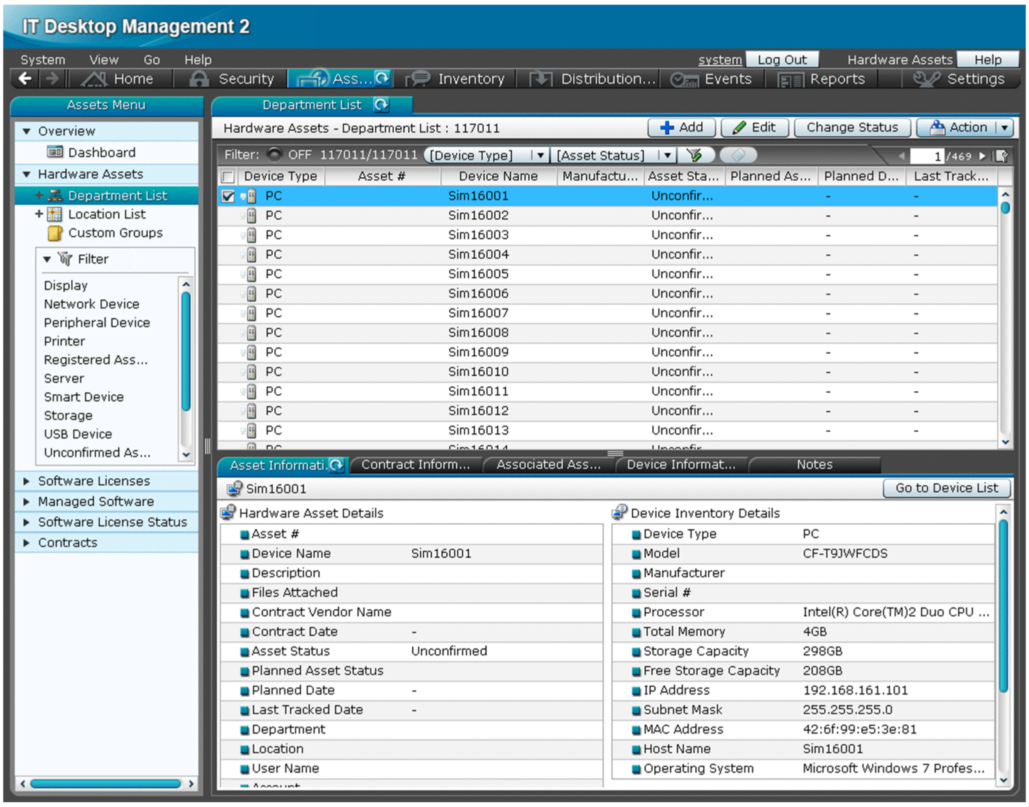
Contract Type	Expired	Mar	Apr	May
Total	14000	0	0	0
Lease	4000	0	0	0
Rent	4000	0	0	0
Maintenance	4000	0	0	0
Support	2000	0	0	0
Fixed	0	0	0	0

Managed Softw...	Dep...	# of License Violation		
		-10	0	10

Checking in the **Hardware Asset** view

You can register hardware assets within an organization, and check their status in a list. Peripheral devices (such as FD drives and DVD drives) and USB devices are also managed in this view.

You can check the status of stocktaking or search for computers in stock. Associating support contract information with hardware assets will enable you to check the contact information about the support center when problems occur on a specific hardware asset.



Hardware Assets - Department List : 117011

Device Type	Asset #	Device Name	Manufactu...	Asset Sta...	Planned As...	Planned D...	Last Track...
☑ PC		Sim16001		Unconfir...		-	-
PC		Sim16002		Unconfir...		-	-
PC		Sim16003		Unconfir...		-	-
PC		Sim16004		Unconfir...		-	-
PC		Sim16005		Unconfir...		-	-
PC		Sim16006		Unconfir...		-	-
PC		Sim16007		Unconfir...		-	-
PC		Sim16008		Unconfir...		-	-
PC		Sim16009		Unconfir...		-	-
PC		Sim16010		Unconfir...		-	-
PC		Sim16011		Unconfir...		-	-
PC		Sim16012		Unconfir...		-	-
PC		Sim16013		Unconfir...		-	-

Sim16001

Hardware Asset Details

Asset #	
Device Name	Sim16001
Description	
Files Attached	
Contract Vendor Name	
Contract Date	-
Asset Status	Unconfirmed
Planned Asset Status	
Planned Date	-
Last Tracked Date	-
Department	
Location	
User Name	

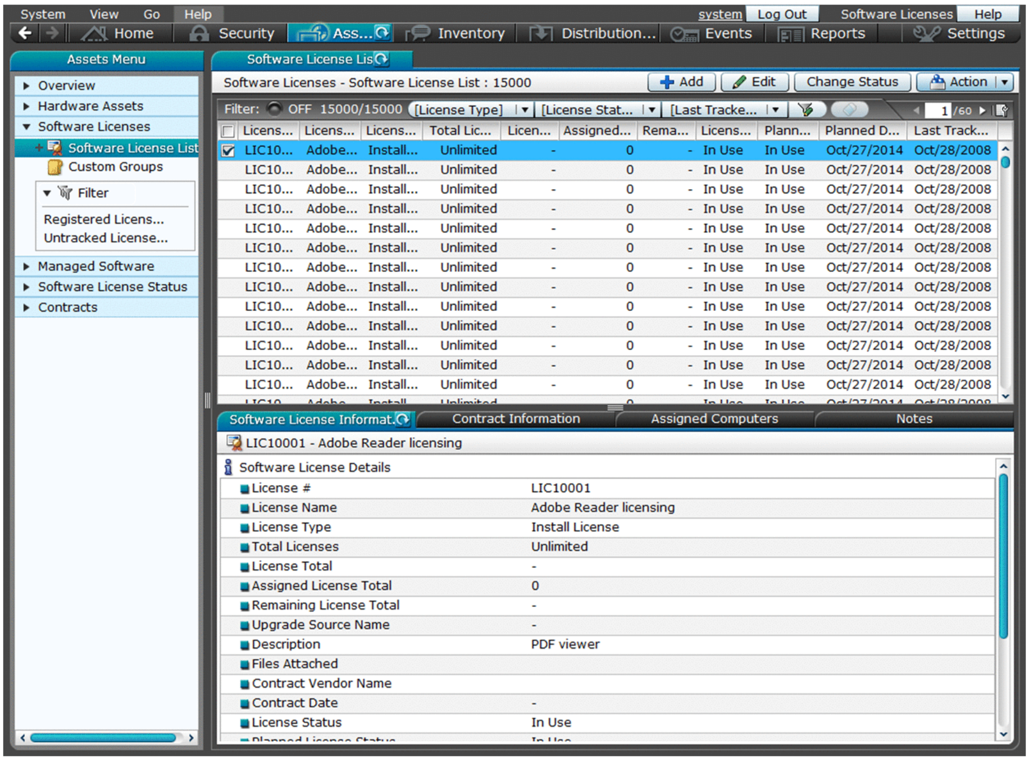
Device Inventory Details

Device Type	PC
Model	CF-T9JWFCDS
Manufacturer	
Serial #	
Processor	Intel(R) Core(TM)2 Duo CPU ...
Total Memory	4GB
Storage Capacity	298GB
Free Storage Capacity	208GB
IP Address	192.168.161.101
Subnet Mask	255.255.255.0
MAC Address	42:6f:99:e5:3e:81
Host Name	Sim16001
Operating System	Microsoft Windows 7 Profes...

Checking in the **Software Licenses** view

You can register software licenses owned by an organization, and manage them in a list. You can check which devices are allowed to use licenses, as well as checking the number of owned licenses.

By associating contract information with software licenses, you can also check the costs for software license contracts and the contract terms.



Software Licenses - Software License List : 15000

Filter: OFF 15000/15000

□	Licens...	Licens...	Licens...	Total Lic...	Licen...	Assigned...	Rema...	Licens...	Plann...	Planned D...	Last Track...
☑	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008
	LIC10...	Adobe...	Install...	Unlimited	-	0	-	In Use	In Use	Oct/27/2014	Oct/28/2008

LIC10001 - Adobe Reader licensing

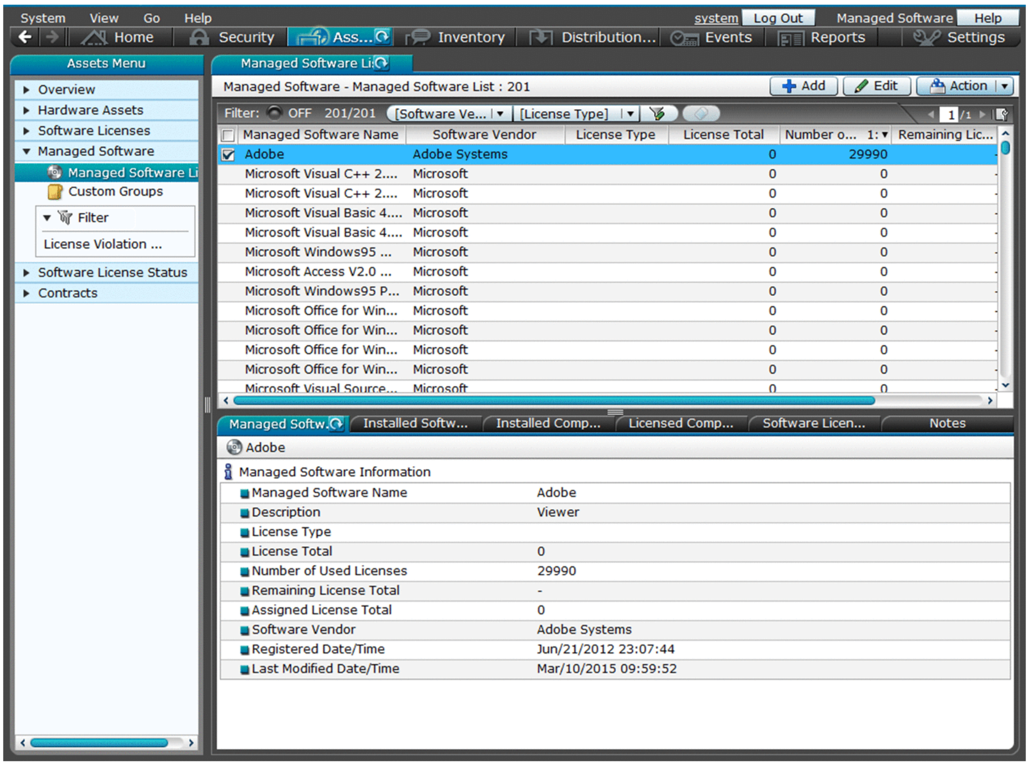
Software License Details

License #	LIC10001
License Name	Adobe Reader licensing
License Type	Install License
Total Licenses	Unlimited
License Total	-
Assigned License Total	0
Remaining License Total	-
Upgrade Source Name	-
Description	PDF viewer
Files Attached	
Contract Vendor Name	
Contract Date	-
License Status	In Use

Checking in the **Managed Software** view

You can register information about software programs for which the number of used licenses is to be counted, and check the usage status for each software program. By associating managed software programs and software licenses, you will be able to check the difference between the number of owned licenses and the number of used licenses.

You can also check which computers each software program has been installed on.


System View Go Help
system Log Out Managed Software Help
Home Security Ass... Inventory Distribution... Events Reports Settings
Assets Menu
Overview
Hardware Assets
Software Licenses
Managed Software
Managed Software Li
Custom Groups
Filter
License Violation ...
Software License Status
Contracts
Managed Software Li
Add Edit Action
Filter: OFF 201/201 [Software Ve... [License Type]
1 /1
Managed Softw... Installed Softw... Installed Comp... Licensed Comp... Software Licen... Notes

Managed Software - Managed Software List : 201

☐	Managed Software Name	Software Vendor	License Type	License Total	Number o...	Remaining Lic...
☑	Adobe	Adobe Systems		0	29990	-
	Microsoft Visual C++ 2....	Microsoft		0	0	-
	Microsoft Visual C++ 2....	Microsoft		0	0	-
	Microsoft Visual Basic 4....	Microsoft		0	0	-
	Microsoft Visual Basic 4....	Microsoft		0	0	-
	Microsoft Windows95 ...	Microsoft		0	0	-
	Microsoft Access V2.0 ...	Microsoft		0	0	-
	Microsoft Windows95 P...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Office for Win...	Microsoft		0	0	-
	Microsoft Visual Source...	Microsoft		0	0	-

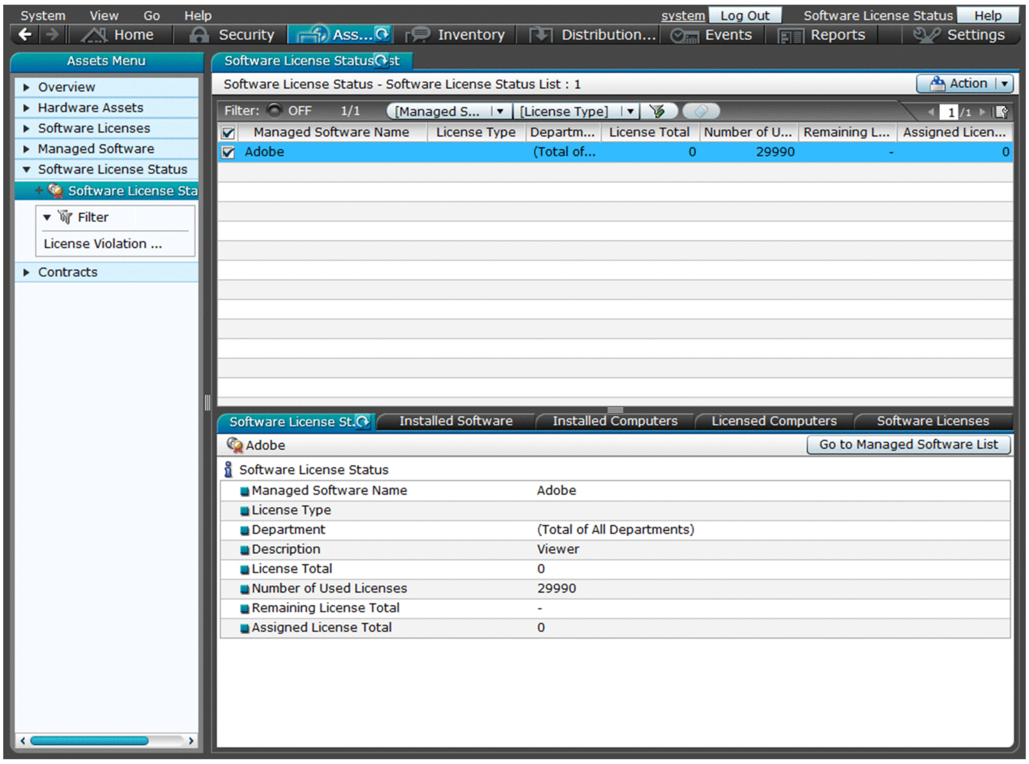
Adobe

Managed Software Information

Managed Software Name	Adobe
Description	Viewer
License Type	
License Total	0
Number of Used Licenses	29990
Remaining License Total	-
Assigned License Total	0
Software Vendor	Adobe Systems
Registered Date/Time	Jun/21/2012 23:07:44
Last Modified Date/Time	Mar/10/2015 09:59:52

Checking in the **Software License Status List** view

You can manage the usage status of software licenses for each managed software program. The total number of owned licenses and the number of remaining licenses are counted so that you can collectively check the usage status of software licenses.


System View Go Help
system Log Out Software License Status Help
Home Security Ass... Inventory Distribution... Events Reports Settings
Assets Menu
Overview
Hardware Assets
Software Licenses
Managed Software
Software License Status
Software License Sta
Filter
License Violation ...
Contracts
Software License Status List
Action
Filter: OFF 1/1 [Managed S... [License Type]
1 /1
Software License St... Installed Software Installed Computers Licensed Computers Software Licenses
Go to Managed Software List

Software License Status - Software License Status List : 1

☑	Managed Software Name	License Type	Departm...	License Total	Number of U...	Remaining L...	Assigned Licen...
☑	Adobe		(Total of...	0	29990	-	0

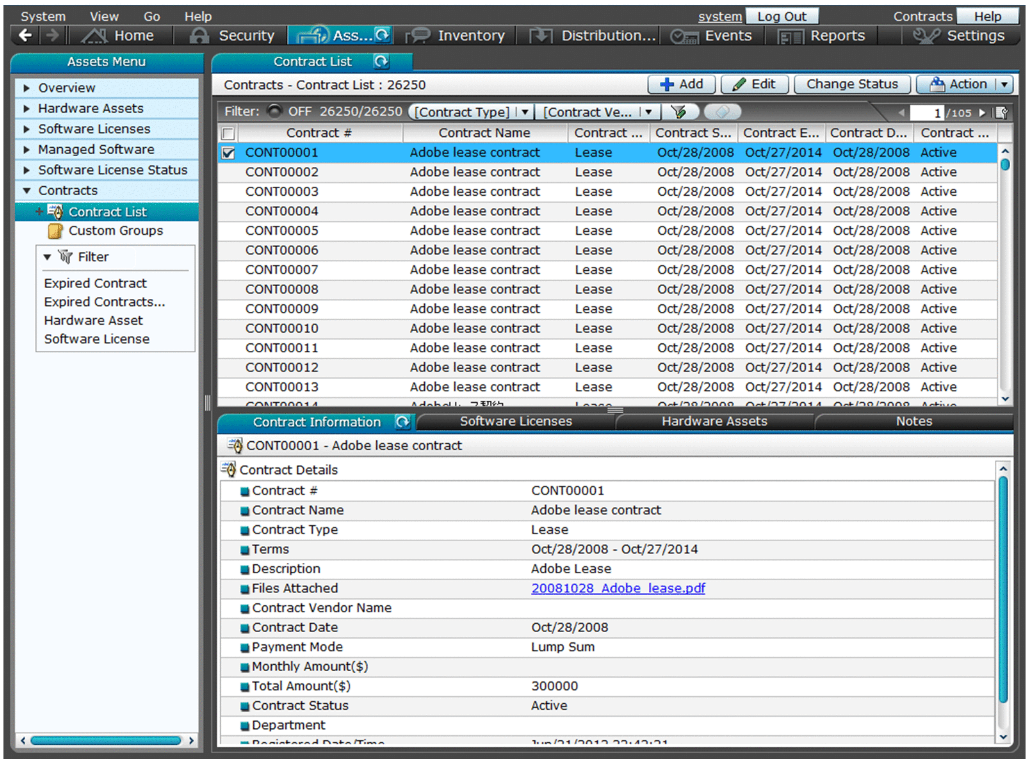
Adobe

Software License Status

Managed Software Name	Adobe
License Type	
Department	(Total of All Departments)
Description	Viewer
License Total	0
Number of Used Licenses	29990
Remaining License Total	-
Assigned License Total	0

Checking in the **Contracts** view

You can register contract information about hardware assets and software licenses, and manage that information in a list. You can check information such as the status and type of a contract, and the expiration date of the contract.



Contracts - Contract List : 26250

Filter: OFF 26250/26250

□	Contract #	Contract Name	Contract ...	Contract S...	Contract E...	Contract D...	Contract ...
☑	CONT00001	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00002	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00003	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00004	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00005	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00006	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00007	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00008	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00009	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00010	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00011	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00012	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active
	CONT00013	Adobe lease contract	Lease	Oct/28/2008	Oct/27/2014	Oct/28/2008	Active

CONT00001 - Adobe lease contract

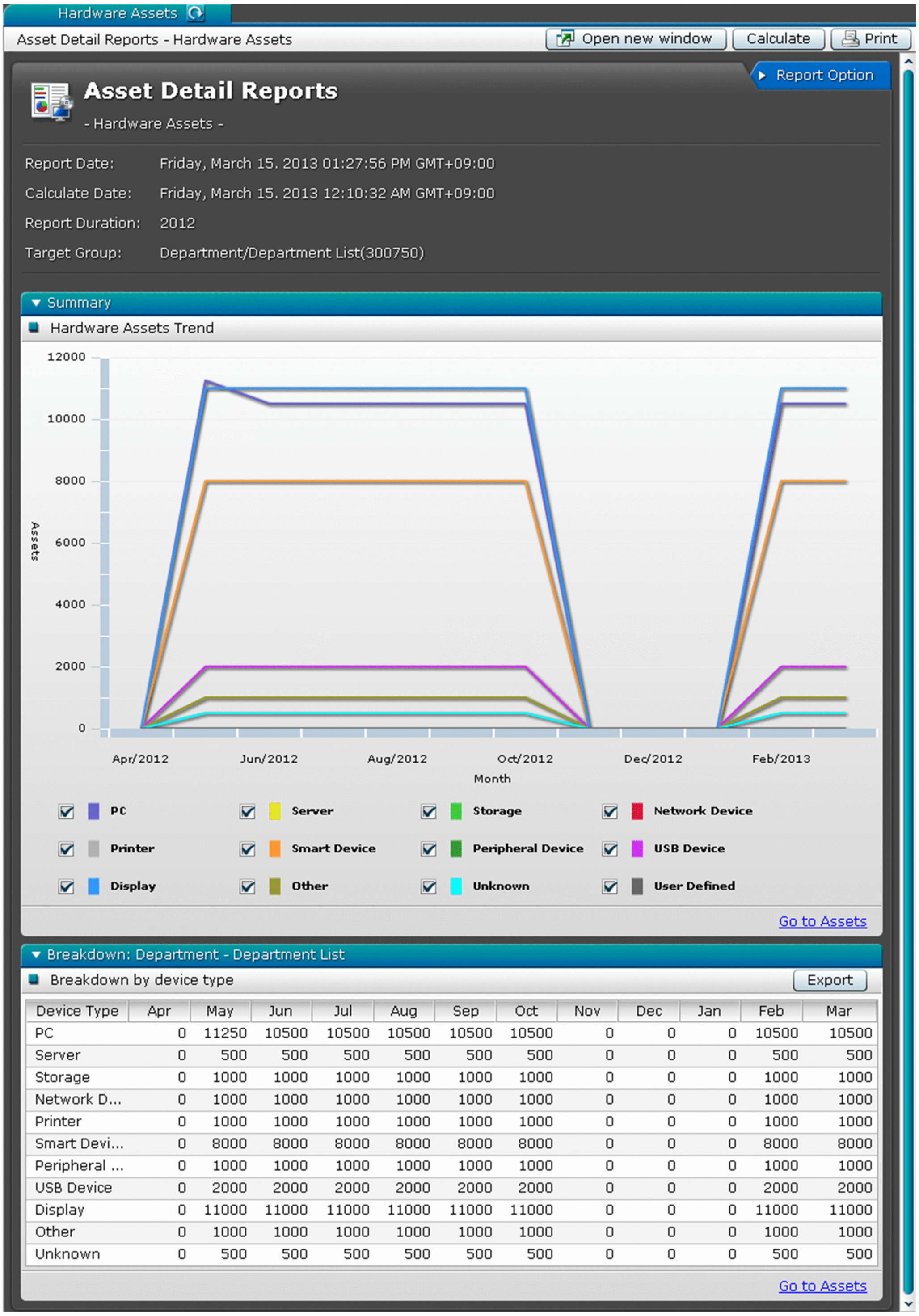
Contract Details

Contract #	CONT00001
Contract Name	Adobe lease contract
Contract Type	Lease
Terms	Oct/28/2008 - Oct/27/2014
Description	Adobe Lease
Files Attached	20081028_Adobe_lease.pdf
Contract Vendor Name	
Contract Date	Oct/28/2008
Payment Mode	Lump Sum
Monthly Amount($)	
Total Amount($)	300000
Contract Status	Active
Department	

Checking a report

In **Summary Reports** and **Asset Detail Reports** , you can check asset status.

In **Summary Reports**, you can check the hardware assets for which replacement is planned, the usage status of software licenses, and the contracts for which the expiration date is approaching. In **Asset Detail Reports**, you can check the transition of the number of hardware assets, excess and deficiency of software licenses, and the costs for assets.



Asset Detail Reports - Hardware Assets

Asset Detail Reports

- Hardware Assets -

Report Date: Friday, March 15. 2013 01:27:56 PM GMT+09:00

Calculate Date: Friday, March 15. 2013 12:10:32 AM GMT+09:00

Report Duration: 2012

Target Group: Department/Department List(300750)

Hardware Assets Trend

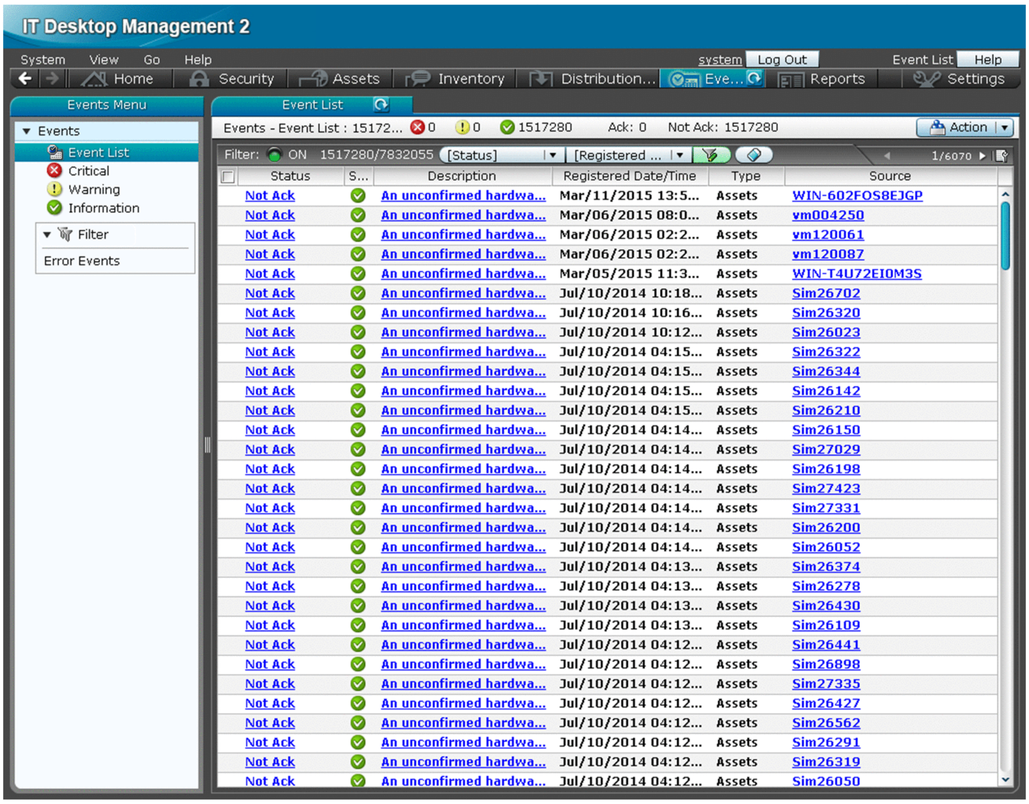
Breakdown: Department - Department List

Breakdown by device type

Device Type	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
PC	0	11250	10500	10500	10500	10500	10500	0	0	0	10500	10500
Server	0	500	500	500	500	500	500	0	0	0	500	500
Storage	0	1000	1000	1000	1000	1000	1000	0	0	0	1000	1000
Network D...	0	1000	1000	1000	1000	1000	1000	0	0	0	1000	1000
Printer	0	1000	1000	1000	1000	1000	1000	0	0	0	1000	1000
Smart Devi...	0	8000	8000	8000	8000	8000	8000	0	0	0	8000	8000
Peripheral ...	0	1000	1000	1000	1000	1000	1000	0	0	0	1000	1000
USB Device	0	2000	2000	2000	2000	2000	2000	0	0	0	2000	2000
Display	0	11000	11000	11000	11000	11000	11000	0	0	0	11000	11000
Other	0	1000	1000	1000	1000	1000	1000	0	0	0	1000	1000
Unknown	0	500	500	500	500	500	500	0	0	0	500	500

Checking in the Events module

In the Events module, you can check events related to asset management, such as registration of assets, changes of asset status, and addition and deletion of software licenses.



Events - Event List : 15172... ⊗ 0 ! 0 ✓ 1517280 Ack: 0 Not Ack: 1517280

Filter: ● ON 1517280/7832055 [Status] [Registered ... 1/6070

□	Status	S...	Description	Registered Date/Time	Type	Source
	Not Ack	✓	An unconfirmed hardwa...	Mar/11/2015 13:5...	Assets	WIN-602FOS8EJGP
	Not Ack	✓	An unconfirmed hardwa...	Mar/06/2015 08:0...	Assets	vm004250
	Not Ack	✓	An unconfirmed hardwa...	Mar/06/2015 02:2...	Assets	vm120061
	Not Ack	✓	An unconfirmed hardwa...	Mar/06/2015 02:2...	Assets	vm120087
	Not Ack	✓	An unconfirmed hardwa...	Mar/05/2015 11:3...	Assets	WIN-T4U72EI0M3S
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 10:18...	Assets	Sim26702
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 10:16...	Assets	Sim26320
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 10:12...	Assets	Sim26023
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:15...	Assets	Sim26322
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:15...	Assets	Sim26344
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:15...	Assets	Sim26142
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:15...	Assets	Sim26210
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim26150
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim27029
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim26198
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim27423
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim27331
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim26200
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:14...	Assets	Sim26052
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:13...	Assets	Sim26374
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:13...	Assets	Sim26278
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:13...	Assets	Sim26430
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:13...	Assets	Sim26109
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26441
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26898
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim27335
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26427
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26562
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26291
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26319
	Not Ack	✓	An unconfirmed hardwa...	Jul/10/2014 04:12...	Assets	Sim26050

(1) Differences between the Device module and the Assets module

The following describes the differences between the Device module and the Assets module.

Device module

The Device module is used to check the status of devices currently connected to the network.

The Device module displays a list of managed devices. The managed devices are basically connected to the network and communicate with the management server. Therefore, in the Device module, you can check the latest information collected from devices, or send notification messages to the displayed devices.

> **Tip**
>
> One license is consumed for one managed device. This means that product licenses are required to display devices in the Device module.

In the **Software Inventory** view of the Device module, you can check software information collected from computers in a list. You can check the number of software programs actually installed, and detailed information about software programs.

Assets module

The Assets module is used to manage the assets owned by an organization.

In the **Hardware Assets** view, you can manage the hardware assets owned by an organization. The owned hardware assets may include devices connected to the network or devices stored offline as stock. Computers and displays might be managed separately. Asset management tasks may include management of disposed assets that no longer exist in an organization. Thus, you can use **Hardware Assets** view to manage the assets owned by an organization and their statuses regardless of whether the assets can communicate with the management server. You can register and manage hardware assets as you like in the **Hardware Assets** view.

> **Tip**
>
> No license is needed to register asset information.

> **Tip**
>
> If a device is set to be managed, hardware asset information related to the device is automatically registered in the **Hardware Assets** view. Therefore, same devices might be displayed in the Device module and in the Assets module immediately after JP1/IT Desktop Management 2 is installed.

Furthermore, in the Device module, only the information collected from devices is displayed, but in the Assets module, the administrator can input and manage information. If a device management ledger already exists, you can utilize that existing information by importing it to the Assets module.

In the Assets module, you can also manage the usage status of software licenses, as well as hardware assets. In the **Software Inventory** view of the Device module, you can check the number of installed software programs. In the Assets module, you can register the number of software licenses owned by an organization and associate software information with the managed software information, so you will be able to check the difference between the number of used licenses and the total number of licenses. As described above, as for software, the Device module is used to check the collected information, but the Assets module is used to check the usage status of software licenses.

Related Topics:

- (2) Identifying related devices and hardware assets

2.11.7 Importing asset information

You can import asset information by using a CSV file. By importing asset information, you can add or edit information about assets in a batch. You can import asset information by using the **Import Assets** wizard or by executing the `ioutils importasset` command. The following five types of asset information can be imported:

- Hardware Assets
- Software Licenses
- Managed Software
- Contracts
- Contract Vendor List

(1) Hardware asset fields and formats in imported CSV files

Data in an imported CSV file must be in defined formats. The table below describes the hardware asset fields that can be imported and the defined formats.

Tip

When data in a CSV file is imported, the data is associated with the existing hardware asset information, using one of several fields as the mapping key. These fields are **Asset #**, **Serial #** (BIOS information), **IP Address**, **MAC Address**, **Host Name**, **IMEI**, and **Contract Phone**. When existing hardware asset information is associated, it is updated according to the imported data for the corresponding fields. When the existing hardware asset information is not associated, the imported data is registered as new hardware asset information.

Tip

In the **Hardware Assets** view of the Assets module, if a hyphen (-) is displayed for a field in the information area, the hyphen (-) changes to a null string after hardware asset information is imported. This is done so that hardware asset information can be correctly imported when exported hardware information is imported without change.

Field	Format of data	Whether can be omitted
Asset #	Alphanumerics with 32 or less characters, and the following signs: exclamation mark (!), double quotation mark ("), hash mark (#), dollar sign ($), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (|), right curly bracket (}), and swung dash (~)	N
Device Name	A character string with 256 or less characters	Y
Tracked Date	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year If omitted, **Jan/01/1970** is set when new hardware asset information is registered.	Y
Description	A character string with 1,024 or less characters	Y
Asset Status	One of the fields registered in **Asset Status**. However, you cannot specify **Unconfirmed**. If omitted, **In Use** is set when new hardware asset information is registered.	Y
Planned Asset Status[#1]	One of the fields registered in **Asset Status**. However, you cannot specify **Unconfirmed**.	Y
Planned Date[#1]	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year	Y
Department	Hierarchical structure of the registered department. Specify the hierarchical structure with 512 or less characters and with 40 or less hierarchies. Specify each hierarchy name with 256 or less characters. Delimit hierarchies by a slash (/). You can omit a slash (/) at the beginning or at the end of the hierarchical structure. However, even if you omit a slash, one character is counted.[#2] Example: `/General Affairs Department/Administration Section/` If the specified hierarchy does not exist, a new hierarchy is created when data is imported. If omitted, **Unknown** is set when new hardware asset information is registered.	Y
Location	Hierarchical structure of the registered location.	Y

Field	Format of data	Whether can be omitted
Location	Specify the hierarchical structure with 512 or less characters and with 40 or less hierarchies. Specify each hierarchy name with 256 or less characters. Delimit hierarchies by a slash (`/`). You can omit a slash (`/`) at the beginning or at the end of the hierarchical structure. However, even if you omit a slash, one character is counted.#2 Example: `/Building A/1F/` If the specified hierarchy does not exist, a new hierarchy is created when data is imported. If omitted, **Unknown** is set when new hardware asset information is registered.	Y
User Name	A character string with 256 or less characters#2	Y
E-mail	A character string with 256 or less characters#2	Y
Phone	A character string with 256 or less characters#2	Y
Account	A character string with 256 or less characters#2	Y
Model	A character string with 256 or less characters	Y
Serial #	A character string with 256 or less characters	N
Total Memory	A number in the range from 0 to 9,223,372,036,854,775,807 (in bytes). You can also add a unit of size (`B`, `KB`, `MB`, `GB`, `TB`, or `PB`) at the end. Do not enter a comma (`,`) as a delimiter.	Y
Storage Capacity	A number in the range from 0 to 9,223,372,036,854,775,807 (in bytes). You can also add a unit of size (`B`, `KB`, `MB`, `GB`, `TB`, or `PB`) at the end. Do not enter a comma (`,`) as a delimiter.	Y
Free Storage Capacity	A number in the range from 0 to 9,223,372,036,854,775,807 (in bytes). You can also add a unit of size (`B`, `KB`, `MB`, `GB`, `TB`, or `PB`) at the end. Do not enter a comma (`,`) as a delimiter. This field is not imported if **Device Type** is **Display**.	Y
IP Address	Write in the following format: *nnn*`.`*nnn*`.`*nnn*`.`*nnn* Specify a value in the range from 0.0.0.0 to 255.255.255.255.	N
Subnet Mask	Write in the following format: *nnn*`.`*nnn*`.`*nnn*`.`*nnn* Specify a value in the range from 0.0.0.0 to 255.255.255.255.	Y
MAC Address	Write in the following format (*x*: 0 to F): • *xxxxxxxxxx* • *xx*`-`*xx*`-`*xx*`-`*xx*`-`*xx*`-`*xx* • *xx*`:`*xx*`:`*xx*`:`*xx*`:`*xx*`:`*xx* Note that you can import data even if hyphens (`-`) and colons (`:`) are mixed as delimiters.	N
Host Name	A character string with 256 or less characters	N
Display Type	One of the fields registered in **Display Type**	Y
Display Size	A number in the range from 0 to 256	Y
Display Graphic Mode	One of the fields registered in **Display Graphic Mode**	Y
UDID	A character string with 128 or less characters	Y
IMEI	A character string with 64 or less characters	Y
IMSI	A character string with 64 or less characters	Y

Field	Format of data	Whether can be omitted
ICCID	A character string with 64 or less characters	Y
Carrier	A character string with 512 or less characters	Y
Contract Phone	Numbers, hyphens (-), and plus signs (+)	Y
Device Type	One of the fields registered in **Device Type**. If omitted, **Unknown** is set when new hardware asset information is registered.	Y
CPU	A character string with 256 or less characters	Y
OS	A character string with 256 or less characters	Y
Manufacturer	A character string with 256 or less characters	Y
Custom Fields	Data type set in the **Asset Field Definitions** view (under **Assets**) of the Settings module	Y #3
Device instance ID	Alphanumeric characters and the following signs, with 256 or less characters: exclamation mark (!), double quotation mark ("), hash mark (#), dollar sign ($), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (|), right curly bracket (}), and swung dash (~)	Y

Legend: Y: The setting can be omitted. N: At least one specification is required.

#1: A set of **Planned Asset Status** and **Planned Date** must be imported.

#2: If the data type is **Text** and characters for the field is restricted, data in a CSV file must follow the restrictions.

#3: Setting is required for custom fields that require input.

Tip

The fields to be imported do not have to be enclosed by double quotation marks ("). However, if the data to be imported includes a comma (,), enclose the data by double quotation marks ("). For example, when you import `AB,CD`, specify it as `"AB,CD"`.

(2) Software license fields and formats in imported CSV files

Data in an imported CSV file must be in defined formats. The table below describes the software license fields that can be imported and their formats.

Tip

When data in a CSV file is imported, the data is associated with the existing software license information, using **License #** as the mapping key. When the existing software license information is associated, it is updated according to the imported data for the corresponding fields. When the existing software license information is not associated, the imported data is registered as new software license information.

Field	Format of data	Whether can be omitted
License #	Alphanumerics with 32 or less characters, and the following signs: exclamation mark (!), double quotation mark ("), hash mark (#), dollar sign ($), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (|), right curly bracket (}), and swung dash (~)	N
License Name	A character string with 256 or less characters	Y
License Type	One of the fields registered in **License Type** If omitted, **Install License** is set when new software license information is registered.	Y
Total Licenses	A number in the range from 0 to 2,147,483,647 If omitted, **Unlimited** is set when new software license information is registered. Do not enter a comma (,) as a delimiter.	Y
Tracked Date	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year	Y
Department	Hierarchical structure of the registered department. Specify the hierarchical structure with 512 or less characters and with 40 or less hierarchies. Specify each hierarchy name with 256 or less characters. Delimit hierarchies by a slash (/). You can omit a slash (/) at the beginning or at the end of the hierarchical structure. However, even if you omit a slash, one character is counted.#3 Example: `/General Affairs Department/Administration Section/` If the specified hierarchy does not exist, a new hierarchy is created when data is imported. If omitted, **Unknown** is set when new hardware asset information is registered.	Y
Description	A character string with 1,024 or less characters	Y
License Status	One of the fields registered in **License Status** If omitted, **In Use** is set when new software license information is registered.	Y
Planned License Status#1	One of the fields registered in **License Status**	Y
Planned Date#1	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year	Y
Custom Fields	Data type set in the **Asset Field Definitions** view (under **Assets**) of the Settings module	Y #2

Legend: Y: The setting can be omitted. N: The setting cannot be omitted.

#1: A set of **Planned Asset Status** and **Planned Date** must be imported.

#2: Setting is required for custom fields that require input.

#3: If the data type is **Text** and the number of characters for the field is restricted, data in a CSV file must follow the restrictions.

Tip

The fields to be imported do not have to be enclosed by double quotation marks ("). However, if the data to be imported includes a comma (,), enclose the data by double quotation marks ("). For example, when you import AB,CD, specify it as "AB,CD".

(3) Managed software fields and formats in imported CSV files

Data in an imported CSV file must be in defined formats. The table below describes the managed software fields that can be imported and their formats.

Tip

When data in a CSV file is imported, the data is associated with the existing managed software information, using **Managed Software Name** as the mapping key. When the existing managed software information is associated, it is updated according to the imported data for the corresponding fields in the imported data. When the existing managed software information is not associated, the imported data is registered as new managed software information.

Field	Format of data	Whether can be omitted
Managed Software Name	A character string with 512 or less characters	N
Manufacturer	A character string with 128 or less characters	Y
Description	A character string with 1,024 or less characters	Y

Legend: Y: The setting can be omitted. N: The setting cannot be omitted.

Tip

The fields to be imported do not have to be enclosed by double quotation marks ("). However, if the data to be imported includes a comma (,), enclose the data by double quotation marks ("). For example, when you import AB,CD, specify it as "AB,CD".

(4) Contract fields and formats in imported CSV files

Data in an imported CSV file must be in defined formats. The table below describes the contract fields that can be imported and their formats.

Tip

When data in a CSV file is imported, the data is associated with the existing contract information, using **Contract #** as the mapping key. When the contract information is associated, it is updated according to the imported data for the corresponding fields. When the contract information is not associated, the imported data is registered as new contract information.

Field	Format of data	Whether can be omitted
Contract #	Alphanumerics with 32 or less characters, and the following signs: exclamation mark (!), double quotation mark ("), hash mark (#), dollar sign ($), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), slash (/), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), backslash (\), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (|), right curly bracket (}), and swung dash (~)	N
Contract Name	A character string with 256 or less characters	Y
Contract Type	One of the fields registered in **Contract Type** If omitted, **Fixed** is set when new contract information is registered.	Y
Contract Date	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year	Y
Contract Start Date	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year	Y #1
Contract End Date	Write in the following format: *mmm*/*dd*/*yyyy* *mmm*: Month, *dd*: Day, *yyyy*: Year	Y #1
Contract Status	One of the fields registered in **Contract Status** If omitted, **Active** is set when new contract information is registered.	Y
Department	Hierarchical structure of the registered department. Specify the hierarchical structure with 512 or less characters and with 40 or less hierarchies. Specify each hierarchy name with 256 or less characters. Delimit hierarchies by a slash (/). You can omit a slash (/) at the beginning or at the end of the hierarchical structure. However, even if you omit a slash, one character is counted.#4 Example: `/General Affairs Department/Administration Section/` If the specified hierarchy does not exist, a new hierarchy is created when data is imported. If omitted, **Unknown** is set when new hardware asset information is registered.	Y
Payment Mode	Either of the following: • Monthly • Lump Sum	N
Monthly Cost	A number in the range from 0 to 9,223,372,036,854,775,807 Write this field when **Payment Mode** is **Monthly**. Do not enter a comma (,) as a delimiter.	Y#1
Total Cost	A number in the range from 0 to 9,223,372,036,854,775,807 Write this field when **Payment Mode** is **Lump Sum**. Do not enter a comma (,) as a delimiter.	Y #2
Description	A character string with 1,024 or less characters	Y
Custom Fields	Data type set in the **Asset Field Definitions** view (under **Assets**) of the Settings module	Y #3

Legend: Y: The setting can be omitted. N: The setting cannot be omitted.

#1: When **Payment Mode** is **Monthly**, **Contract Start Date**, **Contract End Date**, and **Monthly Cost** must be set.

#2: Setting is required when **Payment Mode** is **Lump Sum**.

#3: For custom fields that require input, be sure to set for the field.

#4: If the data type is **Text** and the number of characters for the field is restricted, data in a CSV file must follow the restrictions.

Tip

The fields to be imported do not have to be enclosed by double quotation marks (`"`). However, if the data to be imported includes a comma (`,`), enclose the data by double quotation marks (`"`). For example, when you import `AB,CD`, specify it as `"AB,CD"`.

(5) Contract vendor fields and formats in imported CSV files

Data in an imported CSV file must be in defined formats. The table below describes the contract vendor fields that can be imported and their formats.

Tip

When data in a CSV file is imported, the data is associated with the existing contract vendor information, using **Contract Vendor Name** as the mapping key. When the contract vendor information is associated, it is updated according to the imported data for the corresponding fields. When the contract vendor information is not associated, the imported data is registered as new contract vendor information.

Field	Format of data	Whether can be omitted
Contract Vendor Name	A character string with 256 or less characters	N
Address	A character string with 256 or less characters	Y
Phone	A number with 256 or less characters, hyphen (-), or plus sign (+)	Y
E-mail	A character string with 256 or less characters	Y
Contact Person	A character string with 256 or less characters	Y
Description	A character string with 1,024 or less characters	Y

Legend: Y: The setting can be omitted. N: The setting cannot be omitted.

Tip

The fields to be imported do not have to be enclosed by double quotation marks (`"`). However, if the data to be imported includes a comma (`,`), enclose the data by double quotation marks (`"`). For example, when you import `AB,CD`, specify it as `"AB,CD"`.

2.11.8 Exporting asset information

You can export asset information to a CSV file. Exported asset information can be used on other management servers or by other software programs. You can export asset information from the **Action** menu or by executing the `ioutils exportasset` command. You can export the following five types of asset information:

- Hardware Asset Information
- Software License Information
- Managed Software Information
- Contract Information
- Contract Vendor List

Tip

The administrator can specify the fields to be exported and target data to create a list suitable for a specific purpose.

For details about the data format output for each type of information, see the related topic.

Related Topics:

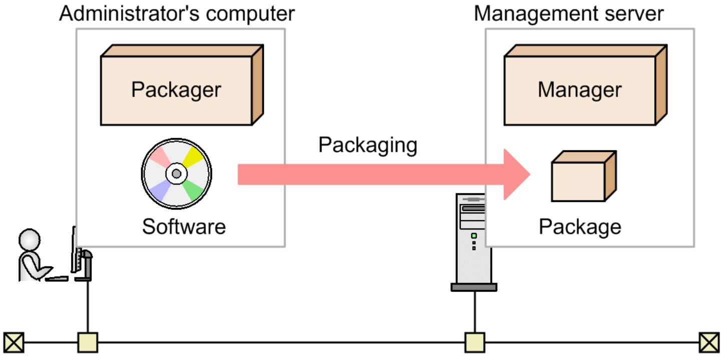
- (1) Hardware asset fields and formats in imported CSV files
- (2) Software license fields and formats in imported CSV files
- (3) Managed software fields and formats in imported CSV files
- (4) Contract fields and formats in imported CSV files
- (5) Contract vendor fields and formats in imported CSV files

2.12 Distributing software and files by using Remote Installation Manager

In JP1/IT Desktop Management 2, you can distribute software and files in a single operation from the management server to users' computers via the network. This section describes the flow of distributing software by using Remote Installation Manager. For details and operation procedures, see *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Distribution Function Administration Guide*.

The following describes the flow of distributing software.

1. Register (package) the software to be distributed.

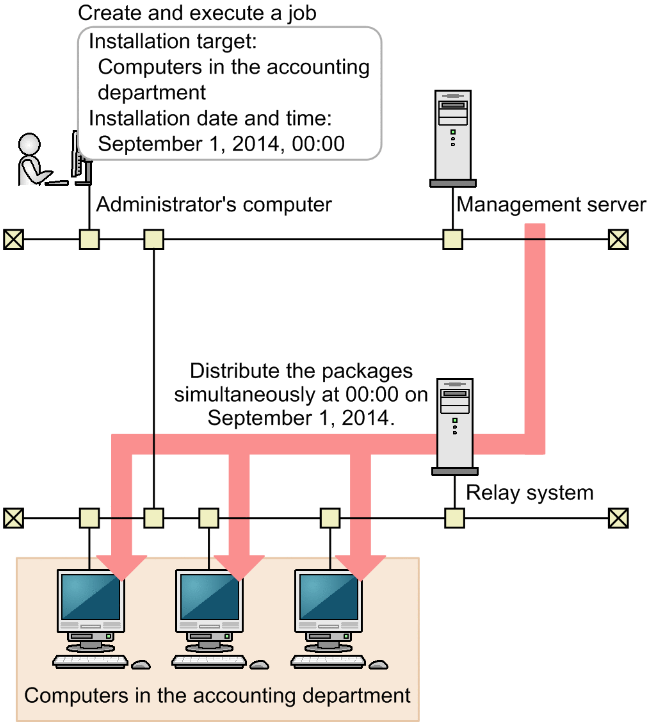


Legend:

Manager: JP1/IT Desktop Management 2 - Manager

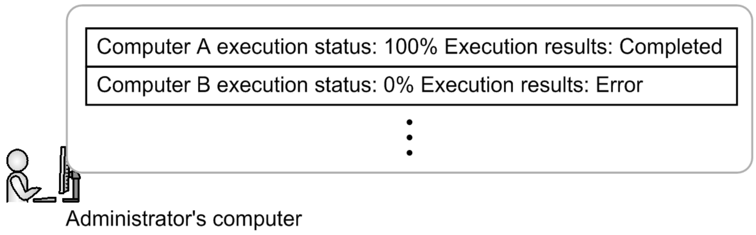
Register (package) the software you want to install on a user's computer to the management server. To package the software, use Packager, a component of JP1/IT Desktop Management 2 - Agent. You can specify the install condition of the distributed software when you package the software. A group of packaged software programs is called a package.

2. Execute a job and distribute (remotely install) the package.


Create and execute a job
Installation target:
Computers in the accounting department
Installation date and time:
September 1, 2014, 00:00
Administrator's computer
Management server
Distribute the packages simultaneously at 00:00 on September 1, 2014.
Relay system
Computers in the accounting department

Use Remote Installation Manager to create a job in which distribution-destination computers and distribution schedule are defined, and execute the job. For example, if you execute a job as defined in the figure above, the package will be distributed only to the computers belonging to the accounting department, at the same time, on September 1, 2014.

3. Checking the distribution status and execution results



Computer A execution status: 100% Execution results: Completed

Computer B execution status: 0% Execution results: Error

Check the distribution status and execution results in the **Job status** window of Remote Installation Manager. If distribution to a computer failed, take actions accordingly, and re-execute the job.

Rather than the system administrator distributing software to users' computers, you can instead allow users to select software and install it by themselves.

2.12.1 Distributing files efficiently using Remote Installation Manager

JP1/IT Desktop Management 2 provides features to efficiently perform distribution using Remote Installation Manager. This section describes some of the features.

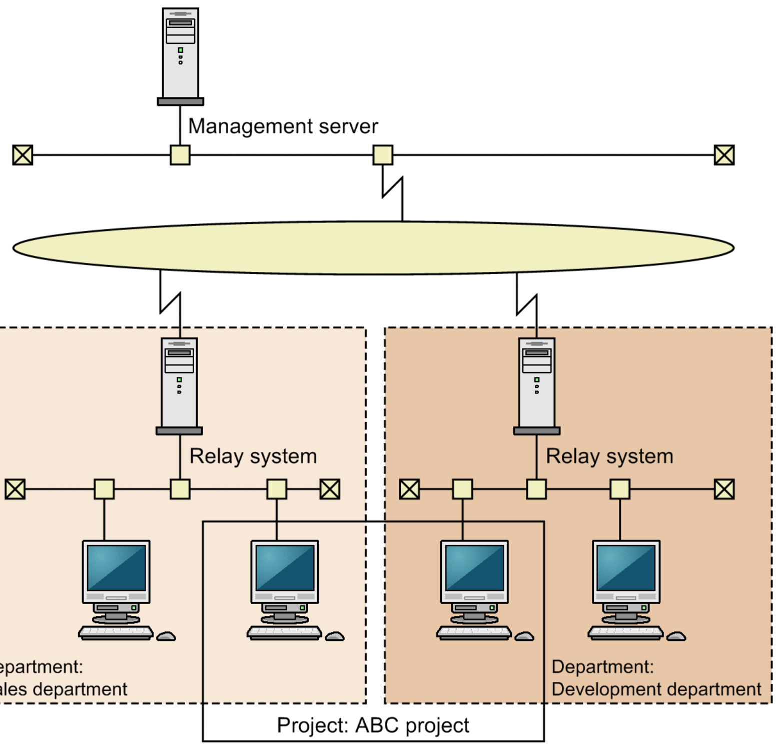
Load share using a relay system

Install a relay system when you have a large scale network or JP1/IT Desktop Management 2 has many managed computers. Installing a relay system can reduce loads on the management server.

Grouping distribution-destination computers.

You can group distribution-destination computers according to their purposes. By grouping computers, you can specify a group of destinations in a single operation. A computer can belong to multiple groups.

The following figure shows a configuration grouped by a department and by a project.



Setting installation conditions

Among the distribution-destination computers, you can perform installation only on the computers that satisfy the specified conditions. You create the conditions when packaging software or when creating a job, and the conditions are judged when the job is executed.

For example, you can configure to install a software program only on computers running Windows 7, or not to install a program on computers whose hard disk free space is 5 GB or less. In addition to conditions on hardware, you can check if a specific software is installed as a condition, or you can create a unique condition by launching an external program provided by the system administrator before installing software.

Specifying a date and time for distribution and for installation

You can specify a date and time on which a package is distributed (data is transferred) to computers, and a date and time on which software is installed on the computers.

Distribution date and time

You can specify a job execution date and time when you create a job. For example, you can distribute packages without placing a load on the network by specifying a job to be executed at nighttime.

Installation date and time

You can specify a time that a package is installed, when you package software, or when you create a job. This allows you to install or upgrade a program at a specified date and time on all destination computers.

Split distribution of a package

You can split a package by a specified volume rather than distributing it at a time. You can also specify a time interval (distribution interval), so that you can reduce the network load when distributing a high-volume package.

Multicast distribution

In normal unicast distribution of a package, the more the number of destination computers, the higher the number of packets sent from an upper-level system (management server or relay system). In multicast distribution of a package, all that is sent is the number of packets for a single job. A smaller number of packets can reduce load on the network.

Suspending and resuming a job

You can suspend a job temporarily. For example, if you planned to distribute software during non-business hours, but could not complete the distribution, you can suspend a job to stop the distribution temporarily, and then resume distribution during the next non-business hours.

Controlling distribution-destination computers

If a distribution-destination computer supports AMT or Wake on LAN, you can automatically turn that computer on or off. For example, you can turn on a shut-down computer during the nighttime, or on holidays, when the network load is light.

2.12.2 Distributing packages to computers managed offline by using Remote Installation Manager

You can distribute a package to computers managed offline without using the network. This feature is called *offline installation*. Offline installation is useful when you want to distribute a package to a standalone computer, or when you want to distribute a high-volume package without placing a load on the network.

To perform offline installation, store a package or data for offline installation on a media such as CD-R or USB memory device, and then execute the installation execution program on the distribution destination computer.

2.13 Distributing software and files to computers managed online (ITDM-compatible distribution)

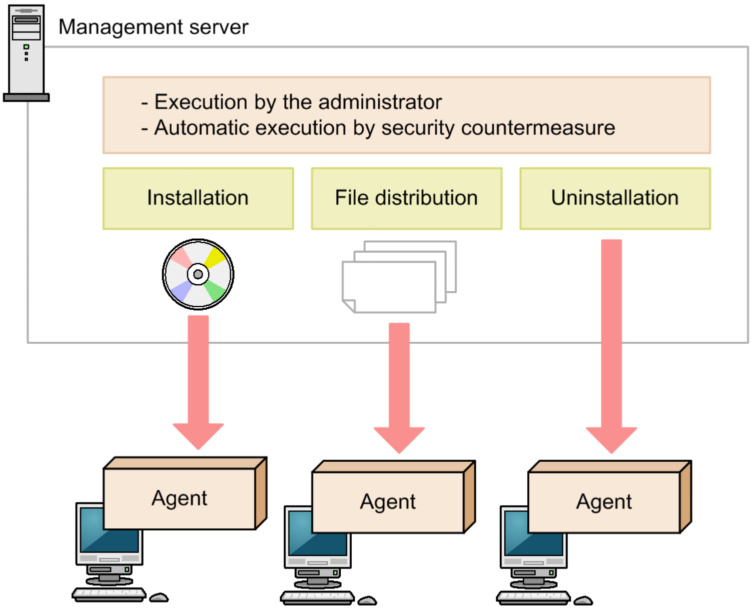
It is usually impractical for administrators to visit the computers within an organization to install new software or uninstall prohibited software.

JP1/IT Desktop Management 2 can use a management server to execute remote operations (such as installing and uninstalling software, and distributing files) on computers managed online. This functionality can reduce the time and effort of software installation or management. Also, software maintenance will become easier. For example, the administrator can install the latest versions of software programs in batch operations.

When you want to apply update files for the business system to all computers within an organization you could, for example, send the files by attaching them to emails or ask users to download the files. However, in such cases, you cannot ensure that the update files are applied to all computers. However, by using JP1/IT Desktop Management 2 to distribute files, you can understand the distribution status and ensure that the files are applied to all computers.

Tip

By using the distribution function, you can automatically install mandatory software or uninstall prohibited software based on the results of security judgment for software in use.


Management server
- Execution by the administrator
- Automatic execution by security countermeasure
Installation
File distribution
Uninstallation
Agent
Agent
Agent

Legend:

Agent: A computer with the agent installed.

Tip

If packages must be distributed to many devices, we recommend that you distribute the packages at different times. This is because distributing packages from the management server to many devices at the same time might overload the management server or network.

2.13.1 Managing packages and tasks (ITDM-compatible distribution)

You can use JP1/IT Desktop Management 2 to register and manage packages and tasks for installing software on target computers or for distributing files.

Definition of a package (ITDM-compatible distribution) and task

- Package (ITDM-compatible distribution)

  A package (ITDM-compatible distribution) is a set of software programs and files to be distributed to computers, and which are registered in JP1/IT Desktop Management 2 in the operation window. You can manage ITDM-compatible distribution packages in the **Packages** view of the Distribution (ITDM-compatible) module.The packages in this view are the packages to be distributed using the Distribution (ITDM-compatible) module. If you want to perform distribution using Remote Installation Manager, you must create a package using Packager.

  For software programs registered as an ITDM-compatible distribution package, you can set installation commands to perform silent installation of the software programs on distribution-destination computers. For the files registered as an ITDM-compatible distribution package, you can distribute the files to computers.

  For details about managing ITDM-compatible distribution packages, see (1) Managing packages.

- Task

  A task defines an execution schedule or action on the target computers, for distributing ITDM-compatible distribution packages to computers, or for uninstalling software from computers. You can manage tasks in the **Tasks** view of the Distribution (ITDM-compatible) module.

  When you create a task for distributing an ITDM-compatible distribution package, the package is distributed to computers based on the execution schedule. When you create a task for uninstalling software, software is uninstalled from computers based on the execution schedule.

  For details about managing tasks, see (2) Managing tasks.

Usage of packages (ITDM-compatible distribution) and tasks

- Installing software

  In the **Packages** view of the Distribution (ITDM-compatible) module, register an ITDM-compatible distribution package for the software you want to install. Then, in the **Tasks** view of the Distribution (ITDM-compatible) module, create a task for distributing the package. You can also use the Install Wizard to install software.

- Distributing files

  In the **Packages** view of the Distribution (ITDM-compatible) module, register an ITDM-compatible distribution package for the files you want to distribute. Then, in the **Tasks** view of the Distribution (ITDM-compatible) module, create a task for distributing the package. You can also use the File Distribution Wizard to distribute files.

- Uninstalling software

  In the **Tasks** view of the Distribution (ITDM-compatible) module, create an uninstallation task. You can also use the Uninstall Wizard to uninstall software. Software will be uninstalled when its name and version exactly match the specified software in the task.

Related Topics:

- 2.13.3 Preparation for distribution (ITDM-compatible distribution)

(1) Managing packages

In the **Packages** view of the Distribution (ITDM-compatible) module, you can create and manage packages.

You can also edit created packages. Registered data cannot be changed, but you can change such information as the installation commands and installation folders.

You can also delete unnecessary packages.

Access permissions for distributed packages are inherited from the distribution-destination folder. Access permissions for distributed packages can be changed on the distribution-destination computer by the user.

Important note

If the same file as a distributed package already exists at the distribution destination, access permissions for the distributed package are inherited from the existing file's access permissions.

Files to be registered in a package

The following table describes how to specify the files for individual types of packages you create.

Type	Files to be registered in a package
Software installation	If the software to be installed is an MSI file or EXE file, register that file.
	If the software to be installed contains multiple MSI files or EXE files or if other files than an MSI file or EXE file are required for installation, compress them in a ZIP file and register the ZIP file. You can store MSI or EXE files in any location in the ZIP file.
File distribution	If you want to distribute only one file, register that file.
	If you want to distribute multiple files at the same time, compress them in a ZIP file and register the ZIP file.

Tip

The maximum size of a file that can be registered in a package is 1 GB. If the file is a ZIP file, the total size of the unzipped files must also be no more than 2 GB.

Tip

Only software programs that support silent installation can be installed. Silent installation automatically performs installation on users' computers without displaying windows for installation. If the software to be installed is an MSI file, a silent installation command is automatically set when the package is created. If the software to be installed is an EXE file, a silent installation command must be manually specified.

Tip

If software does not have an installer, distribute the software as a file.

Tip

If a ZIP file is registered in a package, the ZIP file is automatically unzipped when the package is distributed to the target computer. If you want to distribute a ZIP file itself, further compress the ZIP file to another ZIP file and then register it in the package.

Tip

Packages used for distributing Widows updates are not displayed in the **Packages** view.

Related Topics:

- 2.13.3 Preparation for distribution (ITDM-compatible distribution)

(2) Managing tasks

In the **Tasks** view of the Distribution (ITDM-compatible) module, you can create and manage tasks. There are the following two types of tasks.

Tasks for package distribution

Tasks for installing software or distributing files. These types of tasks also execute automatic countermeasures for software (including Windows updates).

Tasks for uninstallation

Tasks for uninstalling software.

You can also edit created tasks. When you edit a task, you can change only the distribution destination without changing the distribution package and its schedule, or change the specified package without changing the distribution destination.

It is convenient to copy a task when you want to distribute multiple packages to the same destination or when you want to uninstall multiple software programs from the same computer.

You can also delete completed and unnecessary tasks.

The **Tasks** view of the Distribution (ITDM-compatible) module displays the execution status of tasks. For a task that failed distribution, investigate and correct the cause and then re-execute the task.

Classes of tasks

There are two classes of tasks.

Tasks executed by the administrator

Tasks created in the **Tasks** view of the Distribution (ITDM-compatible) module by the administrator of JP1/IT Desktop Management 2

Tasks executed by automatic countermeasure

Tasks automatically created based on the settings of automatic countermeasures for security policies. For details, see 2.13.2 Distribution enforced as an automatic countermeasure for security (ITDM-compatible distribution).

Related Topics:

- 2.13.3 Preparation for distribution (ITDM-compatible distribution)

2.13.2 Distribution enforced as an automatic countermeasure for security (ITDM-compatible distribution)

The distribution function can be used to automatically distribute Windows Updates and mandatory software. It can also be used to automatically uninstall software prohibited by a security policy.

Automatically installing Windows updates

When you set installation of Windows updates in a security policy, you can set installation of Windows updates as an automatic countermeasure.

When you set distribution of Windows updates as an automatic countermeasure, if Windows updates have not been installed on any computers for which the security policy is applied, Windows updates will be automatically distributed to and installed on those computers.

Automatically installing mandatory software

When you set mandatory software in a security policy, you can set installation of the mandatory software as an automatic countermeasure.

When you set installation of mandatory software as an automatic countermeasure, if the mandatory software programs have not been installed on any computers for which the security policy is applied, the software programs will be automatically distributed to and installed on those computers.

Automatically uninstalling prohibited software

When you set prohibited software in a security policy, you can set uninstallation of the software programs as an automatic countermeasure.

When you set uninstallation of software as an automatic countermeasure, if the prohibited software programs have been installed on any computers for which the security policy is applied, the software programs will be automatically uninstalled from those computers.

Note that a software program that does not appear in the **Add/Remove Programs** window in Windows is not uninstalled. If you want to uninstall such a program, create an uninstallation task in the **Tasks** view, and execute the task. For execution of an uninstallation task, see 2.13.1 Managing packages and tasks (ITDM-compatible distribution).

If you set distribution of Windows updates as an automatic countermeasure when setting a security policy, the Windows Update file and task will be automatically created. In this case, the task is displayed in the **Tasks** view of the Distribution (ITDM-compatible) module. However, the Windows Update file is not displayed in the **Packages** view. You can check whether the Windows Update file has been registered in the **Windows Update** view of the Security module.

If you set installation or uninstallation of software, set a package when specifying a security policy. A task is automatically created. In this case, the package and task are displayed in the **Packages** view and **Tasks** view of the Distribution (ITDM-compatible) module.

The type of the task created when an automatic countermeasure is set in a security policy is `Policy Based Task`. A task executed as an automatic countermeasure cannot be edited or copied. Also, when you delete a task, cancel the automatic countermeasure setting, or delete the Software Use setting for the security policy. The task will be automatically deleted depending on the security policy setting.

2.13.3 Preparation for distribution (ITDM-compatible distribution)

The following describes preparation for installing software, distributing files, and uninstalling software. First, common preparation for using the distribution function is described. Next, preparation for individual tasks is described.

Common preparation

Consider the following before using the distribution function.

Distribution destination computers

Determine the distribution-target computers. When you have many target computers, we recommend that you create a custom group for those computers.

Distribution schedule

Determine the distribution schedule. Setting schedules will enable you to perform distribution at night so that the distribution task will not affect business or to perform multiple tasks at the same time. You can also start distribution immediately without setting any schedules.

Automatic startup

You can configure the setting so that if the target computers are turned off, they will be turned on and distribution will be performed. Consider the use of this function when you want to perform distribution at night or to unused computers. Note that, to control computer power, the computers must support AMT or Wake on LAN.

Execution timing

You can set the timing of installing or uninstalling software or storing files after the task is received at a target computer. You can choose one from the following: execute immediately after the task is received, execute when a user logs on, or execute the next time the computer starts. For example, if a running business application may interfere with installation, it is better for you to perform the installation the next time the computer starts.

Messages to be displayed

You can display messages immediately before or after installation or uninstallation of software or distribution of files after a package is distributed. Use messages to notify users of installation or uninstallation, or of notes on the installed software.

Reducing load by distribution

You can reduce network load by restricting the network bandwidth used for distribution. You can also set an upper limit on the amount of data transferred per second when packages are distributed to computers to prevent agent software from occupying too much communication bandwidth with package transfer. For details, see 2.13.7 Reducing load by distribution (ITDM-compatible distribution).

Preparation for installing software

Prepare the software you want to install. You can install software whose installer is an MSI file or EXE file. If multiple files are required for installing software, compress them in a ZIP file. If a ZIP file includes multiple installers, you must check which installer will be used.

> **Tip**
>
> Only the software programs that support silent installation can be installed. Silent installation automatically performs installation on users' computers without displaying windows during installation.

> **Tip**
>
> If software does not have an installer, distribute the software as a file.

Preparation for distributing files

Prepare the file you want to distribute. If you want to distribute multiple files, compress them in a ZIP file. Also, determine the folder to be used for storing the file on the distribution target computers.

> **Tip**
>
> If a ZIP file is registered in a package, the ZIP file will be automatically unzipped when the package is distributed to the target computer. If you want to distribute a ZIP file itself, further compress the ZIP file in another ZIP file and then register it in the package.

> **Tip**
>
> When you determine the folder for storing files, use a folder that is common to the distribution target computers. If the specified folder does not exist on a target computer, the specified folder will be created.

When you distribute a file, you can configure the setting so that a command will be automatically executed on the distribution target computer after the distribution file is received. For example, if you set a command for executing a batch file, you can distribute the batch file and then run that batch file. If you want to use a command, check whether the command can be correctly executed beforehand.

Preparation for uninstalling software

Check whether information about the software program you want to uninstall is displayed in the **Software Inventory** view of the Device module. If it is not displayed, check the execution file name of the software program you want to uninstall.

> **Tip**
>
> If you uninstall a software program that is not displayed in Windows' **Programs and Features**, the execution file searched for by the software search conditions (or the file name specified when the task was created) will be deleted.

> **Tip**
>
> The software programs that are displayed in Windows' **Programs and Features** and that were installed by the Windows installer (MSI) can be automatically uninstalled without the uninstallation window being displayed on users' computers (silent uninstallation). For other software programs, the uninstallation window is displayed on the users' computer and the users must uninstall them.

Related Topics:

- (1) Conditions for power control

2.13.4 Types of software that can be uninstalled by the distribution function (ITDM-compatible distribution)

The following two types of software can be uninstalled by the distribution function.

Software registered in **Programs and Features**

These are software programs registered in Windows' **Programs and Features**.

If an uninstallation command is the Windows Installer, uninstallation is performed with the silent option (`/qn`) and the option for suppressing restart (`ReallySuppress`) specified. The return value is judged as follows:

- ERROR_SUCCESS(0): Normal termination
- ERROR_SUCCESS_REBOOT_INITIATED(1641): Restart is required.
- ERROR_SUCCESS_REBOOT_REQUIRED(3010): Restart is required.
- Other codes: Abnormal termination

If an uninstallation command is not the Windows Installer, the specified uninstallation command is executed. If the uninstallation command is executed, uninstallation is judged to have finished successfully.

Software registered in the **Software Search Conditions** view

These are software programs whose information was collected by a search for executable files (such as EXE files) on a computer with the conditions registered in the **Software Search Conditions** view of the Settings module.

2.13.5 Notes on distribution (ITDM-compatible distribution)

When you use the distribution function to install or uninstall software, set up a test environment for evaluation and verify that software is normally installed and uninstalled with local system account permission. Then, schedule the execution of tasks. This is because the specification and operation of the installer used for the distribution function is determined by the manufacturer of the installer, not by JP1/IT Desktop Management 2.

The following are notes on installing and uninstalling software, and distributing files:

- If the file you want to distribute and install is an EXE file, the target computer might not be restarted after installation.
- If the file you want to install is an EXE file, the value returned from the installer cannot be judged. So, the result of installation might not be correctly displayed.
- When you install software, if an MSI file is started from an EXE file, and the EXE file finishes execution before the result of installation is received, the result of installation might not be correctly displayed.
- If immediately after a distribution file is received at a target computer a command further distributes the file to another computer, the result of file distribution might not be correctly displayed.
- If the time is different on the management server and an agent-installed computer, power cannot be controlled normally.
- If the software you want to uninstall is an MSI file, silent uninstallation is executed. If the software is an EXE file, a dialog box is displayed on the computer. The user must manually uninstall the software as instructed by the dialog box.
- Do not specify, as an uninstallation task, software and OSs that cannot be uninstalled from **Programs and Features** in the Control Panel. Such uninstallation tasks will fail.
- Do not uninstall the software and files shown below. If you uninstall them, the OS or JP1/IT Desktop Management 2 might not correctly run.
    - Software and files that are related to OS operations
    - JP1/IT Desktop Management 2 and JP1/IT Desktop Management 2 components
    - Software and files that are related to JP1/IT Desktop Management 2 operations
- When some software programs are installed, files and folders may be created with specific user permissions. If such a software program is uninstalled by the distribution function, some of the files and folders might not be deleted. In such a case, the user must delete those files and folders after uninstallation.
- When some software programs are installed, shortcut icons may be created on the Desktop. If such a software program is uninstalled by the distribution function, the shortcut icon might not be deleted. In such a case, the user must delete the shortcut icon after uninstallation.
- Do not specify a software program as both mandatory software and prohibited software when automated countermeasures are set for installation and uninstallation. If you do so, automatic countermeasures for installation and uninstallation will be alternately performed because the software program is always judged to violate security settings.
- If the installer or uninstaller dialog box is displayed, the installer or uninstaller will be automatically terminated forcibly in one hour.

- When software is installed or uninstalled by the distribution function, the task is executed with local system account permissions. Also, when a command is executed after a file is distributed by the distribution function, the task is executed with local system account permissions.
- When you install an agent or network monitor agent, display the **Task Status Details** dialog box by clicking the link on the **Task Information** tab at the bottom of the **Task List** view. Then, check the result of installation. If the return code displayed in **Description** is `0`, the installation finished successfully.
- ITDM-compatible distribution on an agent and job execution cannot occur at the same time on the agent. Therefore, if a job is executed on the agent, the ITDM-compatible distribution status might remain *Waiting for execution*.

2.13.6 Postponing download or installation on a computer to which a package is distributed (ITDM-compatible distribution)

On a computer to which a package is distributed, the package will be downloaded and the software registered in the package will be installed.

The user of the computer can postpone downloading the package or installing the software if needed. Postponing download or installation can prevent the user from suspending ongoing processing during a hasty or important task. You can postpone download and installation again and again.

You can also postpone uninstallation or file distribution as well as installation.

Important note

You cannot postpone such operations when logging on to the computer by using the Remote Desktop function.

The following table describes how long download and installation can be postponed.

Operation	How long the operation can be postponed
Download	30 minutes In 30 minutes, download will automatically restart.
Installation	The user can specify how long it will take until the dialog box for starting installation is redisplayed from the following: • 10 minutes • 30 minutes • 1 hour

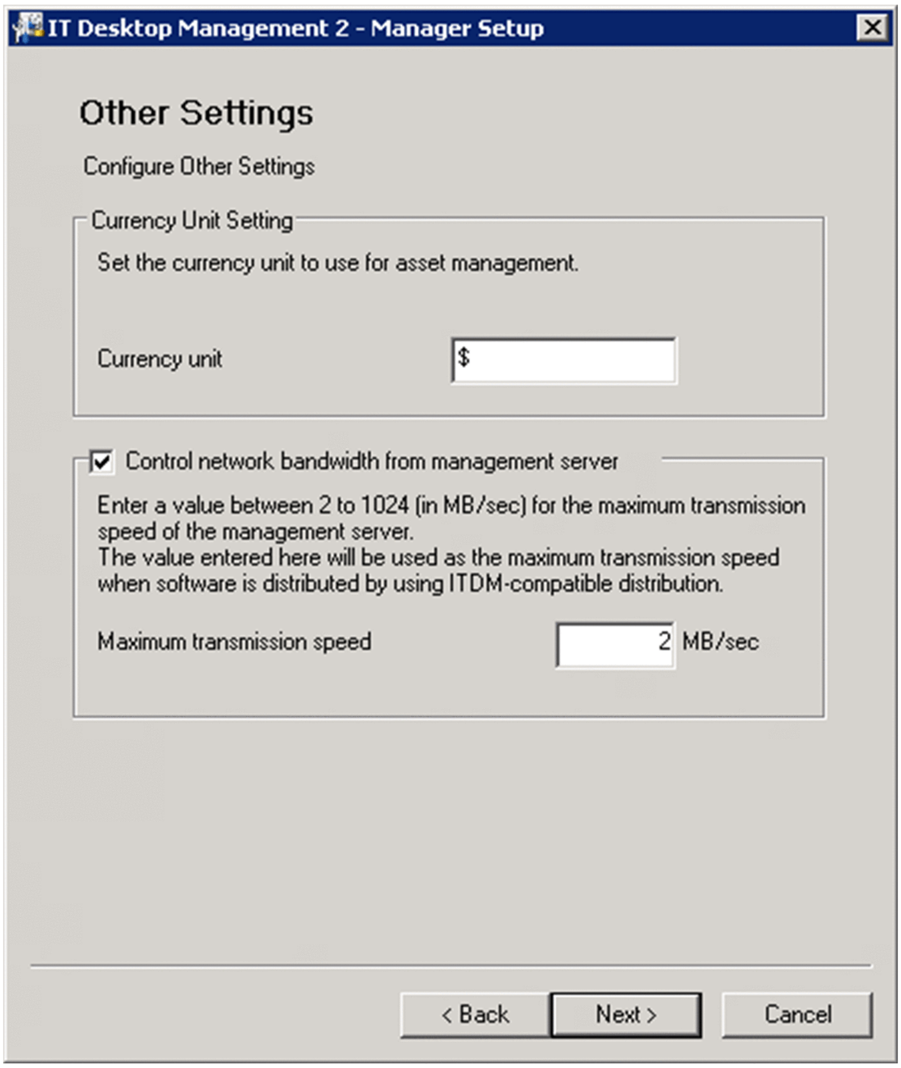
2.13.7 Reducing load by distribution (ITDM-compatible distribution)

When large amounts of software and files are distributed from the management server to user computers, the network or computers might become overloaded. To prevent such an overload, you can restrict the network bandwidth used for the distribution function and set an upper limit on the amount of data transferred per second.

Controlling the network bandwidth

If you specify a maximum transfer rate in the setup for JP1/IT Desktop Management 2 , the network bandwidth is controlled and data transfers will be limited to that setting. The maximum transfer rate is the maximum value that can be used for sending and receiving data between the management server and agent-installed computers. If the total amount of data sent and received per second reaches the specified upper limit, data transfer is temporarily suspended on the management server. This enables you to transfer data without overloading the network.

You can specify the maximum transfer rate in the Setup dialog box for the management server.



Other Settings

Configure Other Settings

Currency Unit Setting

Set the currency unit to use for asset management.

Currency unit: $

☑ Control network bandwidth from management server

Enter a value between 2 to 1024 (in MB/sec) for the maximum transmission speed of the management server.
The value entered here will be used as the maximum transmission speed when software is distributed by using ITDM-compatible distribution.

Maximum transmission speed: 2 MB/sec

Set an upper limit on the amount of data transferred per second

You can set an upper limit (percentage) on the amount of data transferred per second when packages are distributed to computers. If you set this percentage, computers will adjust the download interval when downloading packages. As a result, network business traffic such as sending or receiving email will be less affected.

You can set the upper limit of the amount of transferred data in **Flow Control** under **Timing of communication with the higher system** under **Basic settings** in the agent configurations. This item is used for maintaining compatibility with the setting in JP1/IT Desktop Management. Do not specify the upper limit of the amount of transferred data, except when you want the same behavior as JP1/IT Desktop Management. If you specify this value, ITDM-compatible distribution might delay so that installation of software or update program and uninstallation of unnecessary software might take a longer time.

2.13.8 Caching distributed packages (ITDM-compatible distribution)

A distributed package is temporarily cached on the distribution target computer. Such a cached package is deleted from the computer only when software installation or file distribution successfully finishes. If such an operation fails, the cached package remains for a specific period of time.

In this case, if you re-execute a task, the package will not be resent and installation or file distribution will be performed using the cached package. Thus, caching distributed packages can reduce the network load.

A package can remain cached for seven days. After the seven days, the cached package will be deleted.

At least 1 GB of free hard disk space is required to cache packages on an agent-installed computer. The maximum capacity of packages that can be cached is 2 GB.

Important note

A package cannot be cached in the following cases:

- The distributed package has been corrupted.
- The free hard disk space on the distribution target computer is less than 1 GB.
- The size of the package is more than 2 GB.

2.13.9 Executing a task when a user is logged off (ITDM-compatible distribution)

You can distribute or install a package even if the user of the distribution target computer is logged off. You can also turn on the distribution target computer, and then turn it off after distribution.

The following table describes which operations can or cannot be executed while a task is executed when the user on an agent-installed computer is logged off.

Operation	Whether the operation can be executed
Distributing a package	Y #
Installation	
Uninstallation	
Turning on and off of the distribution target computer	
Restarting the distribution target computer	
Displaying messages immediately before and after executing a task	N
Postponing download	
Postponing installation	

Legend: Y: Can be executed. N: Cannot be executed.

#: Uninstallation using an EXE file cannot be performed when the user is not logged on.

Related Topics:

- 2.13.10 Power control by the distribution function (ITDM-compatible distribution)

2.13.10 Power control by the distribution function (ITDM-compatible distribution)

If you enable automatic startup of distribution target computers when setting a package distribution task, you will be able to turn on the distribution target computers and distribute the package. This enables you to distribute packages even at night when no one is using computers.

If you want to turn on the distribution target computers for distribution, select the **If target PC is OFF, turn ON power automatically.** check box when you create a task.

Tip

If you select the option **After executing the task, shut down only the computer that started automatically.** while creating a task, and also, if the computer is turned on within one hour after the task was executed, a dialog box appears. The user can select for the computer to be automatically turned off after distribution finishes.

Important note

Distribution target computers must support AMT or Wake on LAN if you want to control the power of the computers.

Important note

If you select the **If target PC is OFF, turn ON power automatically.** check box and the distribution target computer is already on, a dialog box announcing that shutdown or restart will be performed after the package is distributed appears on the target computer's window.

Whether "**If target PC is OFF, turn ON power automatically.**" is selected or not	Whether restart of the computer is necessary or not after distribution	How the computer is started	Timing of starting the computer and executing the task	Computer's behavior#
Selected (**After executing the task, shut down only the computer that started automatically.** is selected.)	Unnecessary	The computer is already running.	--	Downloads the package.
		The user must start the computer.	The computer is started before the task is executed.	Downloads the package, and displays a dialog box announcing shutdown.
			The task is executed, and then the computer is started within an hour.	
			The task is executed, and after more than one hour passes, the computer is started.	Downloads the package.

Whether "**If target PC is OFF, turn ON power automatically.**" is selected or not	Whether restart of the computer is necessary or not after distribution	How the computer is started	Timing of starting the computer and executing the task	Computer's behavior#
Selected (**After executing the task, shut down only the computer that started automatically.** is selected.)	Unnecessary	The computer is automatically started when the task is executed.	The computer is started before the task is executed.	Downloads the package, and displays a dialog box announcing shutdown.
			The task is executed, and then the computer is started within an hour.	
			The task is executed, and after more than one hour passes, the computer is started.	Downloads the package.
		The user must restart the computer.	The computer is started before the task is executed.	Downloads the package, and displays a dialog box announcing shutdown.
			The task is executed, and then the computer is started within an hour.	
			The task is executed, and after more than one hour passes, the computer is started.	Downloads the package.
	Necessary	The computer is already running.	--	Downloads the package, and displays a dialog box announcing restart.
		The user must start the computer.	The computer is started before the task is executed.	Downloads the package, and displays a dialog box announcing shutdown.
			The task is executed, and then the computer is started within an hour.	
			The task is executed, and after more than one hour passes, the computer is started.	Downloads the package.
		The computer is automatically started when the task is executed.	The computer is started before the task is executed.	Downloads the package, and displays a dialog box announcing shutdown.
			The task is executed, and then the computer is started within an hour.	
			The task is executed, and after more than one hour passes, the computer is started.	Downloads the package, and displays a dialog box announcing restart.
		The user must restart the computer.	The computer is started before the task is executed.	Downloads the package, and displays a dialog box announcing shutdown.

Whether "**If target PC is OFF, turn ON power automatically.**" is selected or not	Whether restart of the computer is necessary or not after distribution	How the computer is started	Timing of starting the computer and executing the task	Computer's behavior#
Selected (**After executing the task, shut down only the computer that started automatically.** is selected.)	Necessary	The user must restart the computer.	The task is executed, and then the computer is started within an hour.	Downloads the package, and displays a dialog box announcing shutdown.
			The task is executed, and after more than one hour passes, the computer is started.	Downloads the package.
	--	The computer is already running.	--	Downloads the package, and displays a dialog box announcing shutdown.
		The user must start the computer.		
		The computer is automatically started when the task is executed.		
		The user must restart the computer.		
Selected (**After executing the task, shut down all target computers.** is selected.)	--	The computer is already running.	--	Downloads the package, and displays a dialog box announcing shutdown.
		The user must start the computer.		
		The computer is automatically started when the task is executed.		
		The user must restart the computer.		
Not selected	Unnecessary	The computer is already running.	--	Downloads the package.
		The user must start the computer.	--	
		The user must restart the computer.	--	
	Necessary	The computer is already running.	--	Downloads the package, and displays a dialog box announcing restart.
		The user must start the computer.	--	
		The user must restart the computer.	--	

Legend: --: Not applicable.

#: The behavior might be different if the times on the management server and the distribution target computer are different.

2.13.11 Judging the result of software installation executed by the distribution function (ITDM-compatible distribution)

Whether software installation executed by the distribution function was successful is judged based on the execution result of the installation command set for the package. The following shows how the result is judged for different formats of files registered in the package:

For MSI files

The execution result of installation is judged depending on the value returned by the Windows Installer. The return value is judged as follows:

- ERROR_SUCCESS(0): Normal termination
- ERROR_SUCCESS_REBOOT_INITIATED(1641): Restart is required.
- ERROR_SUCCESS_REBOOT_REQUIRED(3010): Restart is required.
- Other codes: Abnormal termination

For files with other formats

If the installation command set for the package is executed, installation is judged to have finished successfully.

Note that if startup of the installation command fails or if a timeout occurs during startup of the installation command or of the started installer, installation is judged to have failed.

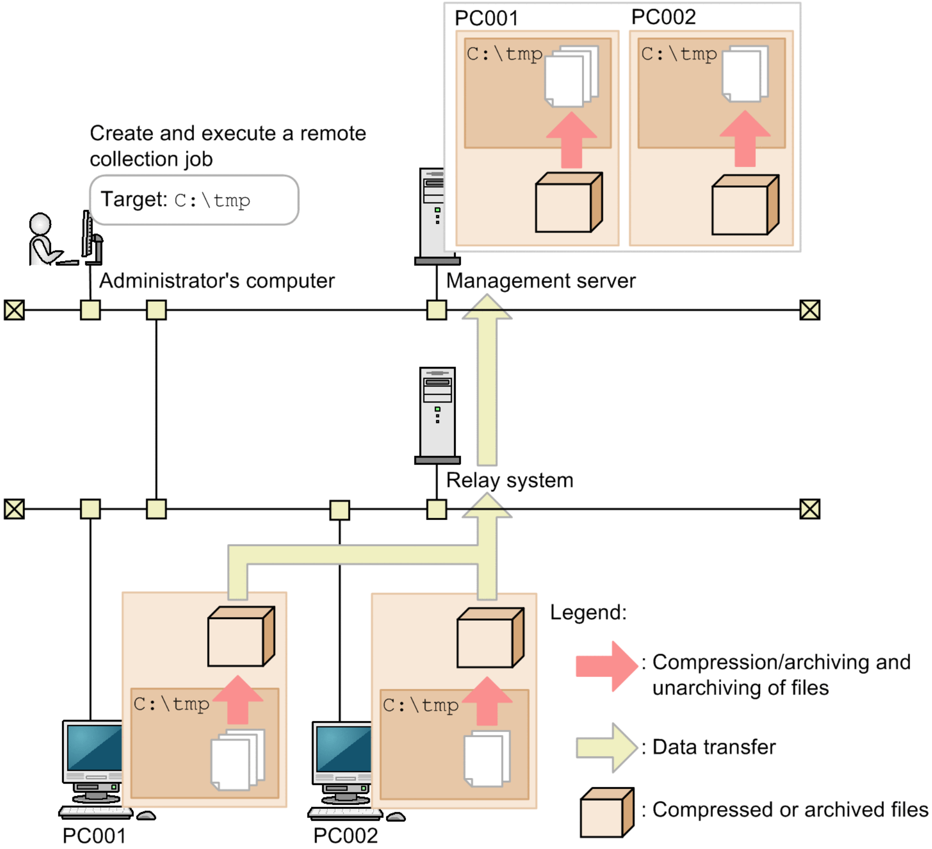
2.14 Collecting files by using Remote Installation Manager

JP1/IT Desktop Management 2 can collect files stored on the managed computers in a single operation. The collected files are stored in the management server. This feature is called *remote collection*. This section provides an overview of file collection. For details and procedures, see *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Distribution Function Administration Guide*.

The remote collection feature can be used for the following operations:

- Collect operation data required for the administrators' job in a single operation.
- Help troubleshooting by collecting and analyzing log information or error information of the software used on the user's computer.

The following figure shows an overview of remote collection:

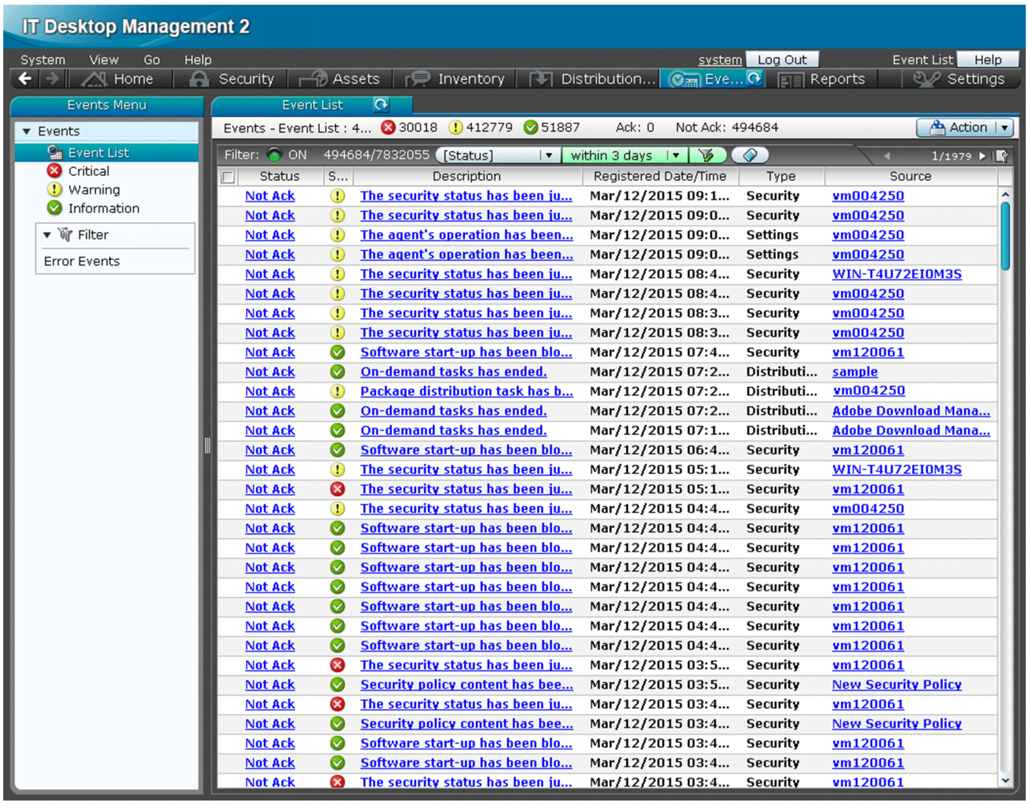


To perform remote collection, create a remote collection job by using Remote Installation Manager. The collected target files are compressed or archived, and then transferred to the management server. To unarchive compressed or archived files, use Unarchiver, which is a component of JP1/IT Desktop Management 2 - Manager.

Providing a relay system can reduce the load on the network caused by remote collection.

2.15 Displaying events

If something occurs that needs immediate countermeasures while JP1/IT Desktop Management 2 is running, it will be output as an event. The results of processing various functions are also output. The administrator can understand what happened while JP1/IT Desktop Management 2 was running by checking events.



□	Status	S...	Description	Registered Date/Time	Type	Source
	Not Ack	!	The security status has been ju...	Mar/12/2015 09:1...	Security	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 09:0...	Security	vm004250
	Not Ack	!	The agent's operation has been...	Mar/12/2015 09:0...	Settings	vm004250
	Not Ack	!	The agent's operation has been...	Mar/12/2015 09:0...	Settings	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:4...	Security	WIN-T4U72EI0M3S
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:4...	Security	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:3...	Security	vm004250
	Not Ack	!	The security status has been ju...	Mar/12/2015 08:3...	Security	vm004250
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 07:4...	Security	vm120061
	Not Ack	✓	On-demand tasks has ended.	Mar/12/2015 07:2...	Distributi...	sample
	Not Ack	!	Package distribution task has b...	Mar/12/2015 07:2...	Distributi...	vm004250
	Not Ack	✓	On-demand tasks has ended.	Mar/12/2015 07:2...	Distributi...	Adobe Download Mana...
	Not Ack	✓	On-demand tasks has ended.	Mar/12/2015 07:1...	Distributi...	Adobe Download Mana...
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 06:4...	Security	vm120061
	Not Ack	!	The security status has been ju...	Mar/12/2015 05:1...	Security	WIN-T4U72EI0M3S
	Not Ack	✗	The security status has been ju...	Mar/12/2015 05:1...	Security	vm120061
	Not Ack	!	The security status has been ju...	Mar/12/2015 04:4...	Security	vm004250
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 04:4...	Security	vm120061
	Not Ack	✗	The security status has been ju...	Mar/12/2015 03:5...	Security	vm120061
	Not Ack	✓	Security policy content has bee...	Mar/12/2015 03:5...	Security	New Security Policy
	Not Ack	✗	The security status has been ju...	Mar/12/2015 03:4...	Security	vm120061
	Not Ack	✓	Security policy content has bee...	Mar/12/2015 03:4...	Security	New Security Policy
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 03:4...	Security	vm120061
	Not Ack	✓	Software start-up has been blo...	Mar/12/2015 03:4...	Security	vm120061
	Not Ack	✗	The security status has been ju...	Mar/12/2015 03:4...	Security	vm120061

2.15.1 Events to be output

An event is output if something occurs (for example, a device is detected, an asset is registered, or judgment based on a security policy is performed) while JP1/IT Desktop Management 2 is running. You can check the output event in Events module.

Events are divided into three severities depending on the details.

✗ (Critical)

Events that require immediate action. Check the details of the event, and take action immediately.

! (Warning)

Events that require a response but not immediately. Check the details of the event, and take action as necessary.

✓ (Information)

Events regarding the results of system processing. No actions are required.

Some events require immediate action. Check `Critical` events first and then `Warning` events. Determine the cause referring to the error message, and take appropriate actions. You can check the total number of events and the number of individual types of events on the **Not Ack Event Summary** panel of the Home module. You can also check the number of unconfirmed events in Summary Reports.

You can set for the administrator to be notified of events when they occur.

Tip

The maximum number of events to be displayed can be calculated by the following formula: *number-of-owned-product-licenses* x 250 + 10,000. If the number of events exceeds this value, older evens will be overwritten. Back up past events to save them.

Related Topics:

- 2.15.2 Event types

2.15.2 Event types

The following are types of events to be output:

Inventory

Events regarding device management, such as addition and deletion of device inventory or software inventory, or addition and deletion of computer accounts.

Security

Events regarding security management, such as change and assignment of security policies, judgment results for security policies, results of actions, or suppression of startup of software.

Assets

Events regarding asset management, such as registration of assets, change of asset statuses, or addition and deletion of software licenses.

Distribution (ITDM-compatible)

Events regarding distribution, such as software installation or uninstallation, or file distribution.

Settings

Events regarding settings, such as device detection, addition of management targets, or agent deployment.

Suspicious Operations

Events regarding suspicious operations, such as detection of emails with attached files, detection of file uploads to Web servers or FTP servers, or detection of files being copied or moved to external media.

Error

Events regarding errors that occurred in various functions.

2.15.3 Event format

Field	Description
Status	This field shows whether the event was checked. Clicking the field changes the status. • Not Ack • Ack
Severity	This field shows the severity of the event. One of the following is displayed: • Critical The event requires immediate action.

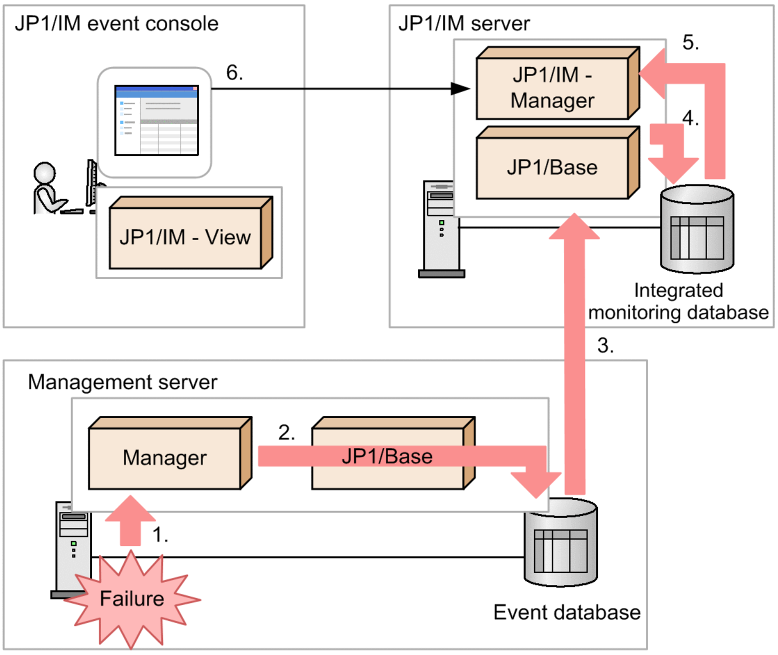
Field	Description
Severity	- Warning The event requires action but not immediately. - Information The event is regarding the results of system processing. No actions are required.
Registered Date/Time	The date and time the event was registered in the management server is displayed.
Type	This field shows the event type. One of the following is displayed: - Inventory - Security - Assets - Distribution (ITDM-compatible) - Settings - Suspicious Operations - Error
Event #	The ID of the event message is displayed.
Source	This field shows information that identifies the target of the event. For example, the device on which the event occurred, or the security policy for which the event occurred is displayed.
Description	Detailed information about the event is displayed.

2.15.4 Checking events on the JP1/IM event console

When JP1/IM is linked, you can monitor error events that occur on managed computers and major events that require judgment by the system administrator on the JP1/IM event console.

JP1/IT Desktop Management 2 can use a JP1/Base function to issue JP1 events when errors occur on managed computers. By linking with JP1/IM, you can use the JP1/IM event console to monitor recent JP1 events or monitor programs of other JP1 products.

The following figure shows the operation flow when an event is displayed on the JP1/IM event console.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager

➡ : Event flow

1. If an error occurs in JP1/IT Desktop Management 2 - Manager, an event is sent to JP1/IT Desktop Management 2 - Manager.

2. The event received at JP1/IT Desktop Management 2 - Manager is registered as a JP1 event in the JP1/Base event database.

3. The JP1 event registered in the event database is forwarded to the JP1/IM server on which JP1/IM - Manager is running.

4. The JP1 event forwarded to the JP1/IM server is registered in the JP1/IM integrated management database.

5. JP1/IM - Manager acquires the JP1 event from the integrated management database.

6. The acquired JP1 event is displayed on the JP1/IM event console.

For events that can be output to the JP1/IM event console, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

2.16 Displaying reports

JP1/IT Desktop Management 2's report function enables you to calculate managed information depending on your purpose. The administrator can refer to reports as necessary for various tasks, or print reports when reporting the current status.

There are the following five types of reports:

- Summary Reports

  You can gain an overview of managed information using a graph or list. You can use these types of reports to check the current status. You can also use them to check future plans to help schedule tasks.

- Security Diagnosis Reports

  You can check the total security assessment and assessments for individual categories in graphs. The assessment levels and points for individual groups are also displayed in lists, so you can check the security status for each group. You can use these types of reports when reporting overall security conditions.

- Security Detail Reports

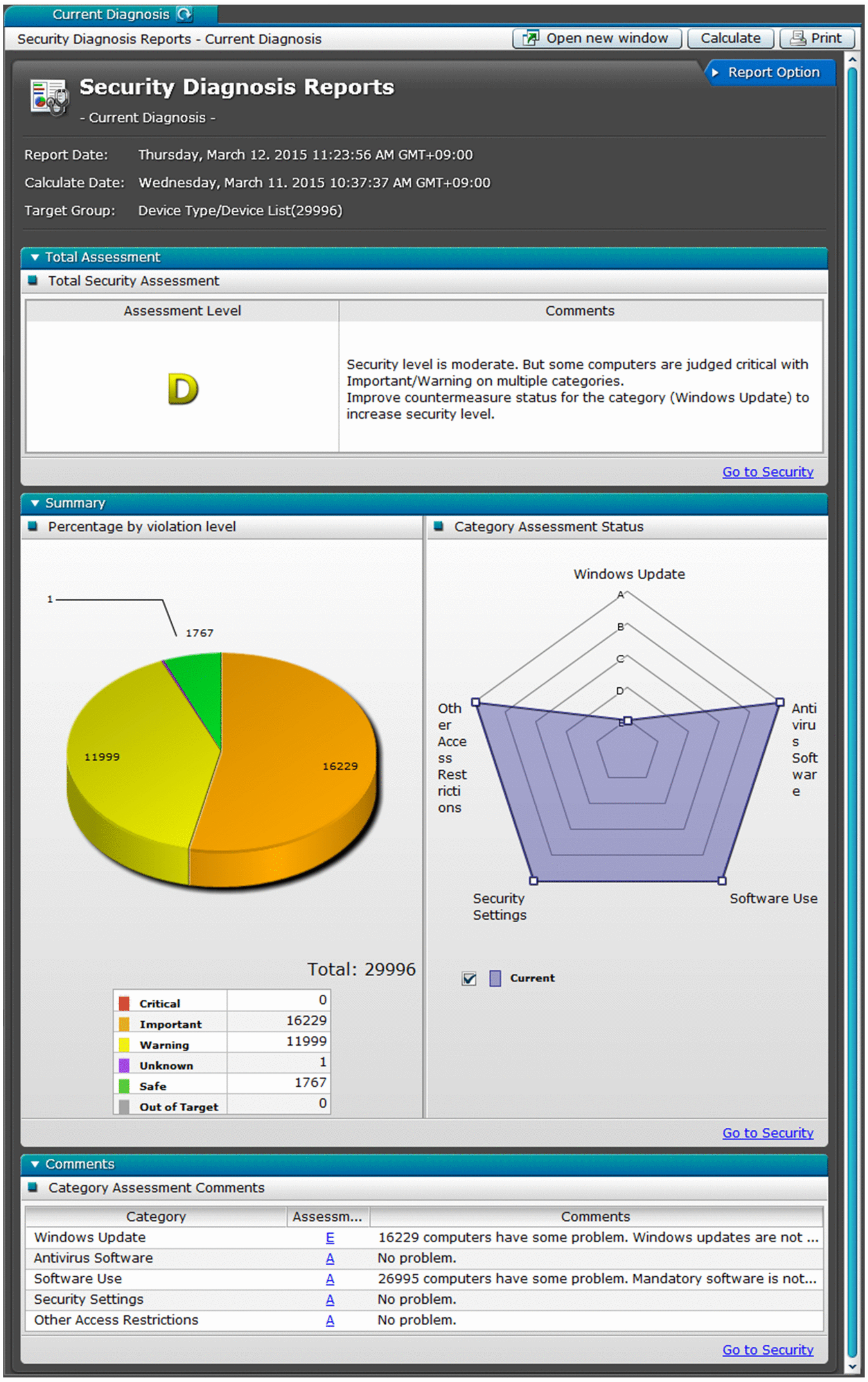
  You can check detailed security status in graphs or lists. You can use these types of reports as a start point for security measures. For example, you can identify problematic computers or check the details of problems.

- Inventory Detail Reports

  You can check the number of managed devices or the power saving settings of individual computers. You can use these types of reports to check the details about the number of devices in a specific department or to understand the status of Green IT efforts.

- Asset Detail Reports

  You can check transitions in the number of managed hardware assets, transitions in contract costs, and the status of software licenses. You can use these types of reports to understand the trends in assets and costs, or to check the usage status of software licenses.



Security Diagnosis Reports

- Current Diagnosis -

Report Date: Thursday, March 12. 2015 11:23:56 AM GMT+09:00

Calculate Date: Wednesday, March 11. 2015 10:37:37 AM GMT+09:00

Target Group: Device Type/Device List(29996)

▼ Total Assessment

Total Security Assessment

Assessment Level	Comments
D	Security level is moderate. But some computers are judged critical with Important/Warning on multiple categories. Improve countermeasure status for the category (Windows Update) to increase security level.

▼ Summary

Percentage by violation level

Category Assessment Status

Total: 29996

🟥 Critical	0
🟧 Important	16229
🟨 Warning	11999
🟪 Unknown	1
🟩 Safe	1767
▨ Out of Target	0

▼ Comments

Category Assessment Comments

Category	Assessm...	Comments
Windows Update	E	16229 computers have some problem. Windows updates are not ...
Antivirus Software	A	No problem.
Software Use	A	26995 computers have some problem. Mandatory software is not...
Security Settings	A	No problem.
Other Access Restrictions	A	No problem.

2.16.1 Viewing reports

In the Reports module, you can view 20 types of reports depending on your purpose. You can print reports or output them to CSV files. The following table lists the report types that can be displayed.

Category	Type	Applicable to a target group#
Summary Reports	Daily Summary	N
	Weekly Summary	N
	Monthly Summary	N

Category	Type	Applicable to a target group#
Security Diagnosis Reports	Current Diagnosis	Y
	Timeframe Diagnosis	Y
Security Detail Reports	Violation Level Status	Y
	Windows Update Status	Y
	Antivirus Software Status	Y
	Mandatory Software Status	Y
	Unauthorized Software Status	Y
	Security Settings Status	Y
	Other Access Restrictions	N
	User Activity	N
Inventory Detail Reports	Device Management Status	Y
	Green IT (Power Saving Settings)	Y
Asset Detail Reports	Hardware Assets	Y
	Hardware Assets Cost	Y
	Software License Cost	Y
	Software (License Violation)	Y
	Software (Surplus License)	Y

Legend: Y: Applicable. N: Not applicable.

#: User-defined groups cannot be the target of a report.

The following is an overview of the above reports and how you can use them:

Summary Reports

Use summary reports to gain an overview of managed information. Check the current status and future plans to schedule future task plans.

Daily Summary

Daily summaries let you check daily information, such as the status of events, the number of assets you plan to change the status of, the status of software licenses, and the status of distribution jobs. The current free database capacity is also displayed. Use these reports to check the current status and future plans, and to help you schedule daily tasks.

Weekly Summary

Weekly summaries let you check weekly information, such as the status of events, the number of assets you plan to change the status of, the status of software licenses, and the status of distribution jobs. For the status of events, transitions in the number of events through a week are displayed. Use these reports to check the current status and future plans, and to help you schedule weekly tasks.

Monthly Summary

Monthly summaries let you check monthly information, such as the status of events, the number of assets you plan to change the status of, the status of software licenses, and the status of distribution jobs. For the status of events, transitions in the number of events through a month are displayed. The results and plans related to the costs for assets are also displayed. Use these reports to check the current status and future plans, and to help you schedule monthly tasks.

Security Diagnosis Reports

Use security diagnosis reports to check the total security assessment level and category assessment levels.

Current Diagnosis

Displays the results of the total assessment of the current security status of computers. Use these reports to check the security status of all managed computers and to consider countermeasures for the items with low security status.

Timeframe Diagnosis

Displays the results of the total assessment of the computers' security status for a specified period. Use these reports to check the transitions of the results of diagnosis and to understand security status trends.

Security Detail Reports

Use security detail reports to check the details of security status.

Violation Level Status

Displays the status of violation levels and the security status of individual groups. Use these reports to check the violation levels of computers and to consider and strengthen security measures.

Windows Update Status

Displays the number of computers on which Windows updates set in the security policy have not been installed and the status of individual groups. Use these reports to target for updating all computers on which relevant Windows updates have not been installed.

Antivirus Software Status

Displays the number of computers to which antivirus software has not been applied and the status of individual groups. Use these reports to help check and update antivirus software.

Mandatory Software Status

Displays the number of computers on which the mandatory software programs set in the security policy have not been installed and the status of individual groups. Use these reports to target installation requests for mandatory software.

Unauthorized Software Status

Displays the number of computers on which the prohibited software programs set in the security policy have been installed and the status of individual groups. Use these reports to target uninstallation requests for prohibited software.

Security Settings Status

Displays the number of computers on which illegal accesses might occur, the number of computers that have problems related to user-defined security settings, and the status of individual groups. Use these reports to check which security measures are problematic and to help enforce appropriate security measures on individual computers.

Other Access Restrictions

Displays information about computers on which printing is restricted, startup of software is restricted, or use of devices is restricted. The computers are displayed in the order of highest to lowest number of restrictions. Use these reports to check for users who have many restrictions applied to them, and to give them advice.

User Activity

Displays the printing activity of computers. Also displays which computers have used USB devices. The computers are listed in the order of the number of uses. Use these reports to investigate the computers from which information might have been illegally moved by printing or by the use of USB devices.

Inventory Detail Reports

Use inventory detail reports to check the number of managed devices and the status of the power saving settings on individual computers.

Device Management Status

Displays the number of managed devices and the increase and decrease of the number of devices. Use these reports to understand the increase and decrease of devices for each OS or to check the details of the devices in a specific department.

Green IT (Power Saving Settings)

Based on the status of the power saving settings on the managed computers, Green IT reports display the difference from the ideal energy consumption. Use these reports to reduce the power consumption of computers or to understand the status of the Green IT efforts.

Asset Detail Reports

Use asset detail reports to check the transitions of the number of managed hardware assets, the transitions of contract costs, and the status of software licenses.

Hardware Assets

Displays the transitions of the number of managed hardware assets for individual device types. Use these reports to understand trends in the transitions of the number of hardware assets through a year or to check the percentage of each hardware asset device type.

Hardware Assets Cost

Displays the transitions of the costs for hardware assets through a year. Use these reports to understand the trends in the transitions of contract costs through a year or to judge whether contract costs are appropriate.

Software License Cost

Displays the transitions of the costs for software licenses through a year. Use these reports to understand the trends in the transitions of contract costs through a year or to judge whether contract costs are appropriate.

Software (License Violation)

Displays information about the software programs for which there are insufficient licenses in the order of the number of insufficient licenses. The software programs listed in these of reports might be violating licenses. Use these reports to check the usage statuses of software licenses and to consider countermeasures, such as purchasing additional licenses.

Software (Surplus License)

Displays information about unused software licenses in the order of the number of excess licenses. Use these reports to confirm license requirements before purchasing software licenses.

2.16.2 Calculation of the assessment level in Security Diagnosis Reports

Security Diagnosis Reports display the results of calculating, analyzing, and diagnosing the outcome of judging the security status of devices. In addition to the total security assessment level, it displays the assessment levels for individual categories (such as the Antivirus Software status and the Security Settings status) and the transitions of assessment levels.

Security Diagnosis Reports display assessments in five levels (A to E). Level A is the safest, and Level E is the most unsafe. An assessment level is determined by the points for individual devices, which are based on the security judgment results. If all security judgment items are in `Safe` status for a device, the device will have 100 points. If some judgment items are not in `Safe` status, points will be deducted based on the judgment results for the security judgment items. Even if the average number of points is high, the assessment level will become low if one or more computers are in `Critical` status during the judgment period.

In Security Diagnosis Reports, an assessment level displayed in the **Category Assessment Status** area will become low if one or more computers are in Critical status, to let you consider countermeasures for items with low security status. On the other hand, an assessment level displayed in the **Assessment and # of Target Trend** is determined based on the average number of points for each category, to let you understand security status trends. For this reason, the assessment levels might be different between **Category Assessment Status** and **Assessment and # of Target Trend**.

The following table lists the points that are to be deducted for individual violation levels.

Violation level	Deduction points
Critical	25
Important	16
Warning	6
Safe	0

Note that points are not deducted when a judgment error occurs, judgment items are missing, or there is not enough information for security judgment.

The following table lists the criteria for the total security assessment level.

Assessment level	Average points	Minimum points	Violation level in the judgment results	Category assessment level
A	90 to 100	90 to 100	No Critical and Important levels	Level A only
B	80 to 89	80 to 89	No Critical levels	Level A and B only
C	65 to 79	50 to 79	No Critical levels	Level A to D only
D	50 to 64	Not defined.	Not defined.	Not defined.
E	0 to 49	Not defined.	Not defined.	Not defined.

For example, assume that the average number of points is 95 (which corresponds to level A), the minimum number of points is 87 (which corresponds to level B), the violation level in the judgment results is "No Critical and Important levels" (which corresponds to level A), and the category assessment level is "Level A and B only" (which corresponds to level B). In this case, the total security assessment level becomes level B. Thus, the lowest assessment level among the above four items ("Average points", "Minimum points", "Violation level in the judgment results", and "Category assessment level") will become the total security assessment level.

The following table lists the criteria of the category assessment levels.

Assessment level	Average points	Minimum points	Violation level in the judgment results
A	90 to 100	90 to 100	No Critical and Important levels
B	80 to 89	80 to 89	No Critical levels
C	65 to 79	50 to 79	No Critical levels
D	50 to 64	Not defined.	Not defined.
E	0 to 49	Not defined.	Not defined.

For example, assume that the average number of points is 95 (which corresponds to level A), the minimum number of points is 87 (which corresponds to level B), and the violation level in the judgment results is "No Critical and Important levels" (which corresponds to level A). In this case, the category assessment level becomes level B. Thus, the lowest assessment level among the above three items ("Average points", "Minimum points", and "Violation level in the judgment results") will become the category assessment level.

2.16.3 Criteria for judging whether Green IT has been applied

You can use the **Green IT (Power Saving Settings)** report to check whether the power saving setting on a computer has been applied. Whether the power saving setting on a computer is applied is judged based on comparison of the power saving setting collected from the computer and the sample PC setting. The following table describes the relationship between the statuses of the power saving settings on a computer and the judgment results.

Status	Judgment
Applicable	*power-saving-setting-on-a-computer* ≤ *judgment-reference-value* (Excluding when the power saving setting on a computer is `None`)
Not Applicable	*power-saving-setting-on-a-computer* > *judgment-reference-value* or the power saving settings on a computer is `None`.
Unknown	The judgment reference value for the power saving setting has been set, but the power saving setting on a computer cannot be acquired.
Out of Target	The judgment reference value has not been set.

2.16.4 Calculation of ideal energy consumption (theoretical value) and energy consumption (theoretical value)

The ideal energy consumption (theoretical value) is calculated based on the reference values for power saving that are set in the **Set Green IT Property** dialog box. The energy consumption (theoretical value) is calculated based on the settings on individual computers.

For the operating time of a computer, the values for the sample settings in the **Set Green IT Property** dialog box are used for both the ideal energy consumption (theoretical value) and energy consumption (theoretical value).

The power consumption per hour is calculated as the total value of the combination of power saving settings shown in the following table.

No.	Status of the monitor	Status of the computer	Power consumption per hour (W)
1	Usual operation# (30)	Usual operation# (39)	69
2		Turn Off Hard Disks (35)	65
3		System Standby (3)	33
4		System Hibernate (0)	30
5	Turn Off Monitor (0)	Usual operation (39)	39
6		Turn Off Hard Disks (35)	35
7		System Standby (3)	3
8		System Hibernate (0)	0

Note: In the above table, the numbers enclosed by parentheses indicate power consumption per hour (unit: W). Note that a computer can only be in one of the above statuses at a time. If multiple patterns of power saving settings are operating at the same time, the power saving settings with lower power consumption is selected.

#: Power saving settings are not operating.

Calculation of ideal energy consumption (theoretical value)

The ideal energy consumption (theoretical value) is the value when the judgment criteria for power saving settings that is set in the **Set Green IT Property** dialog box is applied to the computers and the computers run as defined in the sample settings.

The following describes how to calculate the ideal energy consumption (theoretical value) with the following conditions:

- Number of managed computers: 100
- Reference values for the power saving settings in the **Set Green IT Property** dialog box (default):
    - Turn Off Monitor (AC): Within 5 minutes
    - Hard Disk Turn Off Time (AC): Within 30 minutes
    - System Standby (AC): Within 1 hour
- Sample settings in the **Set Green IT Property** dialog box (default):
    - Operating time for a computer (per day): 8 hours
    - Time a computer is not operated: 60 minutes x 1 and 10 minutes x 6

The ideal energy consumption (theoretical value) is calculated for the time computers are operated and for the time computers are not operated separately. These calculations are based on the values in the above table.

Time a computer is operated

According to the sample settings, the time a computer is not operated (60 minutes x 1 + 10 minutes x 6) is excluded from the operating time per day (8 hours). In this example, the operating time becomes as follows:

8 hours - 2 hours = 6 hours

When a computer is operated, power saving settings are not operating. So, No.1 in the above table is applied. The calculation formula is as follows:

69 x 6 hours = 414 (Wh)

Time a computer is not operated

There are two types ("60 minutes x 1" and "10 minutes x 6") of energy consumption according to the sample settings.

Energy consumption for "60 minutes x 1"

For **Monitor Turn Off Time**, 5 minutes is set. So, the status of No.1 in the above table continues for 5 minutes, and then the monitor is turned off. For **Hard Disk Turn Off Time**, 30 minutes is set. So, the status of No. 5 in the above table continues for 25 minutes, and then the power of the hard disk is turned off. For **System Standby**, 1 hour is set. So, the remaining 30 minutes will be in the status of No.6 in the above table. Thus, the calculation formula is as follows:

(69 x 5 minutes / 60 minutes) + (39 x 25 minutes / 60 minutes) + (35 x 30minutes / 60 minutes) = 39.5 (Wh)

Energy consumption for "10 minutes x 6"

This type of energy consumption is also calculated in the same way as the above type of energy consumption (60 minutes x 1). The status of No.1 in the above table continues for 5 minutes, and then the status of No.5 in the above table continues for 5 minutes. These status changes repeat 6 times. Thus, the calculation formula is as follows:

{(69 x minutes / 60 minutes) + (39 x 5 minutes / 60 minutes)} x 6 = 54 (Wh)

Calculation formula for ideal energy consumption (theoretical value)

The ideal energy consumption (theoretical value) results from multiplying the total energy consumption for the time a computer is operated and for the time a computer is not operated, by the number of computers. Thus, the calculation formula is as follows:

(414 + 39.5 + 54) x 100 = 50,750 (Wh)

Calculation of energy consumption (theoretical value)

The energy consumption (theoretical value) is the value when computers operate following the power saving settings on individual computers and the sample settings (for computers' usage).

The energy consumption (theoretical value) can be calculated in the same way as the ideal energy consumption (theoretical value). The following shows the number of computers, an example setting, and calculation of energy consumption (theoretical value) for that setting:

- Number of managed computers: 100
- Computer settings:
  - Turn Off Monitor (AC): 10 minutes
  - Turn Off Hard Disks (AC): 30 minutes
  - System Standby (AC): 90 minutes

  This example assumes that all computers have the same settings.
- Sample settings in the **Set Green IT Property** dialog box (Example)
  - Operating time for a computer (per day): 8 hours
  - Time a computer is not operated: 60 minutes x 1 and 10 minutes x 6

Calculation formula for energy consumption (theoretical value)

Energy consumption per computer (theoretical value): (69 x 6 hours) + (69 x 10 minutes / 60 minutes) + (39 x 20 minutes / 60 minutes) + (35 x 60 minutes / 60 minutes) +{(69 x 10 minutes / 60) x 6} = 542.5 (Wh)

Energy consumption for 100 computers (theoretical value): 542.5 x 100 = 54,250 (Wh)

Thus, energy consumption values for individual computers are calculated based on the settings, and totaled as the energy consumption (theoretical value). Note that the energy consumption (theoretical value) is calculated based on only the computers whose power saving setting information can be acquired.

2.16.5 Calculation schedules for reports

When you display reports, the results of calculations executed according to the calculation schedule or the current calculation results are displayed. Calculation schedules differ depending on the report type. Also, the duration for calculating a report and for storing data differ depending on the report type. The following table lists the data calculation schedule, report duration, and storage duration for individual reports.

Reports		Calculation target	Schedule	Report duration	Storage duration	Whether a schedule can be set
Summary Reports	Daily Summary	All information items	Every day at 6:00	For the previous day	For 7 days	N

Reports			Calculation target	Schedule	Report duration	Storage duration	Whether a schedule can be set
Summary Reports	Weekly Summary		All information items	On the start day of every week after calculation for Daily Summary finishes	For the previous week	For 5 weeks	Y
	Monthly Summary			On the start day of every month after calculation for Daily Summary finishes	For the previous month	For 3 months	Y
Security Diagnosis Reports	Current Diagnosis		Devices (by group or by security policy)	On-demand[#1]	At the execution time	Only the most recent	N
				Every day after the regular judgment finishes (at 0:00 by default)	At the calculation time		Y[#2]
	Timeframe Diagnosis	Weekly	Devices (by group or by security policy)	Every day at 1:00	For this week (daily)	For 6 weeks	Y
		Monthly			For this month (daily)	For 3 months	Y
		Quarterly		On the start day of every month (after daily calculation finishes)	For this quarter (monthly)	For 5 years[#3]	Y
		Half Yearly			For this half-year (monthly)	For 5 years[#3]	Y
		Yearly			For this year (monthly)	For 5 years[#3]	Y
Security Detail Reports	Violation Level Status		Devices (by group or by security policy)	On-demand[#1]	At the execution time	Only the most recent	N
				Every day at 1:10	At the calculation time		N
				On the start day of every month at 0:30	For the previous month	For 1 year	Y
	• Windows Update Status • Antivirus Software Status		Devices (by group or by security policy)	On-demand[#1]	At the execution time	Only the most recent	N

Reports		Calculation target	Schedule	Report duration	Storage duration	Whether a schedule can be set
Security Detail Reports	• Mandatory Software Status • Unauthorized Software Status • Security Settings Status	Devices (by group or by security policy)	Every day at 1:10	At the calculation time	Only the most recent	N
	Other Access Restrictions	Events (by device or by user account)	When an event occurs	At the calculation time	--	N
	User Activity					
Inventory Detail Reports	Device Management Status	Devices (by group)	On-demand[#1]	At the execution time	Only the most recent	N
			Everyday at 0:40	At the calculation time		N
			On the start day of every month at 0:30	For the previous month	For 1 year	Y
	Green IT (Power Saving Settings)	Devices (by group)	On-demand[#1]	At the execution time	Only the most recent	N
			Every day at 0:40	At the calculation time		N
			On the start day of every month at 0:30	For the previous month	For 1 year	Y
Asset Detail Reports	Hardware Assets	Hardware assets (by group)	On-demand[#1]	At the execution time	Only the most recent	N
			Every day at 0:10	At the calculation time		N
			On the start day of every month at 0:00	For the previous month	For 5 years[#3]	Y
	Hardware Assets Cost	Contract (by contract)	On the start day of every month at 0:00	For the previous month	For 5 years[#3]	Y
	Software License Cost					
	Software (License Violation)	Managed software (by managed software program)	When a report is displayed	At the time a report is displayed	--	N
	Software (Surplus License)					

Legend: Y: Can be set. N: Cannot be set. --: Not applicable.

#1: The current data is calculated if you click the **Calculate** button displayed in a report.

#2: The calculation schedule is changed if you set the schedule in the **Security Schedule** view (under **Security**) of the Settings module.

#3: You can set this value in the **Duration and Start Date** view (under **Reports**) of the Settings module.

Important note

When there is data that has already been calculated, if you change the setting of the start date, a date redundantly calculated for multiple periods or a date that is not calculated for any period might occur. Therefore, after you change the start date, only use the data calculated after the change.

2.16.6 Printing reports

The reports displayed in the Reports module can be printed in A4 size almost as displayed. However, buttons and scroll bars that are not directly related to the contents of the report are not printed. A report with many display items such as Summary Reports is printed in several pages depending on the display contents. Also, a page number is printed at the bottom center of each page.

2.16.7 Deleting reports

The data in the following reports increases through the period of using the reports because calculated data is accumulated. Deleting unnecessary reports can reduce disk consumption.

- Security Diagnosis Reports - Monthly assessment
- Asset Detail Reports - Hardware Assets
- Asset Detail Reports - Hardware Assets Cost
- Asset Detail Reports - Software License Cost

You can delete a report by changing its storage duration. If you shorten the storage duration of a report so that the storage duration has expired, the report will be deleted at the next regular calculation time (once a day). For example, if you change the storage duration of reports from two years to one year, the reports created one year and three month ago will be deleted at the next regular calculation time.

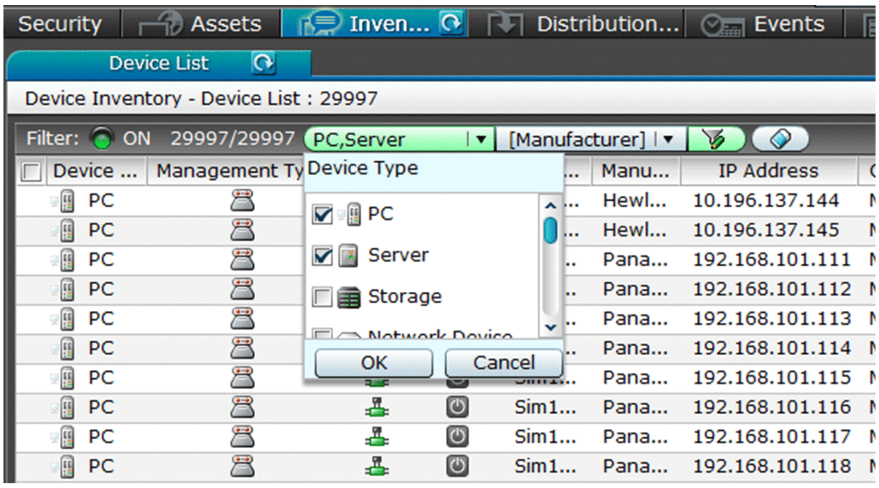
You can set the storage duration of reports in the **Duration and Start Date** view (under **Reports**) of the Settings module. The default storage duration is five years.

You can use filters to narrow the conditions for the information to be displayed.

There are two types of filters: *simple filter* and *detailed filter*.

simple filter

From the provided filter items, you can select the conditions for filtering information. From the pull-down menu displayed above the list, you can select the conditions (filter items) for information to be displayed. Thus, you can quickly filter information.



Device Inventory - Device List : 29997

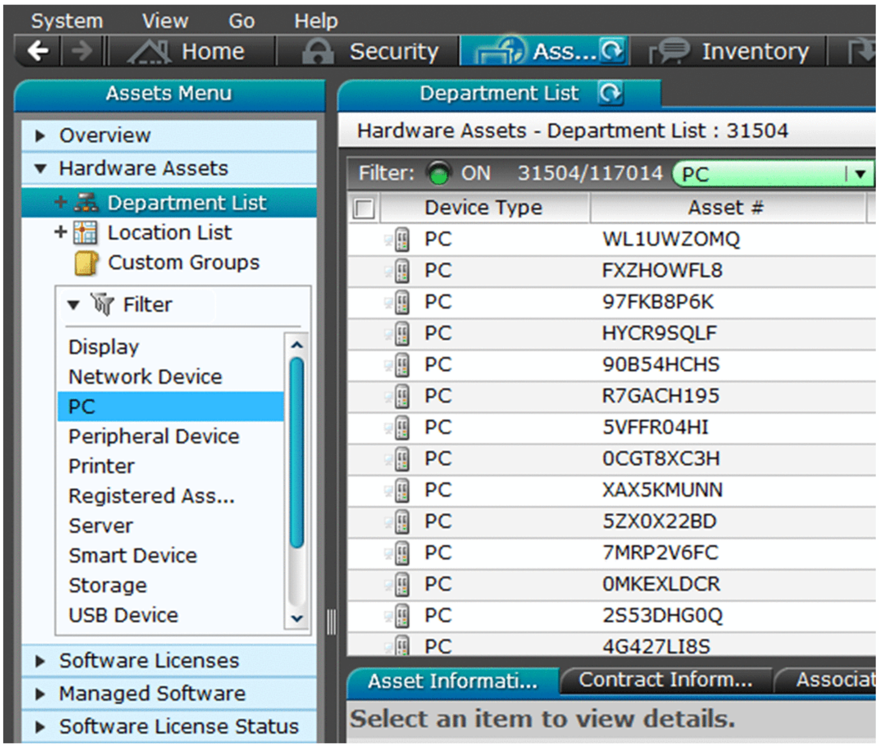
Filter: ● ON 29997/29997 PC,Server [Manufacturer]

Device ...	Manu...	IP Address
PC	Hewl...	10.196.137.144
PC	Hewl...	10.196.137.145
PC	Pana...	192.168.101.111
PC	Pana...	192.168.101.112
PC	Pana...	192.168.101.113
PC	Pana...	192.168.101.114
PC	Pana...	192.168.101.115
PC	Pana...	192.168.101.116
PC	Pana...	192.168.101.117
PC	Pana...	192.168.101.118

detailed filter

You can set a combination of multiple detailed conditions. Use detailed filters when you cannot filter the target information as desired by using simple filters.

Detailed filters include the filter items provided by JP1/IT Desktop Management 2. If you select a filter displayed under **Filter** in the menu area, you can apply the filter to the displayed view.



Hardware Assets - Department List : 31504

Filter: ● ON 31504/117014 PC

Device Type	Asset #
PC	WL1UWZOMQ
PC	FXZHOWFL8
PC	97FKB8P6K
PC	HYCR9SQLF
PC	90B54HCHS
PC	R7GACH195
PC	5VFFR04HI
PC	0CGT8XC3H
PC	XAX5KMUNN
PC	5ZX0X22BD
PC	7MRP2V6FC
PC	0MKEXLDCR
PC	2S53DHG0Q
PC	4G427LI8S

Select an item to view details.

In the above figure, the **PC** filter is applied to the list displayed in the **Department List** view (under **Hardware Assets**) of the Assets module. The selected filter and the view it is applied to are shown in blue in the menu area.

You can also add a detailed filter that specifies optional conditions. Place the mouse cursor on **Filter** in the menu area, and then click ➕ . If you enter a filter name, the **Edit Filter Conditions** dialog box is displayed, and you will be able to set various conditions depending on your purpose. For example, to filter the computers to be replaced, you can set the conditions as follows: set 3 years ago or older for **Registered Date/Time**, and Windows 7 for **OS**.

> **Tip**
>
> Save frequently used filter conditions to avoid the task of specifying conditions every time. You can select saved filter conditions in the menu area to apply them to a list.

> **Tip**
>
> If you use **All Hardware Asset Items** when you set filter conditions for asset information, you can display asset information that includes any character string you specify.

Note that you can also display the **Edit Filter Conditions** dialog box by clicking the ▽ button.

If you apply filters, **Filter: OFF** displayed above the list changes to **Filter: ON**, the green indicator lights, and the number of filtered computers (in the above figure) is displayed.

To cancel the filter, click the ◇ button. The display changes to **Filter: OFF** and the conditions are cancelled.

> **Tip**
>
> You can also export or import detailed filter conditions by executing commands.

Related Topics:

- 2.17.1 Filters provided by JP1/IT Desktop Management 2

2.17.1 Filters provided by JP1/IT Desktop Management 2

The following describes the conditions set for the filters provided by JP1/IT Desktop Management 2.

Filters in the Security module

The following table describes the filter conditions displayed in the menu area of the Security module.

Filters in the **Computer Security Status** view

Filter name	Conditions
Violation Level	*violation-level*, **contains neither of**, and **Out of target**, **Safe**

Filters in the **Windows Update** view

Filter name	Conditions
Recent Updates (last 30 days)	• **Release Date**, **or later**, **month(s)**, **1**, and **before** • **Release Date**, **or before**, and **Today**

Filters in the Assets module

The following table describes the filter conditions displayed in the menu area of the Assets module.

Filters in the **Hardware Assets** view

Filter name	Conditions
Unconfirmed Asset	**Asset Status**, **contains any of** , and **Unconfirmed**
PC	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **PC**
Server	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Server**
Storage	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Storage**
Peripheral Device	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Peripheral Device**
USB Device	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **USB Device**
Network Device	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Network Device**
Printer	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Printer**
Smart Device	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Smart Device**
Display	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Device Type**, **contains any of**, and **Display**
Registered Assets (last 6 months)	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Registered Date/Time**, **or after**, **month**, **6**, and **before** • **Registered Date/Time**, **or before**, and **Today**
Untracked Assets (last 6 months)	• **Asset Status**, **contains neither of**, and **Unconfirmed**, **Disposed** • **Tracked Date**, **before**, **month**, **6**, and **before**
Unconfirmed USB Device	• **Asset Status**, **contains any of**, and **Unconfirmed** • **Device Type**, **contains any of**, and **USB Device**

Filters in the **Software Licenses** view

Filter name	Conditions
Registered Licenses (last 6 months)	• **License Status**, **contains neither of** , and **Disposed** • **Registered Date/Time**, **or after**, **month**, **6**, and **before** • **Registered Date/Time**, **or before**, and **Today**
Untracked Licenses (last 6 months)	• **License Status**, **contains neither of** , and **Disposed** • **Tracked Date**, **before**, **month**, **6**, and **before**

Filters in the **Managed Software** view

Filter name	Conditions
License Violation Software	• **License Type**, **contains any of** , and **Install License** • **Remaining License Total** , **<**, and **0**

Filters in the **Software License Status** view

Filter name	Conditions
License Violation Software	• **License Type**, **contains any of** , and **Install License** • **Remaining License Total** , <, and **0**

Filters in the **Contract** view

Filter name	Conditions
Hardware Asset	**Hardware Asset**, >, and **0**
Software License	**Software License**, >, and **0**
Expired Contract	• **Contract Status**, **contains neither of** , and **Canceled**, **Expired** • **Contract End Date**, **before**, and **Today**
Expired Contracts (next 1 month)	• **Contract Status**, **contains neither of** , and **Canceled**, **Expired** • **Contract End Date**, **or before**, **month**, **1**, and **after** • **Contract End Date**, **or after**, and **Today**

Filters in the Device module

The following table describes the filter conditions displayed in the menu area of the Device module.

Filters in the **Device Inventory** view

Filter name	Conditions
New Devices (last 7 days)	• **Registered Date/Time**, **or after**, **week**, **1**, and **before** • **Registered Date/Time**, **or before**, and **Today**
Not Confirmed Devices (last 30 days)	**Last Alive Confirmation Date/Time**, **before**, **month**, **1**, and **before**

Filters in the **Software Inventory** view

Filter name	Conditions
New Software (last 7 days)	• **Registered Date/Time**, **or after**, **week**, **1**, and **before** • **Registered Date/Time**, **or before**, and **Today**

Filters in the Distribution (ITDM-compatible) module

The following table describes the filter conditions displayed in the menu area of the Distribution (ITDM-compatible) module.

Filters in the **Packages** view

Filter name	Conditions
Removable Packages	**Total Tasks**, =, and **0**

Filters in the **Tasks** view

Filter name	Conditions
Failed Tasks	**Failed Computers**, >, and **0**

Filters in the Events module

The following table describes the filter conditions displayed in the menu area of the Events module.

Filter name	Conditions
Error Events	**Type**, **contains any of** , and **Error**

Filters in the Network Filter Settings view

The following table describes the filter conditions displayed in the **Network Filter Settings** view of the Settings module.

Filter name	Conditions
Reviewed Devices	**Reviewed**, **is**, and **Reviewed**

Related Topics:

- 2.17 Using filters

2.18 Operations in a cluster system

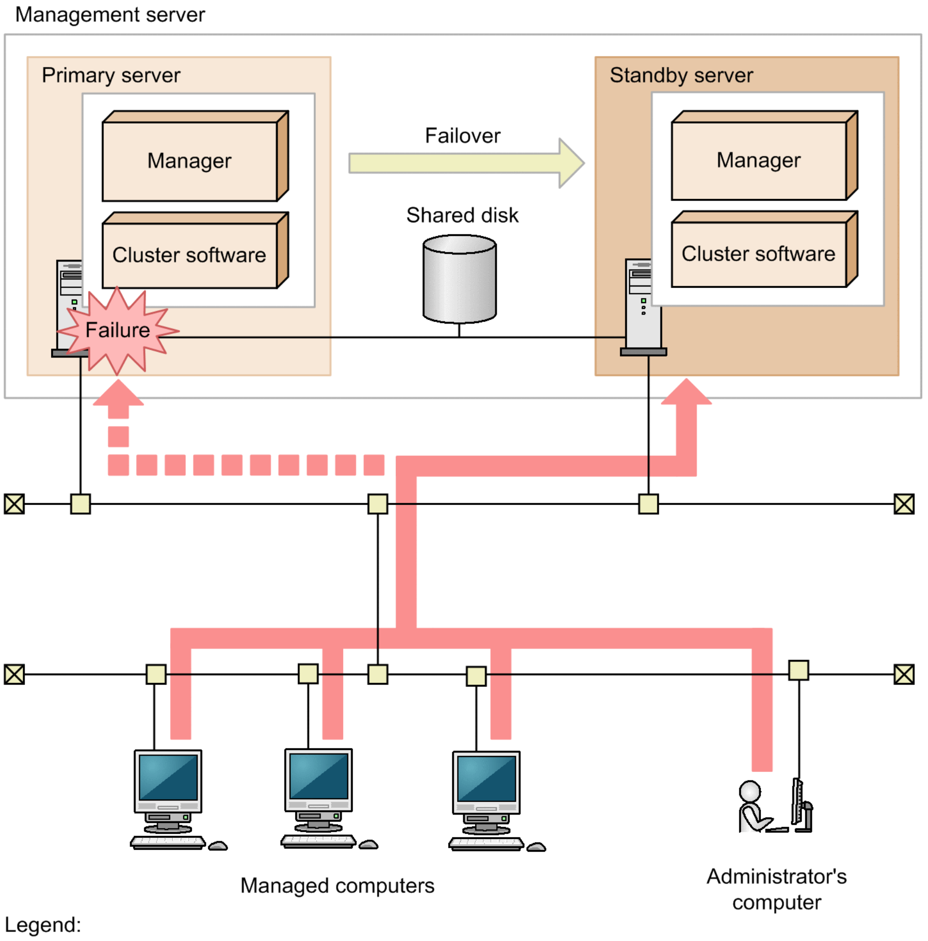
JP1/IT Desktop Management 2 supports operations in a cluster system.

In a cluster system, when a problem occurs in the operating server, operations are automatically switched to a backup server. A cluster system can realize stable operations, where the entire system does not stop. By using a cluster system, you can continue using the services provided by JP1/IT Desktop Management 2 without being affected by problems.

JP1/IT Desktop Management 2 can introduce a cluster system using Windows Server Failover Cluster, and supports an active-standby configuration. An active-standby configuration consists of two servers: one is set as the primary node (main server) and the other is set as the secondary node (backup server).

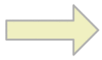
The behavior of switching operations from the main server to the backup server is called *failover*. After a failover occurs, operations are performed on the backup server. The main server can then be restored to recover a normal operation environment.

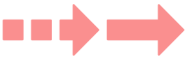
The following figure shows an overview of a cluster system where JP1/IT Desktop Management 2 is installed.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager


: Failover flow


: Access flow

When a cluster system is used, a logical host name or a logical IP address is set for the management server. Managed computers connect to this host name or IP address.

For the logical host name or logical IP address, the host name or IP address of the management server is associated. Even if the associated host name or IP address is changed, the logical host name or logical IP address will not change. Therefore, even after a failover occurs, operations can continue without the need of changing the setting of the connection target on computers.

Important note

Only the management server supports a cluster system. You cannot establish a cluster system with network monitors.

2.19 Managing the database

JP1/IT Desktop Management 2 stores various kinds of information managed by JP1/IT Desktop Management 2 in a special database created on the management server.

You must regularly maintain the database by creating a backup in preparation for problems or by re-organizing it to increase performance.

To maintain the database, use the database manager provided by JP1/IT Desktop Management 2.

The following are the database manager functions:

Backup

This function creates a backup of the database. If a disk failure should occur, information in the database might be erased or corrupted. Therefore, regularly make backups when the database is operating.

You can also back up the database by executing the `exportdb` command.

Restore

This function restores the database from a backup created by the backup function or by the `exportdb` command. If an error occurs in the database, you can use the backup to restore the database to the status as of the backup.

You can also restore the database by executing the `importdb` command.

Reorganize

Fragmentation of database area might occur if the database has been used for a long time. This might cause problems, such as slowdown of access speed. To prevent such problems, JP1/IT Desktop Management 2 can reorganize the database. Reorganizing the database can be done while the data remains stored, and can help to make performance more efficient. We recommend that you reorganize the database before the usage rate of the database reaches 80%. You can check the usage rate of the database in the database manager.

You can also reorganize the database by executing the `reorgdb` command.

In addition, you can use the JP1/IT Desktop Management 2 setup to upgrade or initialize the database, and to change the storage folder.

2.19.1 Data output during backup

When the database is backed up, in addition to the management information stored in the database, backup files for other management data stored in the database folder will be created. The following table describes the files created during backup.

File name	Description
jdnexport.info	Backup information is registered in this file.
jdnexportdata.bak	Management data other than that in the database is archived in this backup file.
table.*table-name*.exp.bin	Tables in the database are backed up in this file.

2.20 Using commands

JP1/IT Desktop Management 2 provides commands to execute various functions. By using these commands in combination with Windows task scheduler or other functions, you can automatically perform operations, such as scheduled backups or output of the latest information.

For major commands such as starting or stopping a service, backing up or restoring a database, and acquiring information for troubleshooting, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*,

For the commands related to distribution utilizing Remote Installation Manager, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Distribution Function Administration Guide*.

For the commands related to asset management utilizing Asset Console, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Planning and Configuration Guide*.

2.21 Operations on users' computers

When a computer is managed online and the user's operation is required, the agent displays a balloon tip or a dialog box. For example, an agent can direct the user who violated a security policy to take an appropriate countermeasure, or let the user select the timing of downloading software. The user must take an appropriate action as indicated in the displayed message.

Users' entry of user information

When custom fields have been set, a dialog box is displayed on each computer to let the user enter user information. This can reduce administrator's tasks because information entered in dialog boxes by users is applied to device inventory. For details about entering user information, see 2.21.1 Users' entry of user information. The display of a user information entry window can be specified in the **User notification settings** view for the agent configuration. For details about the agent configuration, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*. For details about how to specify the agent configuration, see the *JP1/IT Desktop Management 2 Online Help*.

Display of balloon tips on users' computers

If there is information that users need, a balloon tip is displayed above a taskbar icon on each computer. The balloon tip can guide the operators to do what is required on their computers. For details about balloon tips, see 2.21.2 Display of balloon tips on users' computers. The display of balloon tips can be specified in the **User notification settings** view for the agent configuration. For details about the agent configuration, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*. For details about how to specify the agent configuration, see the *JP1/IT Desktop Management 2 Online Help*.

Behavior when users are directed to turn off the computers

After the management server directs shutting down of computers, a dialog box confirming the shutdown operation is displayed on each target computer. Each user can select to shut down the computer immediately or to manually shut down the computer later. For details, see 2.21.3 Behavior when users are directed to turn off computers.

Behavior when users are directed to restart the computers

After the management server directs restart of computers, a dialog box confirming the restart operation is displayed on each target computer. Each user can select to restart the computer immediately or to manually restart the computer later. For details, see 2.21.4 Behavior when users are directed to restart computers.

Behavior when distribution is performed on users' computers

A balloon tip is displayed above a taskbar icon while software is being downloaded. Users can click the balloon tip to suspend the download.

When installation of a downloaded software program starts, a pre-installation message is displayed to users (if one has been set). Each user can select whether to install the software immediately or to install it later.

For details, see 2.21.5 Behavior when distribution is performed on users' computers. The display of balloon tips can be specified in the **User notification settings** view for the agent configuration. For details about the agent configuration, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*. For details about how to specify the agent configuration, see the *JP1/IT Desktop Management 2 Online Help*.

Behavior when operations are restricted on users' computers

Users' attempts to start improper software, print large amounts of data, or use prohibited external media can be restricted. Attempts to move information in or out can also be restricted. For details, see 2.21.6 Behavior when operations are restricted on users' computers.

Connection request for remote control

In an NAT environment (where devices cannot be viewed from the controller) or in an NAPT environment (where IP addresses for devices change), it is difficult for the controller to remotely connect to computers. In such a case, connection requests from user computers to the controller, can be used to initiate remote control. For details, see 2.7.16 Issuing connection requests from remote computers to controllers.

2.21.1 Users' entry of user information

A window for entering user information can be displayed on online-managed computers when, for example, the settings for custom fields are changed on the management server. Whether to display a user information entry window can be selected in the **User notification settings** view for the agent configuration.

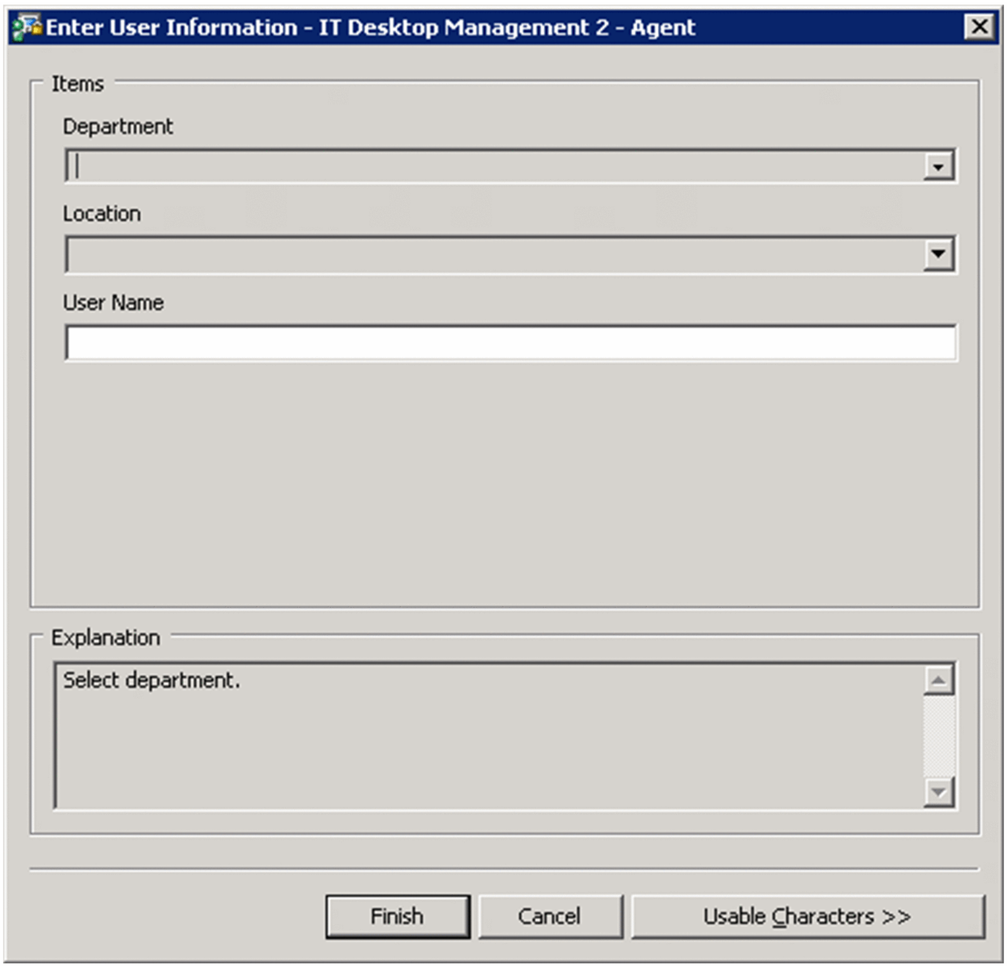
If entry of user information is being requested, users can also open a context menu from the taskbar icon ( ) to display a window for entering user information.

If the data source for asset fields is **End User**, a user information entry window appears when one of the following occurs.

- Asset fields are added, edited, or deleted on the management server (if asset fields are deleted, there must be remaining asset fields whose data source is **End User**).
- The latest information of a device is obtained by selecting **Update Device Details** from the **Action** menu.
- The time specified in the dialog box that opens by selecting **Enable End User Form (Frequent Pop-up)** from the **Action** menu is reached.
- The time specified in **Specified (a specified date and time for starting entry, in the local time of the user computers)** in **Start Date for Entry of User Information** of the Settings module is reached.
- 30 minutes have passed since the user information entry window was last displayed.
- 30 minutes have passed since the user information entry window was closed with no information entered.
- A user logs on to the computer.

User information can be entered in the **End User Form** view. The fields displayed in this view differ depending on the extended information specified on the management server.

The following shows an example of display in the **End User Form** view.



Select department.

The following describes how to enter individual fields. Note that the fields with an asterisk (*) are mandatory.

Fields in which text is directly entered

You can enter no more than 256 characters in text fields. To check the characters that can be entered, click the **Allowed Characters** button and check the character information.

Fields for which text is selected from a pull-down menu

You can select a text from the pull-down menu. Selection items might be displayed in a tree. Select the relevant text.

Back button

Clicking this button returns the previous page. This button is displayed when there are 6 or more fields in a page. This button is not displayed for the first page.

Next button

Clicking this button moves to the next page. This button is displayed when there are 6 or more fields in a page. This button is not displayed for the last page.

Complete button

Clicking this button notifies the management server of the entered user information, and then closes the **End User Form** view. If the mandatory fields have not been filled, a message requesting entry is displayed.

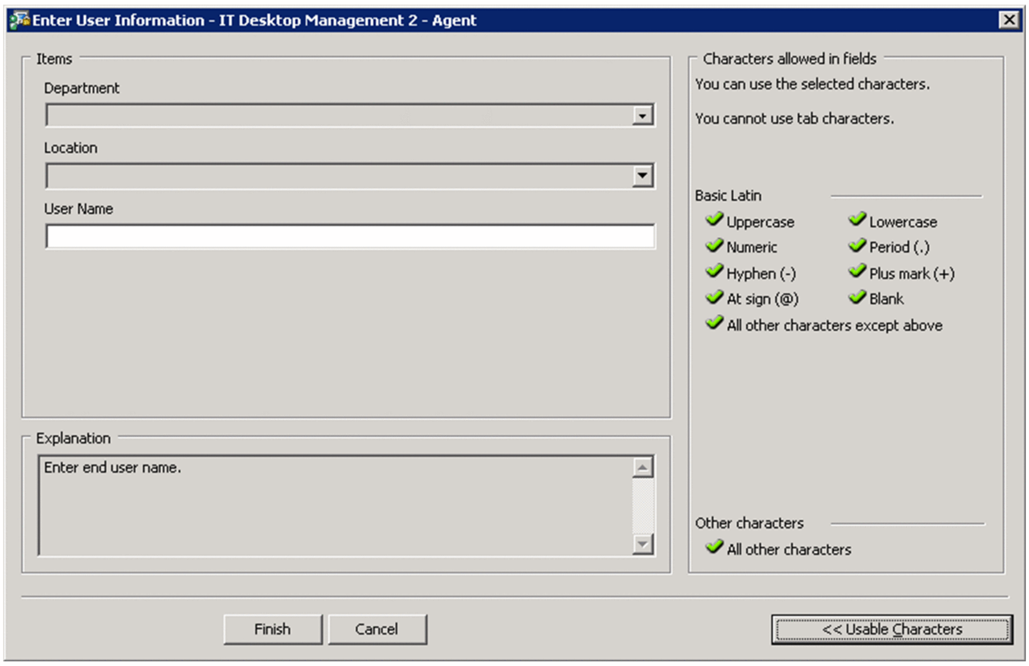
Cancel button

Clicking this button cancels the information you entered.

Allowed Characters

Select a target field and click this button. The characters that can be entered in that field are displayed.

The following figure is an example showing a display of characters that can be entered.



Enter end user name.

Characters allowed in fields

You can use the selected characters.

You cannot use tab characters.

Basic Latin

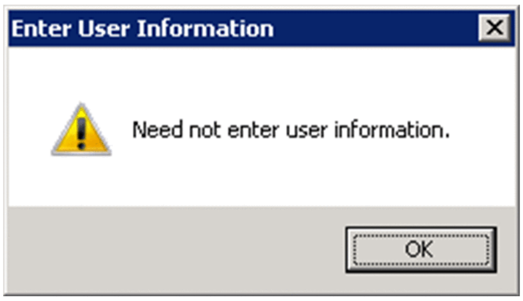
- ✓ Uppercase
- ✓ Lowercase
- ✓ Numeric
- ✓ Period (.)
- ✓ Hyphen (-)
- ✓ Plus mark (+)
- ✓ At sign (@)
- ✓ Blank
- ✓ All other characters except above

Other characters

- ✓ All other characters

To hide the display of characters that can be entered, click the **Allowed Characters** button again.

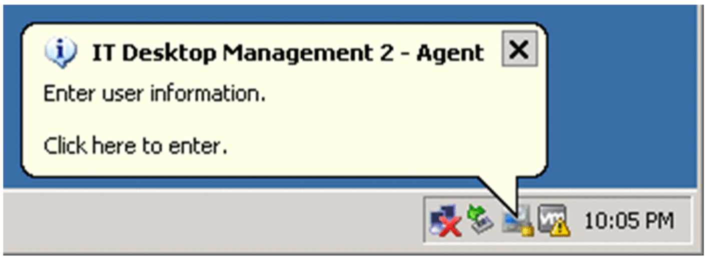
Before the start time specified for entry of user information reaches, selecting Windows **Start**, **All Programs**, **JP1_IT Desktop Management 2 - Agent**, and then **End User Form** on the user's computer causes the following window to appear:



Need not enter user information.

2.21.2 Display of balloon tips on users' computers

When a user operation is required, a balloon tip is displayed on a taskbar icon. Users can check balloon tips to understand the necessary operations. The following figure shows an example of a balloon tip.



Enter user information.

Click here to enter.

A balloon tip starts with an icon which indicates the message type. The following are the meanings of the icons:

- ℹ : Information
- ⚠ : Warning (Lower level risk)
- ✖ : Critical (Higher level risk)

Whether to display balloon tips can be selected in the **User notification settings** view for the agent configuration. The following table describes behavior when balloon tips are displayed and hidden.

Trigger	Message to be displayed	Behavior when the balloon tip is clicked	Influence if balloon tips are hidden, and action to be taken
A message about security judgment results is received from the system administrator.	You received a new message on *message-title* from Administrator. Click here to view.	A message about the results of the security status judgment is displayed.	To view the message, the user must open a context menu from the taskbar icon and then select **Display Message**.
A security policy that requires restart of the computer is applied.#	Restart the computer. The computer must be restarted for the following reasons. (1) The security policy was applied and the computer settings were changed. (2) The latest component was installed on the computer. (3) Software or an updated program was installed on the computer.	None	If the computer is not restarted immediately, security measures for the computer might be delayed. Specify to hide balloon tips on computers that need not be prompted to restart. For servers that are not restarted under normal conditions, specify to display balloon tips to show the necessity of a restart.
Entry of user information is requested from the system administrator.	Enter user information. Click here to enter.	The **End User Form** view appears.	To display a window to enter user information, open a context menu from the taskbar icon, and then select **End User Form**.

#: The following security policies require restart of a computer: Disable Anonymous Access, Enable Automatic Windows Update, Disable Remote Desktop, Disable Administrative Share, Disable DCOM, device write-operation restriction, and enable or disable operation logs or suspicious operations. Note that for security policy "Enable Windows Firewall", restart is required if Windows 7, Windows Server 2008, or Windows Vista is running on the computer.

Tip

Balloon tips are also displayed while software is being downloaded. For details, see 2.21.5 Behavior when distribution is performed on users' computers.

If more than one trigger occurs, balloon tips are stacked and displayed in the order of the triggers listed in the above table. Closing the displayed balloon tip will display the next balloon tip.

A balloon tip is closed when 10 seconds have passed since it was displayed or when the ☒ button is clicked. Also, for Windows 2000, nothing occurs when you click the balloon tip. If the user does not take action indicated in the balloon tip, the same balloon tip will be displayed again in 30 minutes. The following table describes the display timing of balloon tips.

Computer status	Display timing of a balloon tip
Logging on	A balloon tip is displayed immediately after a trigger (such as receiving a message about security judgment results) occurs.
	If the user does not take the action indicated in the balloon tip, the same balloon tip will be displayed again 30 minutes later.
	If the user does not take the action indicated in the balloon tip, the same balloon tip will be displayed again when the agent service is restarted.
Logging off	A balloon tip will be displayed at the next logon.
Computer is locked	A balloon tip will be displayed when the computer is unlocked.

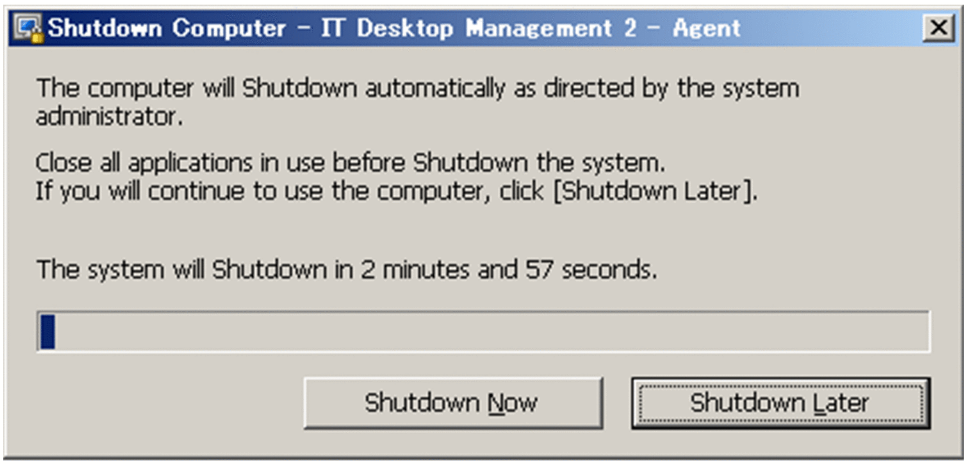
Important note

When the computer OS is Windows 8.1, Windows 8, Windows Server 2012 R2, Windows Server 2012, Windows 7, or Windows Server 2008 R2, the icon in the taskbar is usually hidden. To keep the icon displayed, customize the notification area of the taskbar (set the behavior of the jdnglogon icon to **Show icon and notifications**).

2.21.3 Behavior when users are directed to turn off computers

When the management server directs agent-installed computers to turn off, the **Shutdown Computer** dialog box will be displayed. Such agent-installed computers will be shut down 180 seconds after the **Shutdown Computer** dialog box is displayed.

The following figure shows the **Shutdown Computer** dialog box.



Shutdown Computer - IT Desktop Management 2 - Agent

The computer will Shutdown automatically as directed by the system administrator.

Close all applications in use before Shutdown the system.
If you will continue to use the computer, click [Shutdown Later].

The system will Shutdown in 2 minutes and 57 seconds.

Shutdown Now button

Clicking this button immediately shuts down the computer.

Shutdown Later button

Clicking this button cancels shutdown of the computer. The **Shutdown Computer** dialog box will not be displayed again, so the user must manually shut down the computer after clicking this button.

The following are notes on shutting down a computer:

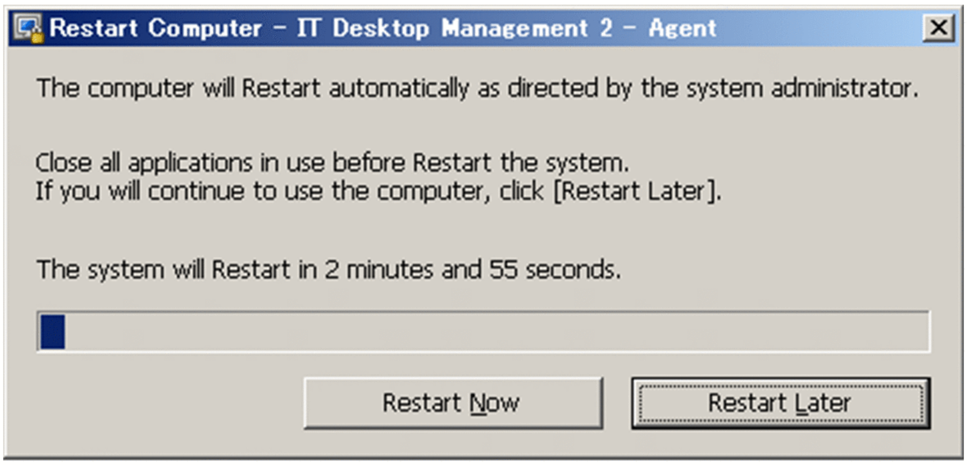
- If the screen saver is activated and the screen is password-protected, the computer will not be automatically shut down.
- If the computer is locked, it will not be automatically shut down.
- If there is a file being edited, the computer will not be automatically shut down.
- If another user is logged on, the computer will not be automatically shut down.
- If no user is logged on, the computer will be automatically shut down without displaying the **Shutdown Computer** dialog box.
- If the computer receives notification of turning off the computer from the management server while the **Shutdown Computer** dialog box is being displayed, subsequent notifications will be disabled.

2.21.4 Behavior when users are directed to restart computers

When the management server directs agent-installed computers to restart, the **Computer Restart Settings** dialog box will be displayed. The behavior (restart timing) related to this dialog box differs depending on the settings in **Settings to shut down and restart the computer** (under **User notification settings**) of Agent Configurations.

- If **Automatically start if no response is received from the user within the specified period** has been selected, the computer will automatically restart when the time specified in Agent Configuration has passed after the dialog box is displayed. This will occur even if the user does not respond to the dialog box.
- If **Follow the response of the user in the dialog box that instructs the user to shut down or restart the computer** has been selected, the computer will restart after the user responds to the dialog box. The computer will not restart automatically.

The following figure shows the **Computer Restart Settings** dialog box when **Automatically start if no response is received from the user within the specified period** has been selected.



Restart Computer - IT Desktop Management 2 - Agent

The computer will Restart automatically as directed by the system administrator.

Close all applications in use before Restart the system.
If you will continue to use the computer, click [Restart Later].

The system will Restart in 2 minutes and 55 seconds.

Immediate Installation button

Clicking this button immediately restarts the computer.

Restart Later button

Clicking this button cancels restart of the computer. The **Computer Restart Settings** dialog box will not be displayed again, so the user must manually restart the computer after clicking this button.

The following are notes on restarting a computer:

- If the screen saver is activated and the screen is password-protected, the computer will not be automatically restarted.
- If the computer is locked, it will not be automatically restarted.
- If there is a file being edited, the computer will not be automatically restarted.
- If another user is logged on, the computer will not be automatically restarted.
- If no user is logged on, the computer will be automatically restarted without displaying the **Computer Restart Settings** dialog box.
- If the computer receives notification of turning off the computer from the management server while the **Computer Restart Settings** dialog box is being displayed, only the notification of turning off the computer will be enabled. In this case, the **Computer Restart Settings** dialog box will be cancelled, and the **Shutdown Computer** dialog box will be displayed.

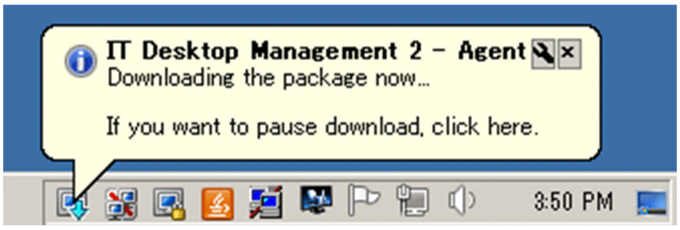
2.21.5 Behavior when distribution is performed on users' computers

When software is distributed, a balloon tip is displayed on a taskbar icon or a dialog box is displayed. To distribute software, you must create a package and task in the Distribution (ITDM-compatible) module. For a task, you can set an execution schedule for software distribution, execution timing of installation after software is distributed to target computers, and a message to be displayed before the installation.

The following describes the behaviors in individual cases:

Download

A balloon tip is displayed on a taskbar icon when download starts or when a user logs on to the computer. The following figure shows an example of a displayed balloon tip.



IT Desktop Management 2 – Agent

Downloading the package now...

If you want to pause download, click here.

A balloon tip starts with an icon which indicates the message type. The following are the meanings of the icons:

- ℹ : Information
- ❗ : Warning (Lower level risk)
- ✖ : Critical (Higher level risk)

Whether to display balloon tips can be selected in the **User notification settings** view for the agent configuration. The following table describes behavior when balloon tips are displayed and hidden.

Trigger	Message to be displayed	Behavior when the balloon tip is clicked	Action to be taken when balloon tips are hidden
Download starts	Downloading the package now... If you want to pause download, click here.	A dialog box confirming that the download will be paused, and the download is paused.	To interrupt the download, click the download icon.
Download restarts			

A balloon tip is closed when 10 seconds have passed since it was displayed or when the ✕ button is clicked. When you click a balloon tip, the behavior corresponding to the tip occurs. The following table describes the timing balloon tips are displayed.

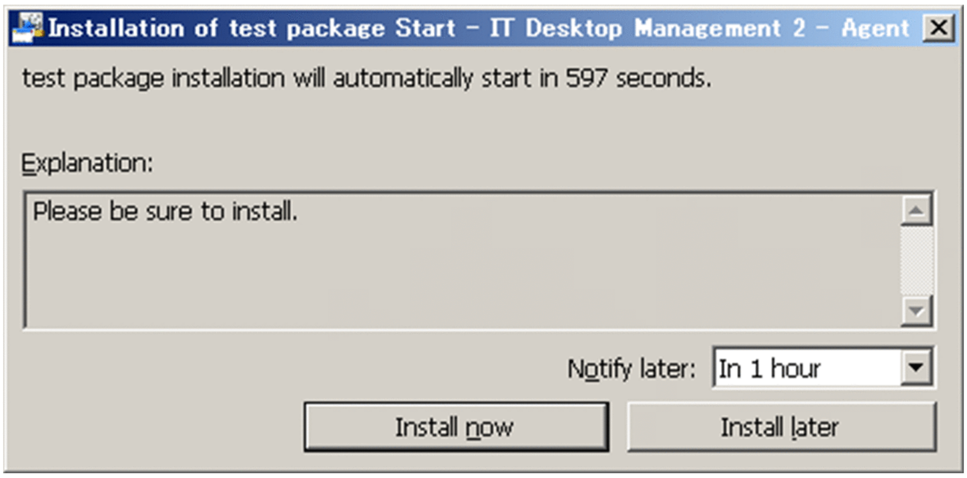
Computer status	Display timing of a balloon tip
Logging on	A balloon tip is displayed immediately after download starts or restarts.
	If the user does not take the action indicated in the balloon tip, the same balloon tip will be displayed again when the agent service is restarted.
Logging off	A balloon tip will be displayed at the next logon.

Important note

When the computer OS is Windows 8.1, Windows 8, Windows Server 2012 R2, Windows Server 2012, Windows 7, or Windows Server 2008 R2, the icon in the taskbar is usually hidden. To keep the icon displayed, customize the notification area of the taskbar (set the behavior of the jdnglogon icon to **Show icon and notifications**).

Installation

When a confirmation message must be displayed before the distributed software is installed, the message is displayed in a dialog box. The following figure shows an example of such a dialog box.



Installation of test package Start - IT Desktop Management 2 - Agent

test package installation will automatically start in 597 seconds.

Explanation:

Please be sure to install.

Notify later: In 1 hour

Immediate Installation button

Clicking this button immediately installs software on the computer.

Install later button

Clicking this button cancels installation of software. If the time specified for **Notify later** has passed, the same dialog box will be displayed again.

A dialog box is displayed before software is installed. The display timing of a dialog box differs depending on the computer status and the installation timing (execution timing) of software set by the administrator for the distribution task.

The following table describes the display timing of the dialog box.

Computer status	Execution timing	Display timing of a dialog box
Logging on	Installation will be performed at the next startup.#	A dialog box is displayed immediately.
	Installation is performed immediately.#	
	Installation is performed when a user logs on.	
Logging off	Installation will be performed at the next startup.	No dialog box is displayed.
	Installation is performed immediately.	
	Installation is performed when a user logs on.	A dialog box will be displayed at the next logon.

#: If a computer is restarted when the confirmation dialog box for installation remains displayed or when the **Install later** button has been clicked, after the computer is restarted, installation will start without displaying the confirmation dialog box for installation.

2.21.6 Behavior when operations are restricted on users' computers

You can restrict user attempts to start improper software, perform print operations, or use a prohibited device. This functionality provides a convenient means of maintaining security within a company, by restricting movement of information.

Blocking startup of software

When a user starts unauthorized software or uses software that is allowed during a specified period only, the **Software Startup Suppression** dialog box might be displayed. The software might be automatically stopped depending on the usage status.

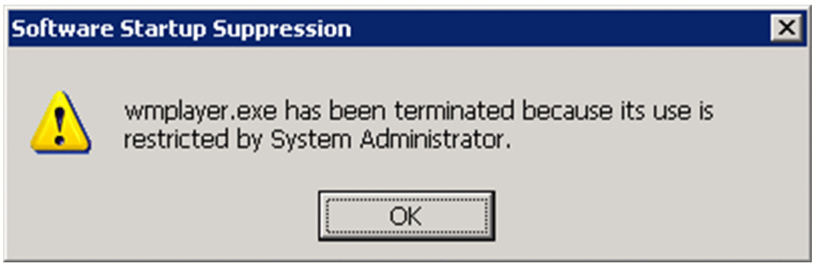
Clicking the **OK** button in the **Software Startup Suppression** dialog box closes the dialog box.

The following describe the notification messages displayed in the **Software Startup Suppression** dialog box.

Note that if the OS on a user's computer is Windows 8.1, Windows 8, or Windows Server 2012, a dialog box is displayed on the desktop of the user's computer.

Notification of blocked software

Displayed when there is an attempt to start unauthorized software. The following figure shows a display example.

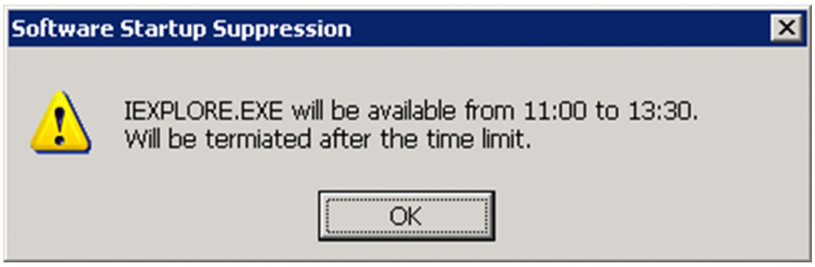


Software Startup Suppression

wmplayer.exe has been terminated because its use is restricted by System Administrator.

Notification of the time the software is available

Displayed when the software allowed for use during a specified period is being used during that period. The following figure shows a display example.

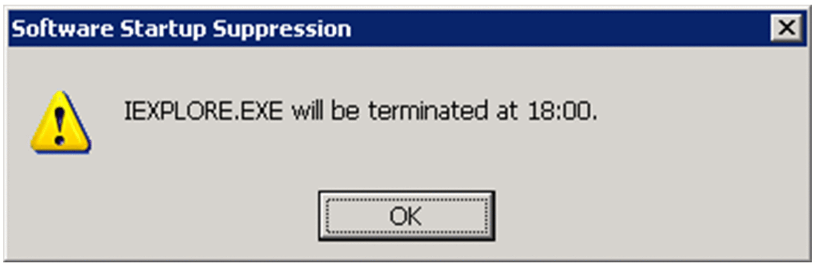


Software Startup Suppression

IEXPLORE.EXE will be available from 11:00 to 13:30.
Will be termiated after the time limit.

Notification of the time the software is unavailable

Displayed when the software allowed for use during a specified period is being used and the period will end soon. When the period has passed, the software is automatically stopped. The following figure shows a display example.



Software Startup Suppression

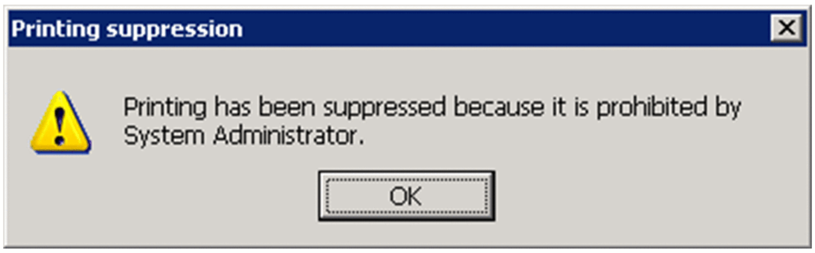
IEXPLORE.EXE will be terminated at 18:00.

Blocking printing

When printing is performed on an agent-installed computer to which a security policy for blocking printing is applied, the **Printing suppression** dialog box for blocking printing is displayed. Clicking the **OK** button closes the dialog box.

Note that if the OS on a user's computer is Windows 8.1, Windows 8, or Windows Server 2012, a dialog box is displayed on the desktop of the user's computer.

The following figure shows the **Printing suppression** dialog box.



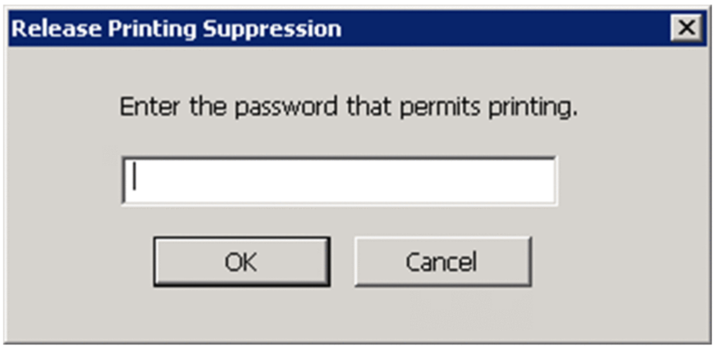
Printing suppression

Printing has been suppressed because it is prohibited by System Administrator.

When allowed, the user can use a password to release the blockage of printing. To perform this, double-click the Block Printing icon ( ) in the taskbar. The **Release Printing Suppression** dialog box (for entering a password) is displayed. Enter the necessary password, and then click the **OK** button.

Note that if the OS on a user's computer is Windows 8.1, Windows 8, or Windows Server 2012, a dialog box is displayed on the desktop of the user's computer.

The following figure shows the **Release Printing Suppression** dialog box (for entering a password).


Release Printing Suppression

Enter the password that permits printing.

If blockage of printing could be released, the **Release Printing Suppression** dialog box (indicating a successful operation) is displayed. The user will then be able to perform printing. If blockage of printing could not be released, the **Release Printing Suppression** dialog box (indicating a failure operation) is displayed. Clicking the **OK** button closes the dialog box.

If the user clicks the Block Printing icon ( ) when a password for releasing blockage of printing cannot be used, a dialog box indicating that printing is being blocked is displayed. Clicking the **OK** button closes the dialog box.

Restricting use of devices

When a device is used on an agent-installed computer with a security policy for restricting the use of the device applied, and if the security policy is configured to display a message, the **Device usage suppression** dialog box appears. Clicking the **OK** button closes the dialog box.

2.21.7 Users who receive notifications from the agent

If more than one user logs on to the same computer, notifications (such as balloon tips and dialog boxes) are informed to only part of the users. By restricting the notification-target users, the users who do not need to take action will not need to deal with unnecessary information.

The following are notification-target users for individual OSs installed on agent-installed computers:

For Windows 8.1, Windows 8, Windows 7, Windows Vista, or Windows XP:

- All logged on users
- Users who logged on by using a Remote Desktop connection

For Windows Server 2012 or Windows Server 2008:

- Users who logged on to the local console
- The user with administrative privileges who logged on first by using a Remote Desktop connection

For Windows Server 2003:

- Users who logged on to the local console
- Users who logged on by using a Remote Desktop connection with the `/console` and `/admin` options specified#

#: If there is no corresponding user, the user with administrative privileges who logged on first by using a Remote Desktop connection becomes the notification target.

2.21.8 Notes on users' computers

- Do not disable the applications below on users' computers. If these applications are disabled, some JP1/IT Desktop Management 2 functions might not work correctly.
    - jdngrcagent.exe
    - jdngrcchat.exe
    - jdnglogon.exe
    - jdngsmclogin.exe

2.22 Controlling smart devices

By linking with MDM systems, JP1/IT Desktop Management 2 can control managed smart devices. This function is convenient because you can control smart devices without the need of operating MDM systems.

By linking with MDM systems, you can perform the following types of control on smart devices:

Locking smart devices

The administrator can lock a smart device so that if the user loses the smart device, a finder cannot operate it.

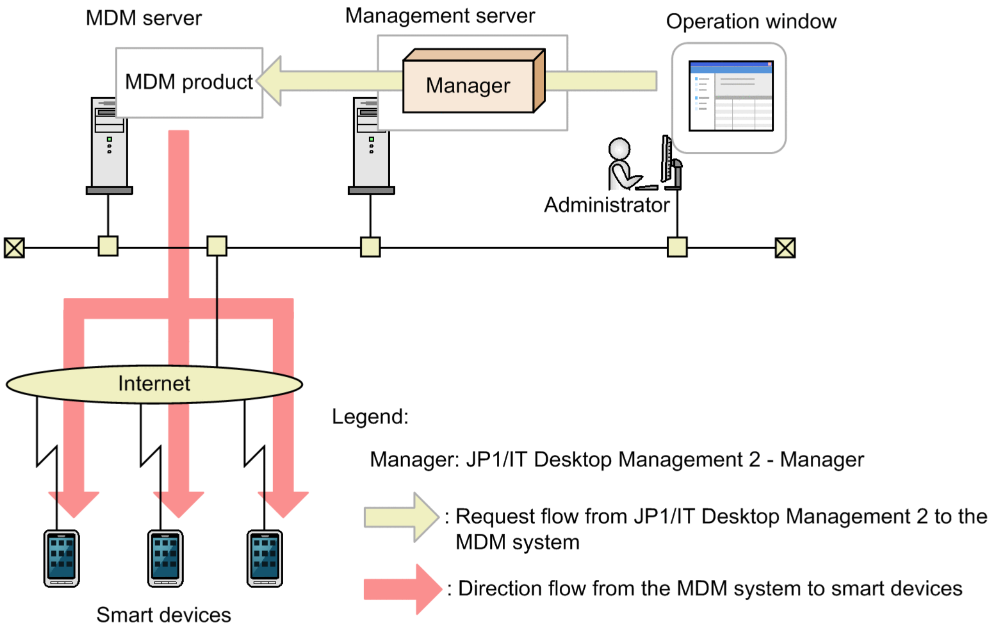
Resetting the passcodes for smart devices

The administrator can reset the passcode for a smart device so that when the user forgets the passcode, the same user can set a new passcode.

Initializing smart devices

The administrator can initialize a smart device to the factory settings when changing the user of a smart device or when disposing of a smart device.

Smart devices are controlled by MDM systems that respond to requests issued by JP1/IT Desktop Management 2. The following figure shows the flow of controlling smart devices.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager

⇨ : Request flow from JP1/IT Desktop Management 2 to the MDM system

➡ : Direction flow from the MDM system to smart devices

Important note

If the settings for linking with an MDM system are deleted, the smart devices managed by that MDM system can no longer be controlled.

Tip

JP1/IT Desktop Management 2 considers that target smart devices have been controlled when an MDM system receives the relevant requests.

Related Topics:

- 2.6.6 Linking with an MDM system

3 About Product Licenses

This chapter describes JP1/IT Desktop Management 2 product licenses.

3.1 Overview of product licenses

JP1/IT Desktop Management 2 uses the node count license method to manage the number of used licenses. This method uses one license for a managed device regardless of the type of the device. This means that as many devices as the number of licenses registered on JP1/IT Desktop Management 2 can be managed. Note that licenses are used for device management only, and not used for asset management.

Use the product edition license key file, which is provided when JP1/IT Desktop Management 2 is purchased, to register a license. If the number of used licenses matches the number of registered licenses, no more devices can be added. Therefore, register a sufficient number of licenses in advance.

If you want to manage more devices than you have registered licenses for, you need to add licenses. To add a product license, purchase a license and then register it.

When automatic registration during a search adds more management targets than there are licenses for, the devices are handled as *discovered devices*. Although the discovered devices are displayed in the view displayed by selecting **Discovery**, and then **Discovered Nodes** in the Settings module, they are not management targets (no licenses are used). If a managed device is changed to an exclusion target or is deleted, the number of used licenses changes.

Tip

In a multi-boot environment, each OS is handled as a different device because information reported to the management server differs depending on the OS.

3.2 Relationship between device status and product license

If a discovered device is added as a management target or if a managed device is excluded from management, the number of used product licenses changes. The following table describes the device statuses and whether a product license is required.

Device status	Product license	Description
Discovered	No	The device is discovered by the network search or network monitoring function.
Managed	Yes	The device is to be managed as a target of device management, security control, and asset management. The managed device is subject to operations performed from the management server and report display.
Ignored	No	The device is excluded from the management. Any device that does not need to be managed must be in the Ignored status.

Legend: Yes: Used, No: Not used

To add a device as a management target of JP1/IT Desktop Management 2, set the device status to Managed. If you set the device status to Managed, a product license is used. A device whose status is Discovered or Ignored does not use a product license. If you change the status of a device from Managed to Ignored, the product license used for that device can be used for another device.

3.3 Cautions about product licenses

Product licenses can be used only on the computer on which they have been registered, and cannot be used on any other computer.

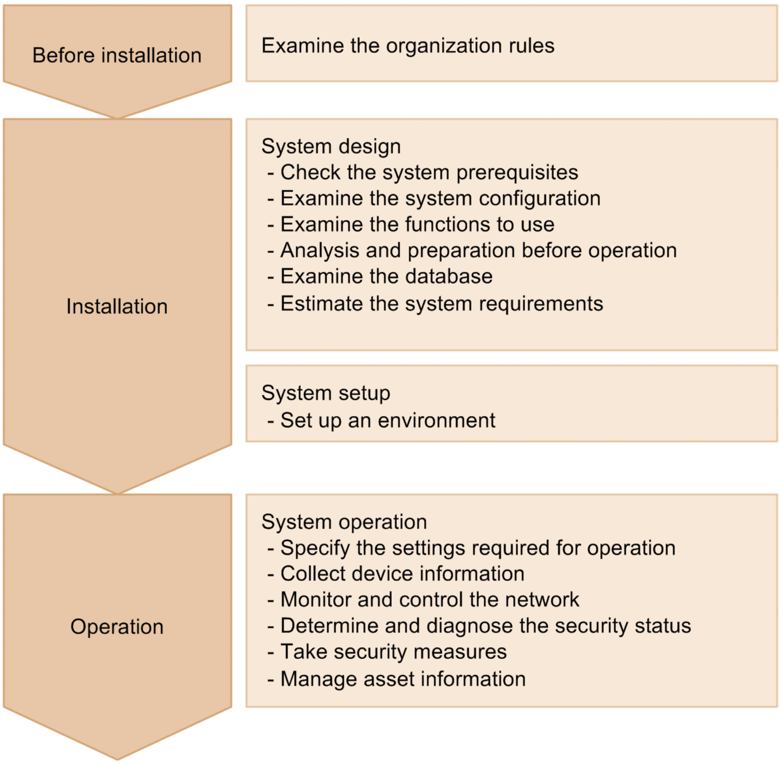
4 System Design

System design for JP1/IT Desktop Management 2 requires the examination of the system configuration, the system operation methods, and an estimate of system requirements.

This chapter provides an overview of how to design a JP1/IT Desktop Management 2 system and start operation. This chapter also describes the issues that must be examined during system design.

4.1 Installation and operation procedure

This section describes the procedure for installation and operation of JP1/IT Desktop Management 2. To install JP1/IT Desktop Management 2, you must first design the system. During system design, determine the system configuration and operation methods. Then, set up the system and start operation. The following figure shows the procedure for installation and operation ofJP1/IT Desktop Management 2.


Before installation
Examine the organization rules
Installation
System design
- Check the system prerequisites
- Examine the system configuration
- Examine the functions to use
- Analysis and preparation before operation
- Examine the database
- Estimate the system requirements
System setup
- Set up an environment
Operation
System operation
- Specify the settings required for operation
- Collect device information
- Monitor and control the network
- Determine and diagnose the security status
- Take security measures
- Manage asset information

For details about the system design and system setup procedures, see 4.1.1 Installation procedure. For details about the system operation procedure, see 4.1.2 Operation procedure.

4.1.1 Installation procedure

To install JP1/IT Desktop Management 2, you must design a system configuration and set up an environment. The following describes the installation procedure for JP1/IT Desktop Management 2.

1. Examine the organization rules

   Examine the security control rules for the organization. You can design, set up, and operate the JP1/IT Desktop Management 2 system based on the examination results.

2. Check the system prerequisites

   Check the prerequisites for the servers and computers in the system. For details about checking the prerequisites, see 4.2 System prerequisites.

3. Examine the system configuration

   Examine the system configuration considering the purpose of the system. For details about examining system configurations, see 4.4 Examining the system configuration.

4. Examine the functions to use

Confirm that the operating environment satisfies the prerequisites for the functions to be used. For details about the prerequisites for each function, see 4.3 Prerequisites for functions.

5. Analysis and preparation before operation

   Examine the system operation methods, including the devices to be managed and the operation schedule. For details about examining operation methods, see 4.6 Analysis and Preparation before operation.

6. Examine the database

   Consider what database size is appropriate for the operation method. For details about examining a database, see 4.5 Examining the database.

7. Estimate the system requirements

   Based on the results in steps 1 to 6, estimate the requirements of the system. For details about estimating system requirements, see A.6 Performance and Estimates.

For details about the system operation procedure, see 4.1.2 Operation procedure.

4.1.2 Operation procedure

After setting up an environment, you can operate the system as determined during system design. The following describes the operation procedure for the JP1/IT Desktop Management 2 system.

1. Specify the settings required for operation

   Use the operation windows of JP1/IT Desktop Management 2 to specify the search schedule and search range for devices and the security policy based on the results of the examination performed before operation.

2. Collect device information

   Search for devices from the management server to automatically collect the latest IT device information. If necessary, install agents on the computers.

3. Monitor and control the network

   Monitor the network for any new computers connected, and prevent unauthorized computers or computers with insufficient security measures from connecting to the network.

4. Determine and diagnose security status

   Confirm that the computers observe the predefined security policy to check for any computers with insufficient security measures. JP1/IT Desktop Management 2 can output a report containing the collected information that you can use to diagnose security status.

5. Take security measures

   Take security measures based on the diagnostic results. If you need to review the policy, return to step 1 and change the security policy.

6. Manage asset information

   Manage all information about the assets owned by the organization, including the devices, software licenses, and contracts. You can keep track of the usage status of hardware assets and software licenses, and check the resources' contract information and costs.

4.2 System prerequisites

This section describes the prerequisites for the network and system components, including the management server installed in the system, and the computers on which agents are installed.

For details about memory requirements, disk space requirements, and available CPUs, see A.6 Performance and Estimates.

Related Topics:

- 4.2.1 Management server prerequisites
- 4.2.3 Prerequisites for a computer on which an agent will be installed
- 4.2.6 Prerequisites for a computer on which the network monitor is enabled
- 4.2.5 Prerequisites for a computer on which the controller will be installed
- 4.2.9 Network prerequisites

4.2.1 Management server prerequisites

The following describes the OSs and software required for the management server.

Note that you can use only alphanumeric characters and hyphens (-) for the computer name of the server on which JP1/IT Desktop Management 2 - Manager is installed. Also note that the computer name must begin with an alphabetic character and end with an alphanumeric character.

OSs

The management server requires one of the OSs listed in the following table.

OS	Details
Windows Server 2012[#1]	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter[#2]
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard[#2]
Windows Server 2008[#1]	Windows Server 2008 R2 Datacenter[#3]
	Windows Server 2008 Enterprise[#4]
	Windows Server 2008 Enterprise without Hyper-V[#4]
	Windows Server 2008 R2 Enterprise[#3]
	Windows Server 2008 Standard[#4]
	Windows Server 2008 Standard without Hyper-V[#4]
	Windows Server 2008 R2 Standard[#3]
Windows Server 2003	Windows Server 2003, Enterprise Edition[#3, #4]
	Windows Server 2003, Enterprise x64 Edition[#3, #4]
	Windows Server 2003 R2, Enterprise Edition[#4]

OS	Details
Windows Server 2003	Windows Server 2003 R2, Enterprise x64 Edition#4
	Windows Server 2003, Standard Edition#3, #4
	Windows Server 2003, Standard x64 Edition#3, #4
	Windows Server 2003 R2, Standard Edition#4
	Windows Server 2003 R2, Standard x64 Edition#4

#1: Server Core cannot be used as an installation option.

#2: Operation in an environment with OneDrive is not supported.

#3: Service Pack 1 is included.

#4: Service Pack 2 is included.

Software

Windows Installer 2.0 or later must be installed on the server on which JP1/IT Desktop Management 2 - Manager is to be installed.

Related Topics:

- A.6 Performance and Estimates

4.2.2 Prerequisites for an administrator's computer

The following describes the software required for using the operation windows and OS, and the software required to install Remote Installation Manager. For prerequisites required to use the computer as a controller, see 4.2.5 Prerequisites for a computer on which the controller will be installed.

Remote Installation Manager and JP1/IT Desktop Management 2 - Agent (relay system) cannot be installed on the same computer.

Software required for using the operation windows

The following table lists the software required to use the operation windows of JP1/IT Desktop Management 2.

Item	Software
Web browser	One of the following is required: • Windows Internet Explorer 7 • Windows Internet Explorer 8 • Windows Internet Explorer 9 • Windows Internet Explorer 10 • Windows Internet Explorer 11 • Firefox 24 or later
Browser plug-in	For OSs other than Windows Server 2012 Adobe Flash Player 11.7 or later For Windows Server 2012 Desktop Experience

Tip

If a dialog box asking you to upgrade Adobe Flash Player appears when you access the JP1/IT Desktop Management 2 login window, upgrade your Adobe Flash Player in response to the request.

OSs required to install Remote Install Manager

A computer on which Remote Installation Manager will be installed requires one of the OSs listed in the following table.

OS	Details
Windows 8.1[#1]	Windows 8.1
	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012[#2]	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter[#1]
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard[#1]
Windows 7[#3]	Windows 7 Enterprise[#4]
	Windows 7 Professional[#4]
	Windows 7 Ultimate[#4]
Windows Server 2008[#2]	Windows Server 2008 R2 Datacenter[#4]
	Windows Server 2008 Enterprise[#5]
	Windows Server 2008 Enterprise without Hyper-V[#5]
	Windows Server 2008 R2 Enterprise[#4]
	Windows Server 2008 Standard[#5]
	Windows Server 2008 Standard without Hyper-V[#5]
	Windows Server 2008 R2 Standard[#3]
Windows Server 2003	Windows Server 2003, Enterprise Edition[#4, #5]
	Windows Server 2003, Enterprise x64 Edition[#4, #5]
	Windows Server 2003 R2, Enterprise Edition[#5]
	Windows Server 2003 R2, Enterprise x64 Edition[#5]
	Windows Server 2003, Standard Edition[#4, #5]
	Windows Server 2003, Standard x64 Edition[#4, #5]
	Windows Server 2003 R2, Standard Edition[#5]

OS	Details
Windows Server 2003	Windows Server 2003 R2, Standard x64 Edition[#5]

#1

Operation in an environment with OneDrive is not supported.

#2

Server Core cannot be used as an installation option.

#3

XP mode is not supported.

#4

Service Pack 1 is included.

#5

Service Pack 2 is included.

Note that you can use only alphanumeric characters and hyphens (-) for the computer name of the server on which Remote Installation Manager is installed. Also note that the computer name must begin with an alphabetic character and end with an alphanumeric character.

To install Remote Installation Manager on a computer different from the management-server-installed computer, the version of Remote Installation Manager and the version of JP1/IT Desktop Management 2 - Manager on the management server must be the same.

Software required to install Remote Installation Manager

Windows Installer 2.0 or later

Related Topics:

- A.6 Performance and Estimates

4.2.3 Prerequisites for a computer on which an agent will be installed

A computers on which an agent will be installed requires one of the OSs listed in the following table.

OS	Details
Windows 8.1[#1]	Windows 8.1
	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8[#2, #3]	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012[#4]	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter[#1]
	Windows Server 2012 Standard

OS	Details
Windows Server 2012[#4]	Windows Server 2012 R2 Standard[#1]
Windows 7[#3, #5, #6]	Windows 7 Enterprise
	Windows 7 Home Basic
	Windows 7 Home Premium
	Windows 7 Professional
	Windows 7 Starter
	Windows 7 Ultimate
Windows Server 2008[#4]	Windows Server 2008 R2 Datacenter[#5]
	Windows Server 2008 Enterprise[#6]
	Windows Server 2008 Enterprise without Hyper-V[#6]
	Windows Server 2008 R2 Enterprise[#5]
	Windows Server 2008 Standard[#6]
	Windows Server 2008 Standard without Hyper-V[#6]
	Windows Server 2008 R2 Standard[#5]
Windows Vista[#3, #6, #7]	Windows Vista Business
	Windows Vista Enterprise
	Windows Vista Home Basic
	Windows Vista Home Premium
	Windows Vista Ultimate
Windows Server 2003	Windows Server 2003, Enterprise Edition[#5, #6]
	Windows Server 2003, Enterprise x64 Edition[#5, #6]
	Windows Server 2003 R2, Enterprise Edition[#6]
	Windows Server 2003 R2, Enterprise x64 Edition[#6]
	Windows Server 2003, Standard Edition[#5, #6]
	Windows Server 2003, Standard x64 Edition[#5, #6]
	Windows Server 2003 R2, Standard Edition[#6]
	Windows Server 2003 R2, Standard x64 Edition[#6]
Windows XP[#3, #8]	Windows XP Home Edition Operating System (Service Pack 2 or 3)
	Windows XP Professional Operating System (Service Pack 2 or 3)

#1: Operation in an environment with OneDrive is not supported.

#2: Not supported when Windows To Go is used.

#3: Remote desktop is not supported. Install an agent on the local console.

#4: Server Core cannot be used as an installation option.

#5: XP mode is not supported.

#6: Service Pack 1 is included.

#7: Service Pack 2 is included.

#8: Fast User Switching feature in the Windows XP is not supported. Install an agent after restarting the computer.

Important note

You must start the Workstation service for the OS. In an environment in which this service has stopped, the security level determined based on the security policy is displayed as **Unknown** because OS account information cannot be acquired.

Software

The following table shows the software required for a computer on which an agent will be installed.

Item	Software
Web browser	One of the following is required: • Windows Internet Explorer 7 • Windows Internet Explorer 8 • Windows Internet Explorer 9 • Windows Internet Explorer 10 • Windows Internet Explorer 11

Related Topics:

- A.6 Performance and Estimates

4.2.4 Prerequisites for a computer on which a relay system will be installed

The following describes prerequisites for a computer on which a relay system will be installed.

JP1/IT Desktop Management 2 - Agent (relay system) and Remote Install Manager cannot be installed on the same computer.

OS

A computer on which a relay system will be installed requires one of the OSs listed in the following table.

OS	Details
Windows 8.1[#1]	Windows 8.1
	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8[#2]	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro

OS	Details
Windows Server 2012#3	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter#1
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard#1
Windows 7#4#5	Windows 7 Enterprise
	Windows 7 Professional
	Windows 7 Ultimate
Windows Server 2008#3	Windows Server 2008 R2 Datacenter#5
	Windows Server 2008 Enterprise#6
	Windows Server 2008 Enterprise without Hyper-V#6
	Windows Server 2008 R2 Enterprise#5
	Windows Server 2008 Standard#6
	Windows Server 2008 Standard without Hyper-V#6
	Windows Server 2008 R2 Standard#5
Windows Vista#5, #6	Windows Vista Business
	Windows Vista Enterprise
	Windows Vista Ultimate
Windows Server 2003	Windows Server 2003, Enterprise Edition#5, #6
	Windows Server 2003, Enterprise x64 Edition#5, #6
	Windows Server 2003 R2, Enterprise Edition#6
	Windows Server 2003 R2, Enterprise x64 Edition#6
	Windows Server 2003, Standard Edition#5, #6
	Windows Server 2003, Standard x64 Edition#5, #6
	Windows Server 2003 R2, Standard Edition#6
	Windows Server 2003 R2, Standard x64 Edition#6
Windows XP	Windows XP Professional Operating System (Service Pack 2, 3)

#1: Operation in an environment with OneDrive is not supported.

#2: Not supported when Windows To Go is used.

#3: Server Core cannot be used as an installation option.

#4: XP mode is not supported.

#5: Service Pack 1 is included.

#6: Service Pack 2 is included.

Important note

You must start the Workstation service for the OS. In an environment in which this service has stopped, the security level determined based on the security policy is displayed as **Unknown** because OS account information cannot be acquired.

Software

The following table lists software required for a computer on which a relay system will be installed.

Item	Software
Web browser	One of the following is required: • Windows Internet Explorer 7 • Windows Internet Explorer 8 • Windows Internet Explorer 9 • Windows Internet Explorer 10 • Windows Internet Explorer 11

Related Topics:

- A.6 Performance and Estimates

4.2.5 Prerequisites for a computer on which the controller will be installed

A computer on which the controller will be installed requires one of the OSs listed in the following table.

OS	Details
Windows 8.1#1	Windows 8.1
	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8#2	Windows 8
	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012#3	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter#1
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard#1
Windows 7#4	Windows 7 Enterprise#5
	Windows 7 Home Premium#5
	Windows 7 Professional#5
	Windows 7 Starter#5
	Windows 7 Ultimate#5

OS	Details
Windows Server 2008#3	Windows Server 2008 R2 Datacenter#5
	Windows Server 2008 Enterprise#6
	Windows Server 2008 Enterprise without Hyper-V#6
	Windows Server 2008 R2 Enterprise#5
	Windows Server 2008 Standard#6
	Windows Server 2008 Standard without Hyper-V#6
	Windows Server 2008 R2 Standard#5
Windows Vista	Windows Vista Business#5, #6
	Windows Vista Enterprise#5, #6
	Windows Vista Home Basic#5, #6
	Windows Vista Home Premium#5, #6
	Windows Vista Ultimate#5, #6
Windows Server 2003	Windows Server 2003, Enterprise Edition#5, #6
	Windows Server 2003, Enterprise x64 Edition#5, #6
	Windows Server 2003 R2, Enterprise Edition#6
	Windows Server 2003 R2, Enterprise x64 Edition#6
	Windows Server 2003, Standard Edition#5, #6
	Windows Server 2003, Standard x64 Edition#5, #6
	Windows Server 2003 R2, Standard Edition#6
	Windows Server 2003 R2, Standard x64 Edition#6
Windows XP	Windows XP Home Edition Operating System (Service Pack 2 or 3)
	Windows XP Professional Operating System (Service Pack 2 or 3)

#1: Operation in an environment with OneDrive is not supported.

#2: Not supported when Windows To Go is used.

#3: Server Core cannot be used as an installation option.

#4: XP mode is not supported.

#5: Service Pack 1 is included.

#6: Service Pack 2 is included.

Related Topics:

- A.6 Performance and Estimates

4.2.6 Prerequisites for a computer on which the network monitor is enabled

A computer on which the network monitor is enabled requires one of the OSs listed in the following table.

OSs

OS	Details
Windows 8.1[#1]	Windows 8.1 Enterprise
	Windows 8.1 Pro
Windows 8	Windows 8 Enterprise
	Windows 8 Pro
Windows Server 2012[#2]	Windows Server 2012 Datacenter
	Windows Server 2012 R2 Datacenter[#1]
	Windows Server 2012 Standard
	Windows Server 2012 R2 Standard[#1]
Windows 7[#3]	Windows 7 Enterprise[#4]
	Windows 7 Professional[#4]
	Windows 7 Ultimate[#4]
Windows Server 2008[#2]	Windows Server 2008 R2 Datacenter[#4]
	Windows Server 2008 Enterprise[#5]
	Windows Server 2008 Enterprise without Hyper-V[#5]
	Windows Server 2008 R2 Enterprise[#4]
	Windows Server 2008 Standard[#5]
	Windows Server 2008 Standard without Hyper-V[#5]
	Windows Server 2008 R2 Standard[#4]
Windows Server 2003	Windows Server 2003, Standard Edition[#4, #5]
	Windows Server 2003 R2, Standard Edition[#5]
	Windows Server 2003, Enterprise Edition[#4, #5]
	Windows Server 2003 R2, Enterprise Edition[#5]

#1: Operation in an environment with OneDrive is not supported.

#2: Server Core cannot be used as an installation option.

#3: XP mode is not supported.

#4: Service Pack 1 is included.

#5: Service Pack 2 is included.

Software

An online management agent or a relay system must be installed.

Network environment

- The IP address must be fixed.
- The computer cannot have multiple IP addresses in the same network segment.

Related Topics:

- 4.2.3 Prerequisites for a computer on which an agent will be installed
- A.6 Performance and Estimates

4.2.7 Prerequisites for agentless management

When using agentless management, setup must be completed on both the management server and user computer to collect device information. The range of information that can be acquired depends on the authentication method. The range of information that can be acquired depends on the authentication method. A limited range of information may result in unknown security states and missing data in reports, causing risks to system operation. Select the best authentication method for your security needs.

Setup to collect most of the available device information is easy if you are using Active Directory to manage the computers in your organization. If you are thinking of using agentless management, first make sure that your computers are managed in Active Directory.

For differences between the types of device information that can be collected, see 2.6.2 Collecting device information.

Important note

Agentless management is not supported in a NAT environment.

Important note

Do not delete the discovery range or authentication information for any agentless managed device discovered in a network search. Likewise, do not delete the Active Directory setting for any agentless managed device discovered by an Active Directory search. Deleting this setting information prevents device information from being collected. If you mistakenly delete the discovery range, authentication information, or Active Directory setting, add them and then re-execute the network search or Active Directory search to discover the devices.

Important note

In a DHCP environment, if a device's IP address changes, moving outside the discovery range, no information will be collected about that device.

When using Windows administrative shares to perform agentless management

All the following conditions must be satisfied:

- Windows firewall is disabled on the user's computer[#1].

- Simple file sharing is disabled on the user's computer.
- File and Printer Sharing is enabled on the user's computer.
- Windows Administrative Share (ADMIN$) is enabled on the user's computer.
- Access to the Interprocess Communications share (IPC$) is enabled on the user's computer.
- The information used for logging in to the target computer by using Windows administrative shares is set on the management server as authentication information for network searches.[#2]

#1: Even if Windows Firewall is enabled, the condition is still satisfied if TCP (port 445) is open for traffic.

#2: The authentication information for logging in to the target computer by using Windows administrative shares must satisfy either of the following conditions:

- The built-in Administrator account and password of the user's computer is used.
- The UAC function is disabled on the user's computer.

How to enable Windows administrative shares differs depending on the OS on the user's computer. The following settings are required to enable Windows administrative shares:

OS	Setting
Windows 8.1	• Disable UAC or enable the Administrator account.[#1] • Enable **File and Printer Sharing** in the Network and Sharing Center window.
Windows 8	
Windows 7	
Windows Vista	• Disable UAC or enable the Administrator account. • Enable **File sharing** in the Network and Sharing Center window.
Windows XP[#2]	• Disable simple file sharing. • Add file shares.
Windows Server 2012	Enable **File sharing** or **File and Printer Sharing** in the Network and Sharing Center window.
Windows Server 2008	
Windows Server 2003	Setup unnecessary (enabled by default).
Windows 2000	Add file shares.
Computer other than Windows	Not supported (cannot be configured).
Network device	Not supported (cannot be configured).

#1: If you are using Windows 8.1 or Windows 8 (no edition), perform this setup by executing the `net user` command at the command prompt. You cannot enable the Administrator account from the Windows Control Panel.

#2: In Windows XP Home Edition (Service Pack 2 and 3), Windows administrative shares cannot be used.

If these conditions are satisfied, you can acquire most of the available device information. The information collected hardly differs from that collected via agents installed on the managed computers.

When using SNMP to perform agentless management

The following conditions must be satisfied:

- SNMP can be used.
- The community name can be authenticated.

The following table describes the setup required to acquire device information using SNMP:

OS	Setting
Windows 8.1	- Install an SNMP agent. - Set up the SNMP agent.
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Computer other than Windows	
Network device	

When using Active Directory to perform agentless management

Both the following conditions must be satisfied:

- Windows firewall is disabled on the user's computer.#
- Using the Active Directory linkage feature, the management server can acquire device information managed by Active Directory.

#: If Windows firewall is enabled, the condition is still satisfied if connection via a port number specified in **Active Directory settings** view accessed from **General** view in the Settings module is open for traffic.

When using ICMP to perform agentless management

ICMP must be available for use.

The following table describes the setup required to acquire device information using ICMP:

OS	Setting
Windows 8.1	Allow incoming ICMP echo requests.#
Windows 8	
Windows 7	
Windows Vista	
Windows XP	
Windows Server 2012	
Windows Server 2008	
Windows Server 2003	
Windows 2000	
Computer other than Windows	
Network device	

#: In Windows XP or later, you must configure the Windows Firewall to allow ICMP traffic or disable Windows Firewall.

Related Topics:

- (1) Types of device information you can collect
- (2) Device status information that can be collected
- (3) System information that can be collected
- (4) Hardware information
- (5) Installed software information
- (6) Security information
- (7) Shared management items for asset information and device information

4.2.8 Prerequisites for linking with JP1/IM

The following shows the software required for linking with JP1/IM.

- JP1/IM 10-00 or later
- JP1/Base 10-01 or later

The required OSs are the same as for JP1/Base.

4.2.9 Network prerequisites

The following describes the prerequisites for a network environment in whichJP1/IT Desktop Management 2 is installed.

> **Important note**
>
> Whether communication is possible across a NAT, WAN, or VPN depends on the environment. Therefore, verify that communication is possible beforehand.

> **Important note**
>
> In a NAT environment, you can install an agent to manage a computer, but cannot perform operations for the agent, such as message notification or acquisition of the latest device information, whenever you want. If you attempt such operations, they are performed when a polling from the agent occurs.

Entire network

Use a static IP address for the global IP address of the management server.

In addition, the TCP protocol ports used by JP1/IT Desktop Management 2 andJP1/IT Desktop Management 2 - Agent must be set up to accept incoming traffic. For details about the port numbers, see A.3 Port number list.

Network connection environment

The following describes the network connection environment for each system component.

For the management server:

The server must be connected to a wired LAN network.

For a computer on which the network monitor is enabled:

The computer must be connected to a wired LAN or a wireless LAN network. Note, however, that if the communication environment has been degraded, it might not be possible to block devices connected to a wireless LAN from the network. Therefore, we recommend that you connect the computer to a wired LAN network.

For a computer on which an agent has been installed:

The computer must be connected to a wired LAN, wireless LAN, WAN, or VPN network. Note, however, that devices connected to a wireless LAN cannot be turned off by using the power-off function. For details about power control, see 2.6.3 Controlling devices.

For an agentless computer:

The computer must be connected to a wired LAN, wireless LAN, WAN, or VPN network.

Network between the management server and managed computers

ICMP communication from the managed computers to the management server is required for optimum operation.

If ICMP communication from the management server to the managed computers is not possible, any operation attempted from the management server for a managed computer (such as software installation, message notification, and acquisition of the latest device information) is performed when a polling from the agent occurs.

> **Tip**
>
> In a DHCP environment, even if an IP address is dynamically assigned to the computer, the same IP address will not be registered twice in JP1/IT Desktop Management 2.

Network between the management server and computers used for window operations

To use the operation windows of JP1/IT Desktop Management 2 on a computer other than the management server, an environment that allows HTTP communication via a Web browser is required.

Network with the Windows Firewall set

The following describes the settings required for each system component.

For the management server:

WhenJP1/IT Desktop Management 2 is installed in an environment in which the Windows firewall is enabled, the program is automatically allowed to pass the Windows firewall (registered as a firewall exception).

However, if the program was installed in an environment in which the Windows firewall was disabled, the program is not allowed to pass the firewall even if the Windows Firewall is subsequently enabled. In this case, execute the `addfwlist.bat` command on the management server to allow communication through the Windows Firewall. The executable file of the command is stored in the following folder.

JP1/IT Desktop Management 2 - Manager installation folder\mgr\bin\

For a computer on which the controller is installed:

When the controller is installed, it is automatically registered as a firewall exception. So, it can pass through the Windows firewall no matter whether the Windows firewall is enabled or disabled. No additional settings are required.

For a computer on which the agent is installed:

When the agent is installed, it is automatically registered as a firewall exception. So, it can pass through the Windows firewall no matter whether the Windows firewall is enabled or disabled. No additional settings are required.

For an agentless computer:

Add the TCP port (port number 445) to the Windows firewall exception list.

Related Topics:

- 4.2.7 Prerequisites for agentless management

4.3 Prerequisites for functions

Related Topics:

- 4.3.1 Device management prerequisites
- 4.3.2 Network monitor prerequisites
- 4.3.3 Prerequisites for remote control
- 4.3.4 Security control prerequisites
- 4.3.5 Prerequisites for acquiring operation logs
- 4.3.6 Asset management prerequisites
- 4.3.7 Prerequisites for the distribution function
- 4.3.8 Prerequisites for reports

4.3.1 Device management prerequisites

Device management requires the management target devices to be connected to the network. To display devices in an operation window of JP1/IT Desktop Management 2, they must be added as management targets by using one of the following methods.

- Install the agent on the computer (the devices are automatically added as management targets).
- Perform a device search and then add the discovered devices as management targets.
- Use network monitoring and then add the discovered devices as management targets.

When you add a device that uses both IPv4 and IPv6 IP addresses as a management target, use only the IPv4 addresses.

Devices having only IPv6 IP addresses can be added as the management targets by only searching for devices registered in Active Directory. In this case, however, you can manage only the existence of the devices.

Related Topics:

- 4.2.3 Prerequisites for a computer on which an agent will be installed

4.3.2 Network monitor prerequisites

Installing the network monitor requires a computer that monitors the network. Provide one online managed computer for each network segment in which you want to install the network monitor, and then enable the network monitor on that computer.

In addition, do not clear the following check boxes in the **Basic settings** in the agent configurations assigned to the computer that monitors the network.

- **Communicate with the higher system**
- **Periodically notify the higher system of the information collected from the computer.**

The network monitor takes effect as long as the agent is running. Therefore, the computer with the network monitor enabled must be running during the time that you want to monitor the network.

Tip

We recommend that you enable the network monitor on a 24-hour computer to consistently monitor the network.

Important note

A computer that monitors the network (online managed computer with the network monitor enabled) accepts connections even from devices that have been blocked from the network due to, for example, insufficient security measures. Therefore, do not configure a mission-critical server, such as a file server, as the computer that monitors the network.

4.3.3 Prerequisites for remote control

The following describes the prerequisites needed to remotely control computers.

Prerequisites for the administrator's computer

The controller, which is a program that remotely controls other computers, must be installed on the administrator's computer. The controller accesses a window of a computer subject to remote control and allows the administrator to perform window operations.

When remote control is started in an operation window, the controller is automatically installed on the computer that displays the operation window.

Prerequisites for the connection destination computer

The conditions required for the connection destination computer vary depending on the method for connecting the controller.

Standard connection

The agent must be already installed and the remote control agent must be running. The remote control agent is a remotely controlled program, and provides the controller with a window on the controlled computer and performs operations in that window according to the instruction from the controller.

The remote control agent is part of the agent program. When the agent is installed, the remote control agent is also installed if you select the remote control agent in the **Components to Install** dialog box.

The remote control agent can be used in JP1/IT Desktop Management 09-50 or later or JP1/IT Desktop Management 2 10-50.

RFB connection

The RFB connection allows the remote control function to be used in agentless mode, that is, without using the remote control agent. However, the RFB connection restricts the remote control function.

To use the RFB connection, one of the following conditions must be satisfied.

- Software providing the VNC server function (for example, the following software) is running.
  - Intel v Pro (if KVM Remote Control is available on a computer on which AMT 6.0 or later is installed)
  - Realness
  - Ultraviolet
  - Firmware Workstation
- The OS is Mac OS X and Apple Remote Desktop Service is running.

Important note

For remote control using the RFB connection, operation is not always guaranteed because a controlled computer might be configured by using free software. Some functions might not be available. Therefore, we recommend that you use a trial version in advance to confirm and verify operation. Note that we do not support any questions about environment setup, specifications, setting methods, and errors related to the controlled hardware or programs using the RFB connection.

Important note

The remote control function of JP1/Remote Control or JP1/Software Control cannot be connected to.

Related Topics:

- 2.7.2 Remote control features
- 2.7.9 Using the remote control feature in NAT and DHCP environments

4.3.4 Security control prerequisites

To perform security control, an agent must be installed on each of the computers subject to security control. For offline managed computers, acquisition of device information must be completed.

The following describes the prerequisites to use the security control functions.

Prerequisites to manage the application of updated programs:

All the following conditions must be satisfied:

- A support services contract has been made.
- MSXML 4.0 Service Pack 2 or MSXML 6.0 is installed.

Prerequisites to determine whether anti-virus products are installed

There are no prerequisites to determine whether anti-virus products are installed.

To check whether anti-virus products are installed, you only have to check whether anti-virus products supported by JP1/IT Desktop Management 2 are installed on the target computer.

Tip

To check whether an anti-virus product not supported byJP1/IT Desktop Management 2 is installed, add that anti-virus product as mandatory software.

Prerequisites for using the suppression functions

Function	Prerequisites
Suppressing startup of the software	The combined length of the file name and folder name of the target software must be less than 260 characters.
Suppressing printing	In the properties for each printer, **Print** and **Manage Documents** must be allowed for all logged on users.#

For the network shared printer, the following prerequisites are added.

- The table below shows the supported combination of the agent and the print server.

Agent	Print server	Printing restriction
Windows XP/2003	Windows XP/2003	Y
Windows XP/2003	Windows Vista or later	Y
Windows Vista or later	Windows XP/2003	N
Windows Vista or later	Windows Vista or later	Y
Any	Others	N

  Legend: Y:Printing can be restricted for this type of printer. N:Printing cannot be restricted for this type of printer.

- RPC communication must be possible between the print server and the agent PC. If RPC communication is not possible, the problem might be caused by one of the following:
  - The print server is a server based on the Internet Printing Protocol (IPP).
  - A firewall, proxy or NAT is present between the print server and the agent PC.
  - The agent PC's Windows firewall is enabled and **File and Printer Sharing** is not set to **Exceptions**.
- The agent PC's **File and Printer Sharing for Microsoft Networks** must be enabled.
- The print server must be able to resolve the name of the agent PC.
- If the agent PC is Windows Vista or later, the agent PC and the print server must join the same domain, or the credential of the print server must be registered on the Credential Manager of the agent PC. The agent PC needs to reboot after registering the credential.

For details about prerequisites for suppressing the use of devices, see (1) Devices whose use can be restricted.

Related Topics:

- (14) Supported anti-virus products

4.3.5 Prerequisites for acquiring operation logs

To acquire operation logs, the agent must be installed on the computer from which you want to acquire operation logs.

Prerequisites for acquiring an operation log vary depending on the log type, as described in the following table.

Operation log type		Prerequisites
Computer operation	Start and stop of the computer	--
	Logon to and logoff from the OS	
Start and termination of the programs		The combined length of the file name and folder name for logged programs must be less than 260 characters.
File and folder operation	File and folder operation in the computer	--
	Upload to and download from the Web	Operation logs for the following Web browsers can be acquired: • Internet Explorer 7, 8, 9, 10, and 11[#1]

Operation log type		Prerequisites
File and folder operation	Upload to and download from the Web	• If your Web browser is Internet Explorer 10 or 11, the **Enable third-party browser extensions** check box must be selected on the **Advanced Settings** tab in the **Internet Options** dialog box. Note that this check box is cleared by default for Internet Explorer installed in Windows Server 2012, Windows Server 2008, or Windows Server 2003. • If your Web browser is Internet Explorer 10 or 11, the add-on for upload monitoring that is added to the user's computer must be enabled. • If your Web browser is Internet Explorer 10 or 11, the *JP1/IT Desktop Management 2 - Agent* add-on must be enabled in the list of add-ons displayed by selecting **Tools**, **Manage Add-ons**, and then **Toolbars and Extensions**.
	E-mail transmission and reception	Operation logs for the following mailers can be acquired: • Microsoft Outlook Express 6 • Microsoft Outlook 2002, 2003, 2007, 2010, and 2013 • Windows Mail 6 • Windows Live Mail 2009, 2011, and 2012
	Save of attached files	
	File transmission and reception	Operation logs for the following Web browsers can be acquired: • Internet Explorer 7, 8, 9, 10, and 11#1
Print operation		In the properties for each printer, **Print** and **Manage Documents** must be allowed for all logged on users.#2
Web access		• Operation logs for the following Web browsers can be acquired: • Internet Explorer 7, 8, 9, 10, and 11#1 • The **Enable third-party browser extensions** check box must be selected on the **Advanced Settings** tab in the **Internet Options** dialog box. Note that this check box is cleared by default for Internet Explorer installed in Windows Server 2012, Windows Server 2008, or Windows Server 2003. • The add-on for Web access monitoring that is added to the user's computer must be enabled. • In addition, JP1/IT Desktop Management 2 - Agent must be enabled in the list of add-ons displayed by selecting **Tools**, **Manage Add-ons**, and then **Toolbars and Extensions**.
Connection and disconnection of devices		--
Window operation		--

Legend: --: None

#1: Operation logs for Web upload, Wed download, file reception, and Web access can be acquired only for desktop Internet Explorer for which Enhanced Protected Mode is disabled.

#2: For the network shared printer, the following prerequisites are added.

- The table below shows the supported combination of the agent and the print server.

Agent	Print server	Collection of operation logs for print operations
Windows XP/2003	Windows XP/2003	Y
Windows XP/2003	Windows Vista or later	Y
Windows Vista or later	Windows XP/2003	N
Windows Vista or later	Windows Vista or later	Y
Any	Others	N

Legend: Y: Operation logs can be collected for this type of printer. N: Operation logs cannot be collected for this type of printer.

- RPC communication must be possible between the print server and the agent PC. If RPC communication is not possible, the problem might be caused by one of the following:
  - The print server is a server based on the Internet Printing Protocol (IPP).
  - A firewall, proxy or NAT is present between the print server and the agent PC.
  - The agent PC's Windows firewall is enabled and **File and Printer Sharing** is not set to **Exceptions**.
- The agent PC's **File and Printer Sharing for Microsoft Networks** must be enabled.
- The print server must be able to resolve the name of the agent PC.
- If the agent PC is Windows Vista or later, the agent PC and the print server must join the same domain, or the credential of the print server must be registered on the Credential Manager of the agent PC. The agent PC needs to reboot after registering the credential.

4.3.6 Asset management prerequisites

Prerequisites for managing smart devices by linking with the MDM system

Asset management requires iOS or Android to be installed on the smart devices to be managed by linking with the MDM system.

To suppress the use of some USB devices based on the security policy, you need an online managed computer to register non-suppression target USB devices as assets.

4.3.7 Prerequisites for the distribution function

To use the distribution function, the agent must be installed on the distribution-target computer.

To install the software, the installer must be an MSI file or EXE file that supports silent installation.

4.3.8 Prerequisites for reports

Prerequisites for displaying a report vary depending on the report type, as described in the following table.

Report type		Prerequisites
Summary Reports	Daily Summary	• The managed devices and asset information appropriate for the displayed information must be registered. • The number of days appropriate for the displayed period must have elapsed.
	Weekly Summary	
	Monthly Summary	
Security Diagnosis Reports	Current Diagnosis	• The managed devices must exist. • The security policy settings must be enabled.
	Timeframe Diagnosis	• The managed devices must exist. • The security policy settings must be enabled. • The number of days appropriate for the displayed period must have elapsed.

Report type		Prerequisites
Security Detail Reports	Violation Level Status	• The managed devices must exist. • The security policy settings for each report must be enabled.
	Windows Update Status	
	Antivirus Software Status	
	Mandatory Software Status	
	Unauthorized Software Status	
	Security Settings Status	
	Other Access Restrictions Top N	
	User Activity Top N	
Inventory Detail Reports	Device Management Status	The managed devices must exist.
	Green IT (Power Saving Settings)	
Asset Detail Reports	Hardware Assets	The hardware asset information must be registered.
	Hardware Assets Cost	The hardware cost must be specified in the contract information.
	Software License Cost	The software cost must be specified in the contract information.
	Software (License Violation)	The management software information and software license information must be registered.
	Software (Surplus License)	

4.4 Examining the system configuration

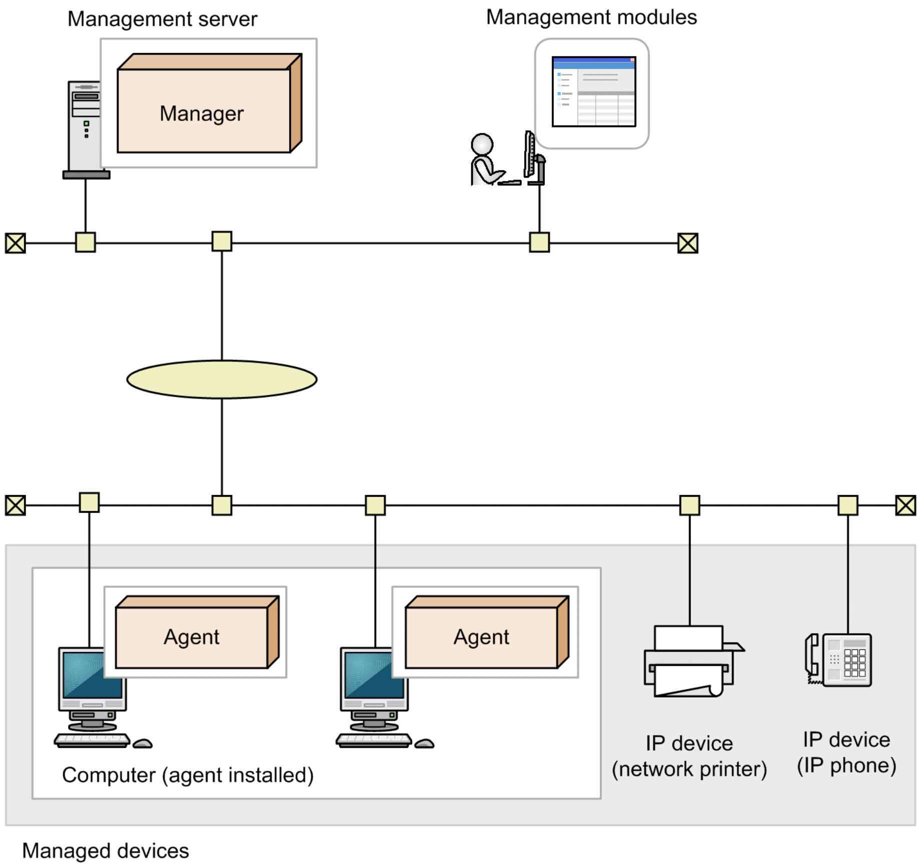
Consider the configuration of the system to be set up. You must select a configuration appropriate for the purpose of the system. The following table describes the types of system configurations that can be set up by using JP1/IT Desktop Management 2.

For system configuration with the asset management server (Asset Console), see the description on the system configuration in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Planning and Configuration Guide*.

System configuration type	Features
Minimum configuration	This configuration consists of the management server and managed devices only.
Basic configuration	This configuration includes a relay system to disperse the load on the management server and network when utilizing Remote Installation Manager for distribution.
Offline management configuration	This configuration contains managed computers that cannot be connected to the network of the management server. This configuration allows you to manage device information for standalone computers and computers that are connected only to the network in a site.
Agentless configuration	This configuration contains agentless computers to be managed.
Support service linkage configuration	This configuration provides a linkage with support service sites. You can download support information files from support service sites to the management server, and apply the latest information about Windows updates. You can also apply the latest Windows updates to the managed computers.
Active Directory linkage configuration	This system configuration is used to collect device information managed by Active Directory. The information collected from Active Directory can be registered on the management server.
MDM linkage configuration	This configuration provides a linkage with an MDM system so that JP1/IT Desktop Management 2 can perform integrated management of devices, including the smart devices managed by the MDM system.
Network monitoring configuration	This configuration provides network monitoring to control network connections of devices. Network connection control of devices is possible if the network monitor agent is installed for the managed computers.
JP1/NETM/NM - Manager linkage configuration	By linking with JP1/NETM/NM - Manager, JP1/IT Desktop Management 2 can control network connections monitored on network control appliance products with JP1/NETM/NM installed.
Remote control configuration	This configuration provides remote control of computers by using the remote control function. File transfer and chatting between computers are also possible.
JP1/IM linkage configuration	This configuration provides a linkage with JP1/IM to allow JP1/IM to perform integrated management of error events generated by JP1/IT Desktop Management 2. Integrated management of information for other linked JP1 products is also possible, allowing you to timely check the information.
Cluster configuration	This system configuration contains a cluster of management servers. If an error occurs on the primary management server, the primary management server is switched to the standby management server on which processing can continue.

4.4.1 Minimum configuration

The following describes the minimum configuration of a system that is set up for JP1/IT Desktop Management 2. The minimum configuration consists of one management server and the managed devices. The following figure shows the minimum configuration:



Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Agent: Agent

The management server diagnoses the security status of the computers according to the specified security policy. Use the operation window to set the security policy and check the security diagnostic results. Use the Web browser to display and use the operation window. In an environment that allows access to the management server from the Web browser, you can log in and use the operation window.

The following describes the prerequisites for the minimum configuration:

- The computers to be managed must be connected to one management server.
- In an environment that allows TCP/IP communication, a computer can be added as a management target irrespective of whether a LAN or WAN is used.
- Because the operation window is used in a Web browser, you can use the operation window on any computer that is available for HTTP communication with the management server.

4.4.2 Basic configuration

A configuration set up for distribution by using Remote Installation Manager with a relay system installed is called a basic configuration. Installing a relay system can reduce loads on the network and the management server.

The following is a guideline for installing a relay system:

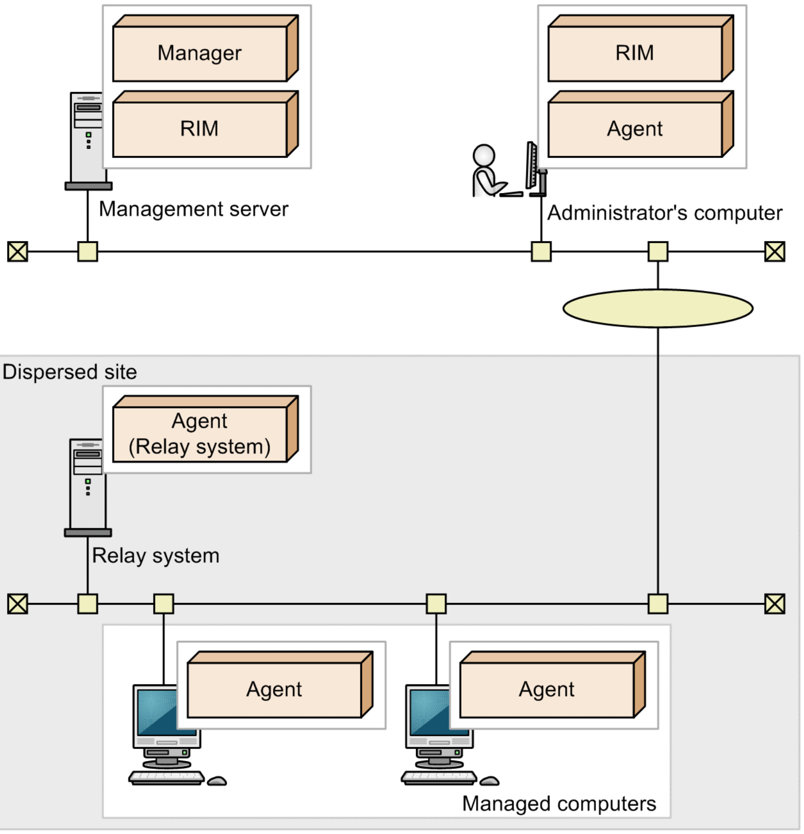
- A relay system is provided for each dispersed site.
- A relay system is provided for 1,000 managed computers.

To configure a relay system, create a dedicated agent configuration and assign the configuration to the relay system. For settings of the agent configuration dedicated to the relay system, see items in (4) Agent parameters.

Tip

You can distribute files by using Remote Installation Manager without installing a relay system. However, we recommend using one or more relay systems to prevent placing excessive load on the network.

The following figure shows the basic configuration.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager
RIM: Remote Installation Manager
Agent: JP1/IT Desktop Management 2 - Agent installed as an agent
Agent (Relay system): JP1/IT Desktop Management 2 - Agent installed as a relay system

Distribution to the managed computers in a dispersed site is executed when polling from the relay system occurs.

Settings required in a NAT environment

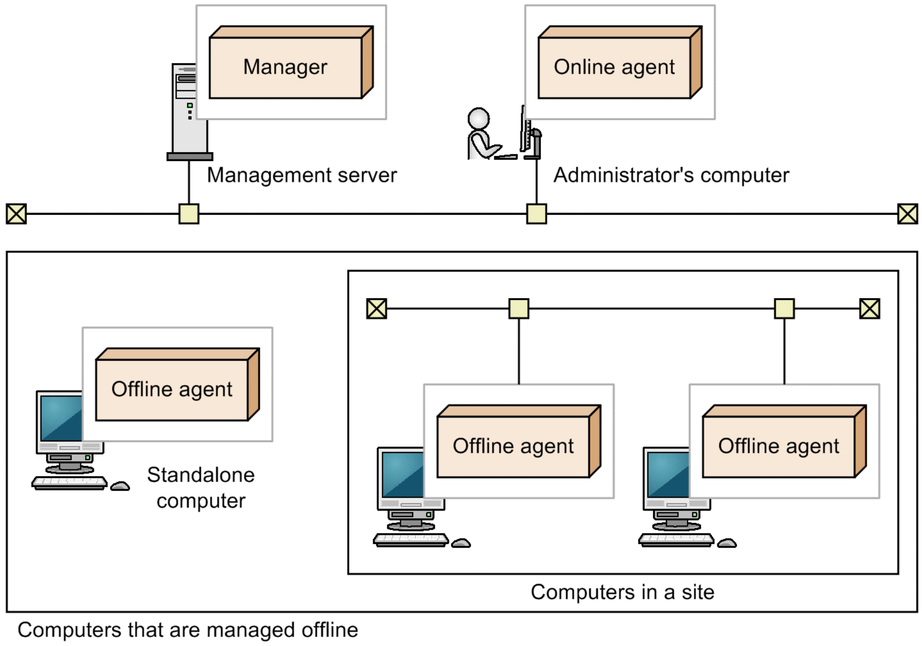
Important note

Network devices located in a dispersed site and agentless devices cannot be managed in a NAT environment.

In the agent configurations for a relay system and agent to be installed on a computer in a dispersed site, specify the management computer to be connected by the global IP address or the host name. If you use the host name, the IP address resolved by using the DNS server or a hosts file must be a global IP address.

4.4.3 Offline management configuration

You can manage computers that cannot be connected to the network of the management server, such as standalone computers and computers in a site. A configuration that contains offline managed computers is called the offline management configuration. The following figure shows the offline management configuration.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager

Online agent: Agent for online management

Offline agent: Agent for offline management

Although the system configuration in this figure consists of only computers on which agents are installed, the configuration can also contain agentless computers.

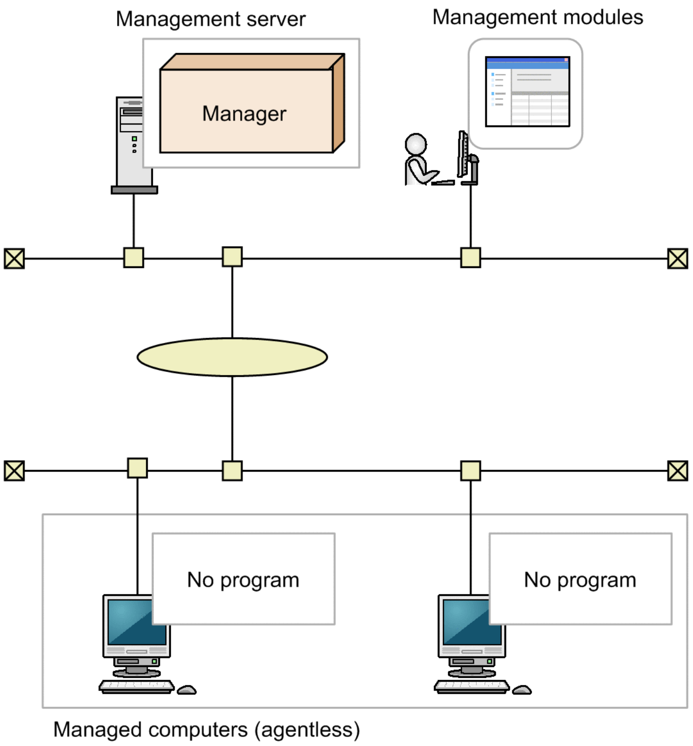
The offline management configuration requires that the online management agent is installed on the administrator's computer. The reason is that, to add offline managed computers as the management targets, device information for the target computers must be collected by using external media and then be reported to the management server from the online management agent.

Important note

There are functional differences between an offline managed computer and an online managed computer. For details, see (1) Functional differences between agent/agentless management.

4.4.4 Agentless configuration

You can manage computers without agents installed, in addition to computers on which agents are installed. A configuration that contains agentless computers is called the agentless configuration. The following figure shows the agentless configuration.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager

Although the system configuration in this figure consists of only agentless computers, the configuration can also contain both agentless computers and computers with agents installed.

The following describes the prerequisites for the agentless configuration.

- The computers that the management server can directly reference by using the search function are applicable to the agentless configuration. The search function searches for the management target devices connected to the network.
- Either of the following types of authentication must be possible.
  - Set the administrative share for the OS on the managed computers so that JP1/IT Desktop Management 2 can authenticate the logon account for the OS.
  - Managed computers can be authenticated by SNMP.

For prerequisites for managing agentless computers, see 4.2.7 Prerequisites for agentless management.

Important note

There are functional differences between an agentless computer and a computer on which the agent is installed. For details about the functional differences, see (1) Functional differences between agent/agentless management.

4.4.5 Support service linkage configuration

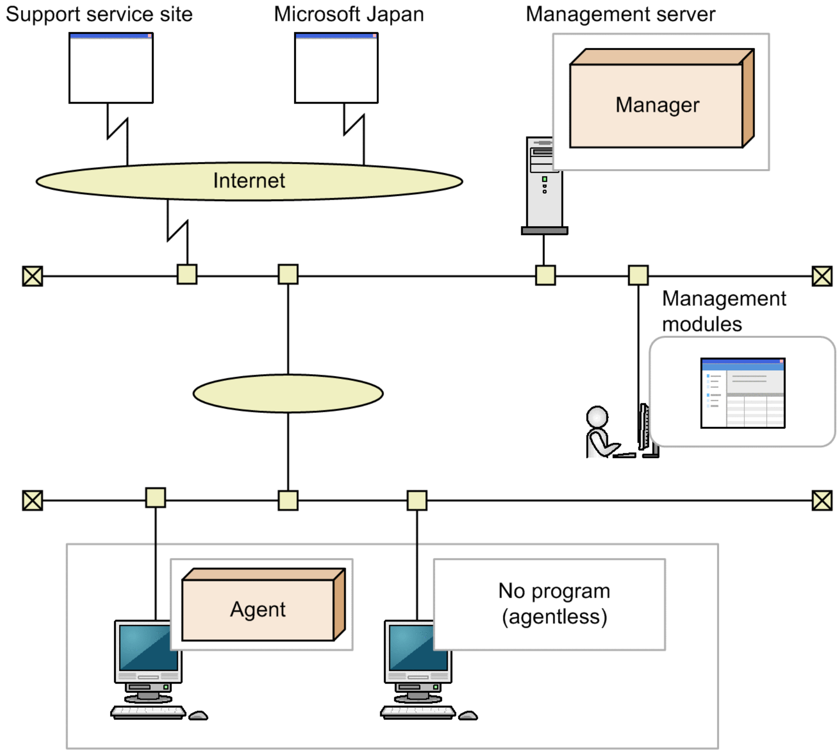
You can download the latest support information file from the support service site and apply the latest Windows updates to the security policy judgment items registered on the management server. You can also automatically download the

Windows updates from the Microsoft Web site and apply them to the managed computers. This configuration is called the support service linkage configuration.

Tip

A support services contract must be made before you can use the support service linkage configuration.

The following figure shows the support service linkage configuration.



Managed computers

Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Agent: Agent

You can use Windows update files to distribute the Windows updates to computers. In an environment that allows Internet connection with the Microsoft Web site, Windows updates are automatically downloaded and a package is created.

The management server automatically updates the Windows update information on a regular basis, that is, once a day (every 24 hours).

In the support service linkage configuration, the management server connects to the support service site and the Microsoft Web site via the Internet. Therefore, confirm that the management server is able to connect to the Internet. For details about other system features and prerequisites, see 4.4.1 Minimum configuration.

Tip

Even in an environment in which the management server is disabled for Internet connection, you can manage Windows update information. In this case, an Internet-connectable computer other than the management server acquires the support information file from the support service site, and then uploads it to the management server.

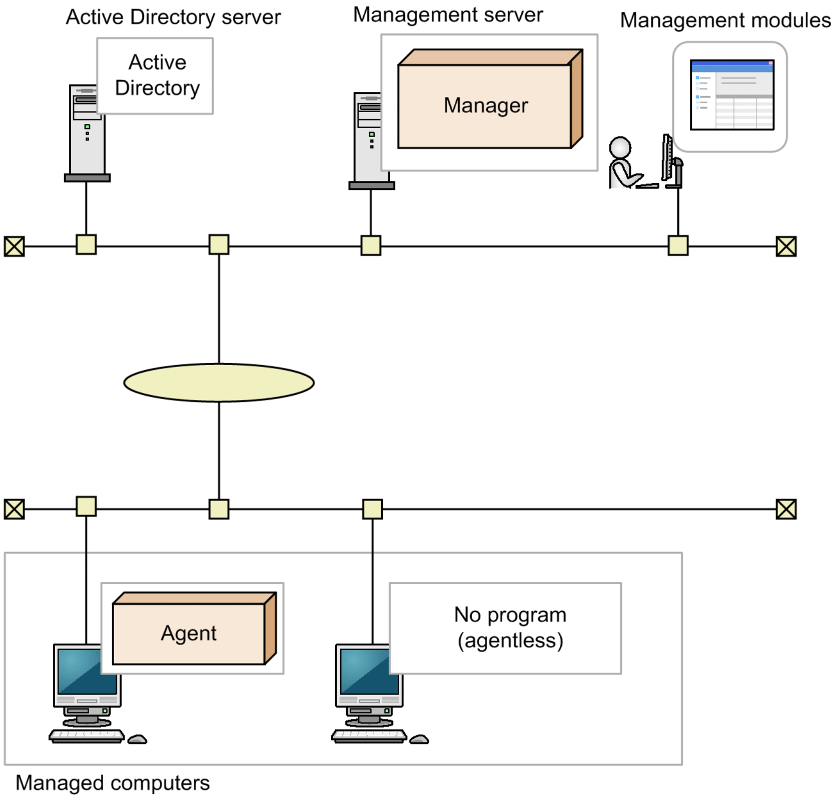
This computer also downloads the executable file for the Windows updates to be distributed from the Microsoft Web site, and then uploads the executable file to management server.

4.4.6 Active Directory linkage configuration

JP1/IT Desktop Management 2 can link with Active Directory so that the information managed by Active Directory can be collected as device information. To link with Active Directory, one of the following OSs is required on the Active Directory server.

- Windows Server 2008
- Windows Server 2003

The following figure shows the Active Directory linkage configuration.



Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Agent: Agent

After you have set up the environment for the Active Directory linkage configuration, use the **Active Directory** view of the Settings module to set the linkage with Active Directory. If necessary, specify the information that is to be acquired as additional device information.

Tip

Multiple Active Directory domains can also be linked so that JP1/IT Desktop Management 2 can perform integrated management of the information managed by multiple domains. There is no restriction on the number of Active Directory domains that can be linked.

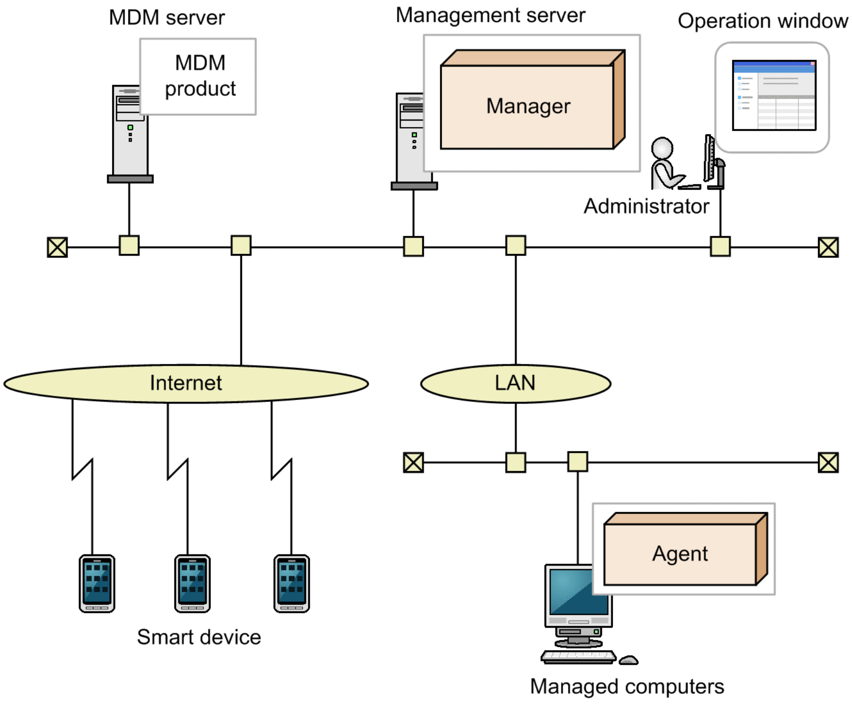
4.4.7 MDM linkage configuration

JP1/IT Desktop Management 2 linked with an MDM system provides integrated management of devices and assets, including the smart devices managed by the MDM system.

The following MDM systems can be linked.

Product	Version
MobileIron	5.8, 5.9

The following figure shows the system configuration that links an MDM system to manage smart devices.



Legend:

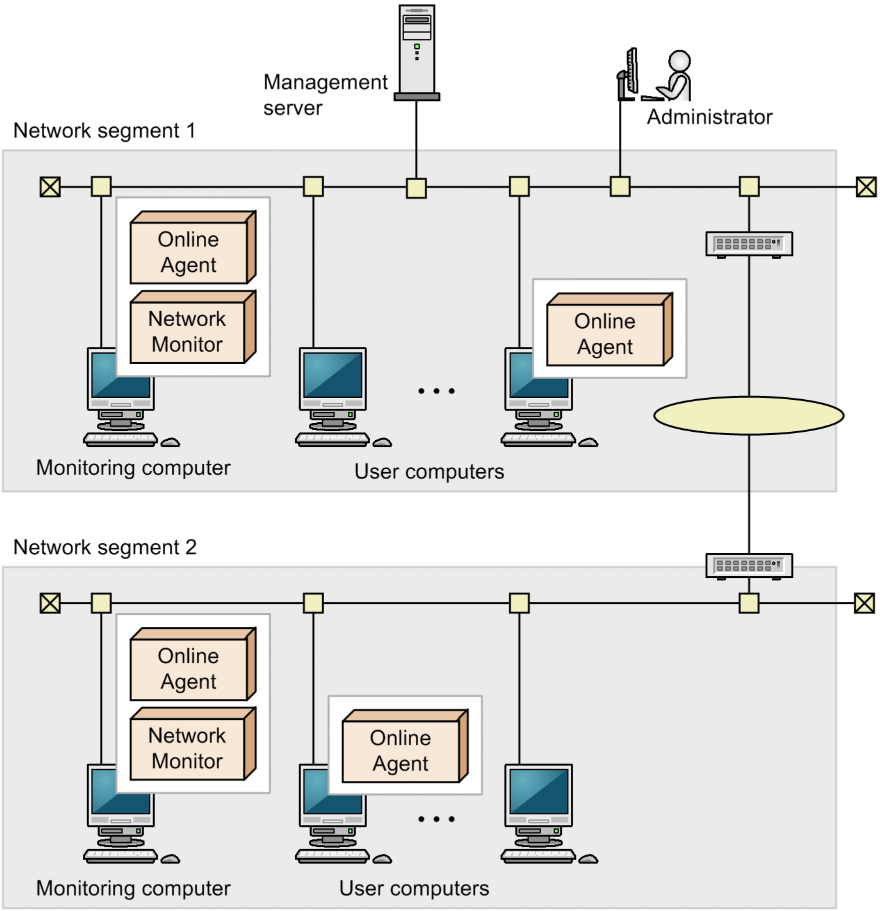
Manager: JP1/IT Desktop Management 2 - Manager
Agent: Agent

After you have set up the MDM linkage configuration, use the **MDM Linkage Settings** view of the Settings module to set the MDM linkage. When the setting is completed, information about smart devices is acquired from the MDM system according to a schedule. The smart devices whose information has been acquired are handled as discovered devices, which can be added as the management targets of JP1/IT Desktop Management 2.

If smart device information is updated in the MDM system, the information in JP1/IT Desktop Management 2 is also updated when the smart device information is acquired. Therefore, when linking the MDM system, we recommend that you set the schedule to acquire information on a regular basis.

4.4.8 Network monitoring configuration

You can monitor the network to control network connection for devices. You can also automatically block the network connections of computers which are determined to have insufficient security measures. The following figure shows a system configuration in which network monitoring is used.



Legend:

Online Agent: Agent used for online management
Network Monitor: Network monitor agent

To monitor the network, you must install an online managed computer with the network monitor enabled (computer that monitors the network) for each network segment.

Do not clear the following check boxes in the **Basic settings** in the agent configurations assigned to the computer that monitors the network.:

- **Communicate with the higher system**
- **Periodically notify the higher system of the information collected from the computer**

In the **Network List** view of the Device module, select one computer for each network segment group (for each broadcast domain), and then enable the network monitor.

Important note

When you use the network monitor, NX NetMonitor and JP1/NETM/NM cannot be used with JP1/IT Desktop Management 2. Before using the network monitor, you must first uninstall any instances of NX NetMonitor and JP1/NETM/NM from the computers within the network segment.

Tip

When you enable the network monitor for a computer, the network monitor agent is installed on that computer.

You can also install JP1/IT Desktop Management 2 - Network Monitor on the online managed computer from the distribution media, and then enable the network monitor.

If the network monitor is enabled, a computer that is newly connected to the network is automatically discovered, and network connections within the network segment are controlled according to the network monitor settings. Note that the network monitor can be enabled on only one computer in a network segment.

Tip

Ensure that the computer with the network monitor enabled is running 24 hours a day. While the computer is turned off, the network monitor cannot control network connection nor discover devices.

Tip

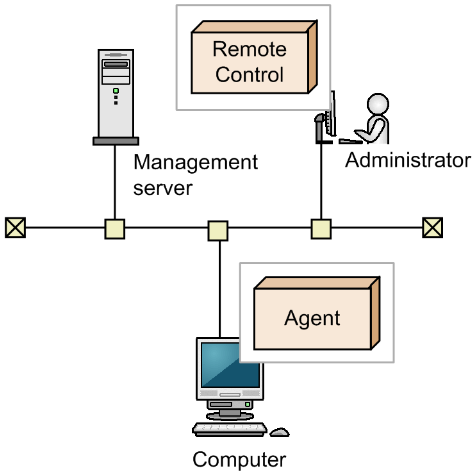
You can join multiple VLANs (Virtual LANs) by using the VLAN trunk connection function to monitor multiple subnetworks (VLANs) on a single computer (and a single network card), provided that the following prerequisites are satisfied.

- The network card of the computer that monitors the network supports EEE 802.1Q (VLAN).
- Tagged VLAN and trunk connection (passing multiple VLANs) can be set on the port of the switch to which the computer that monitors the network is connected.

4.4.9 Remote control configuration

An administrator can connect to and operate remote computers.

The following figure shows a remote control configuration.



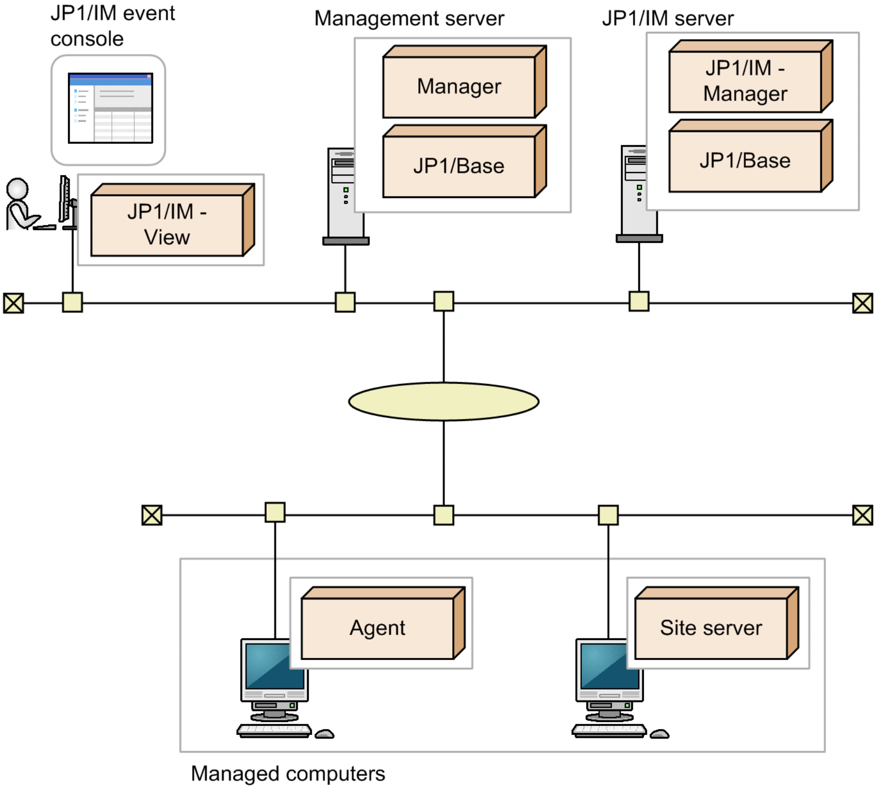
Legend:

Agent: JP1/IM Desktop Management - Agent
Remote Control: Controller

The computer that connects to remote computers requires a controller. When you click the **Remove Control** button in the Device module, the controller is automatically installed on the computer.

4.4.10 JP1/IM linkage configuration

This system configuration allows you to link with JP1/IM. This allows JP1/IM to manage, as JP1 events, error events generated in managed computers and severe events that require the intervention of the administrator. The following figures show JP1/IM linkage configurations.



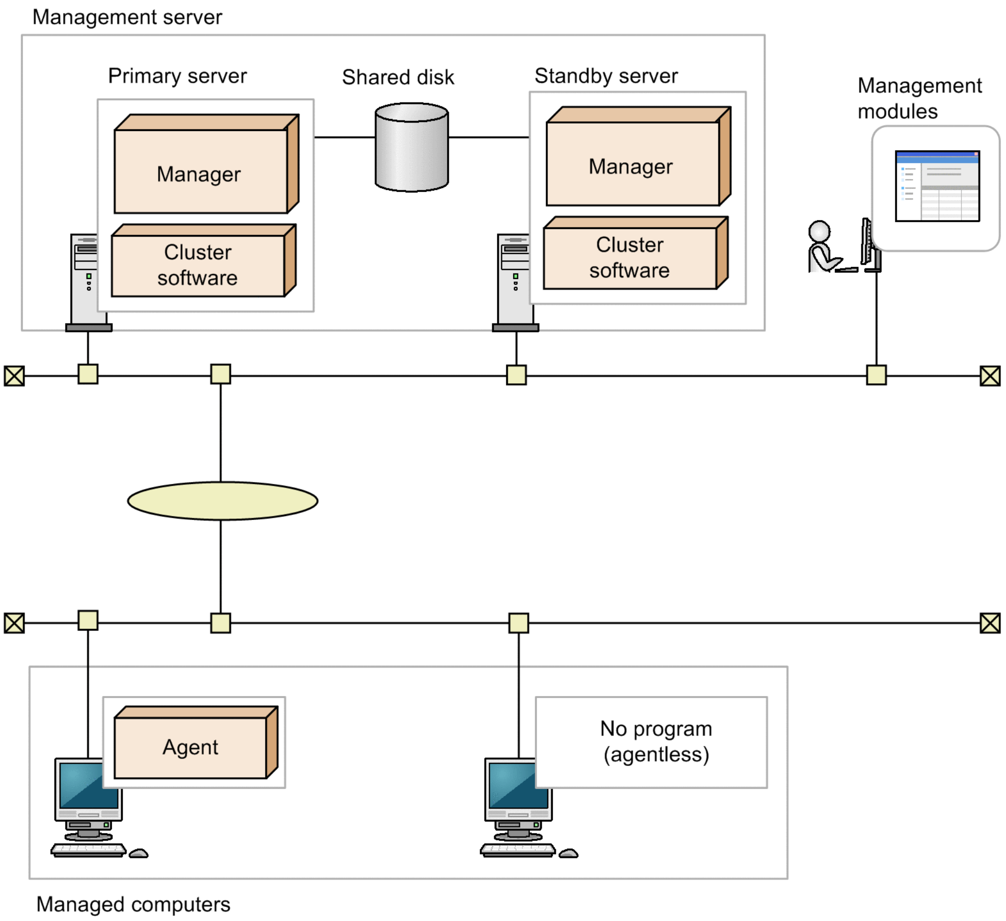
Legend:
Manager: JP1/IT Desktop Management 2 - Manager
Agent: JP1/IT Desktop Management 2 - Agent

The JP1/IM linkage configuration requires JP1/IM and JP1/Base.

During setup of the JP1/IM linkage configuration, you must define the configuration file and the definition file for the extended event attributes.

4.4.11 Cluster configuration

The management server can be configured in a cluster configuration, which consists of a running server (called the primary server) and a standby server. If an error occurs in the primary server, processing is passed to the standby server via a shared disk. The cluster configuration of a server allows processing to continue even if an error occurs in the primary server. The following figure shows a cluster configuration:



Legend:

Manager: JP1/IT Desktop Management 2 - Manager
Agent: Agent

The following describes the prerequisites for a cluster configuration.

- The usable cluster software programs are Windows Failover Cluster Server.
- On the managed computers, specify the logical network name and logical IP address in the connection-destination management server settings. By doing so, the computers do not need to identify the management server they are connected to.

Important note

A network monitor cannot be configured in a cluster configuration.

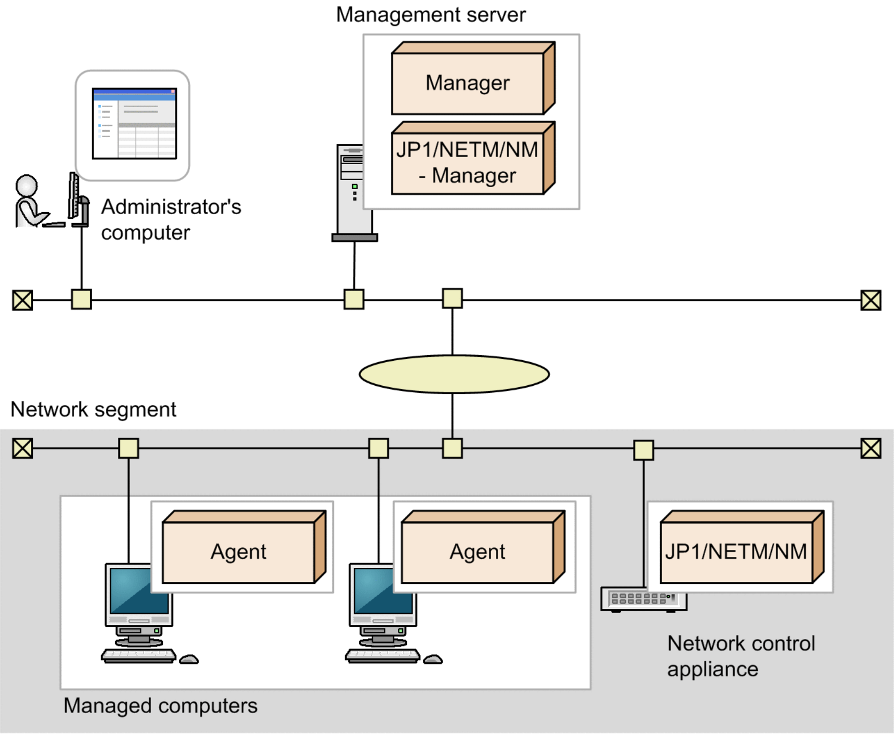
4.4.12 JP1/NETM/NM - Manager linkage configuration

By linking with JP1/NETM/NM - Manager, JP1/IT Desktop Management 2 can control network connections monitored on network control appliances.

Important note

You cannot place a network control appliance in a network segment with the network monitor enabled.

The following figure shows a JP1/NETM/NM - Manager linkage configuration.



Legend:

Manager: JP1/IT Desktop Management 2 – Manager
Agent: JP1/IT Desktop Management 2 - Agent

4.5 Examining the database

JP1/IT Desktop Management 2 uses a database to manage information necessary for management, including the information collected from managed devices and information calculated for reports.

The database is created during setup of an environment. Estimate the required database size in advance according to the system configuration and operation method, and provide the appropriate environment.

> **Tip**
>
> After starting operation, you can use the database manager to back up and restore the management server database and to perform maintenance for efficient use of the database.

Related Topics:

- 4.5.1 Database overview
- 4.5.2 Maximum disk space requirements for the management server
- 4.5.8 Guidelines for recommended disk space
- 4.5.4 Guidelines for disk space requirements for the operation log database
- 4.5.3 Guidelines for disk space requirements for operation log backup folder

4.5.1 Database overview

JP1/IT Desktop Management 2 has multiple database folders and data storage folders according to the type.

The destination of each folder can be specified when you set up the management server.

The following table lists and describes the folders.

Folder type	Description	Created?
Database folder	A folder in which a database area is created for storing management information, including device information, asset information, security policies, events, and reports	Yes
Data folder	A folder that stores data, such as the registered agents and packages created by the distribution function	Yes
Local data folder	A folder used as a management server temporary folder during operation	Yes
Operation log backup folder	A folder for saving backed-up operation log data. When you restore operation logs in the operation window, the data in this folder is stored in the operation log database folder, which allows you to reference past operation logs.	C
Operation log database folder	A database area that stores operation log data, from which you can view operation logs collected from computers. Automatically restored operation logs and manually restored logs are stored.	C
Revision history output folder	A folder to which revision histories are output periodically for archival purposes.	C
Database extraction folder	A folder for temporarily saving data when the database folder is changed. This folder is not used during normal operation	Yes

Legend: Yes: Always created, C: Created depending on the setting

Tip

Only the local disk on the management server can be specified for the folders. Note, however, that for the operation log backup folder, a network folder can be specified in addition to the local disk. Therefore, we recommend that you use large-capacity storage for the operation log backup folder and use a hard disk on the management server for other folders. Also note that you cannot specify a storage device that is identified as a removable disk.

4.5.2 Maximum disk space requirements for the management server

The following describes the maximum disk space requirements for data folders on the management server.

In addition to the disk space shown in the table below, we recommend that you allocate 1 GB of free space to a local data folder for use as a work folder during operation. To acquire operation logs, you need to add 500 MB of disk space for 5,000 managed computers. AlthoughJP1/IT Desktop Management 2 uses information not covered in the following table, such information requires a relatively small space and therefore has little influence on the estimate.

Data folder	Saved data	Storage period	Maximum space
Database folder	The following information used by the management server: • Security policy • Group • Agent settings	Stored until deleted.	0.5 GB
	The following asset information: • Hardware asset information • Managed-software information • Software license information • Contract information	Stored until deleted.	5 GB Actually, the disk space might exceed 5 GB because the folder size increases with the number of registered items. We also assume that the following information items have been registered, each item has no additional management items, and many large files are not registered. To register many large files to be managed, allocate sufficient free space separately. • Hardware asset information: 20,000 items • Managed-software information: 500 items • Software license information: 100 items • Contract information: 100 items
	Device information for managed devices	Stored until deleted.	10 GB This is based on the assumption that 10,000 devices are managed.
	Revision history	Stored until the used disk space reaches the maximum. If the maximum space is exceeded, entries are deleted beginning from the oldest.	Approximately 7 GB This is based on the assumption of a system with 10,000 managed devices, in which the number of device information changes recorded daily per device is the total of the following: • Number of changes recorded in day-to-day operation: 14

Data folder	Saved data	Storage period	Maximum space
Database folder	Revision history	Stored until the used disk space reaches the maximum. If the maximum space is exceeded, entries are deleted beginning from the oldest.	• Number of invalid changes: 0.1 (one invalid change per device in 10 percent of devices)
	Events	Stored until the used disk space reaches the maximum. If the maximum space is exceeded, events are deleted, beginning from the oldest.	(250 x 10,000 licenses owned + 10,000) x 1.5 KB = Approximately 4 GB This is based on the assumption that the following conditions exist: • 250 events are generated for one managed device per day • The number of owned licenses (managed devices) is 10,000. • 10,000 events are generated per day irrespective of the number of managed devices. • One event requires 1.5 KB of disk space.
Reports for the specified storage period	Stored for the specified number of years (from 1 to 10) as the storage period.	10 GB This is based on the assumption that reports are stored for 10 years.	Approximately 10 GB This is based on the assumption that 1,000 10 MB packages are registered.
Data folder	Packages used by the distribution function	Stored until deleted.	
	Temporary storage data of operation logs	Stored until the data is stored in the operation log backup folder.	Approximately 150 GB Required for acquiring operation logs. This is based on the assumption that the following conditions exist, and when operation log backup to the backup folder has not been performed for 2 weeks (5 business days per week): • Number of managed computers: 10,000 • All the operation logs are acquired. • Periodic export of the operation logs are not performed.
Operation log database folder	Operation logs when only operations closely related to information leakage are logged (automatically restored operation logs)	Operation logs are stored for a period specified in the **Period for storing automatically restored operation logs** field under **Operation Log Settings** in the Settings module.	Approximately 15.3 GB This is based on the assumption that the following conditions exist: • Number of managed computers: 10,000 • The amount of operation logs per computer per day is 80 KB. • 1 month (20 business days per month) of operation logs are acquired.
	Operation logs when all operations are logged (automatically restored operation logs)	Operation logs are stored for a period specified in the **Period for storing automatically restored operation logs** field under **Operation Log Settings** in the Settings module.	Approximately 297 GB This is based on the assumption that the following conditions exist: • Number of managed computers: 10,000 • The amount of operation logs per computer per day is 1.52 MB. • All the operation logs are acquired. • 1 month (20 business days per month) of operation logs are acquired.
	Operation logs restored from the backup folder for reference in the operation log list	Stored until deleted.	Approximately 17.9 GB This is based on the assumption that the following conditions exist: • The amount of operation logs per computer per day is 1.52 MB.

Data folder	Saved data	Storage period	Maximum space
Operation log database folder	(manually restored operation logs)	Stored until deleted.	• All the operation logs are acquired. • 3 months (3 x 20 business days) of operation logs for 200 computers are acquired.
Operation log backup folder	Backed up operation logs	These logs are stored until deleted when the operation log backup folder is specified. If you attempt to reference the restored operation logs in the operation log list, they are restored in the operation log database folder, but the operation logs in the operation log backup folder are not deleted.	There is no space limitation. Prepare a backup folder by referring to the value obtained as follows: Storage period (days) defined by the administrator x number of managed computers x 70 (KB per day per device). This is based on the assumption that the following conditions exist: • All the operation logs are acquired. • Periodic export of the operation logs is not performed.
Revision history output folder	Archived revision history	When you enable output of the revision history archive, revision histories are output to this folder as CSV files at regular intervals.	Approximately 10 GB This is based on the assumption that 10,000 devices are managed, and the revision history archive spans five years.

Related Topics:

- A.6 Performance and Estimates

4.5.3 Guidelines for disk space requirements for operation log backup folder

The following table shows the guidelines for disk space requirements for storing operation logs for one year in the backup folder.

Number of managed computers	Required disk space (GB)	
	Operation log data	CSV file output by the periodic export operation
500	8	75
1,000	16	151
2,000	32	302
5,000	80	754
10,000	160	1,509
30,000	480	4,826

Note: One year is calculated as 240 days (20 business days per month).

Related Topics:

- A.6 Performance and Estimates

4.5.4 Guidelines for disk space requirements for the operation log database

Use the following formula as a guideline for estimating the disk space required for automatically restoring operation logs to the database.

When all the operation logs are acquired

Number of managed computers x Period for storing automatically restored operation logs (days)# x 1.52 (MB) = Disk space required for automatic restoration (in MB)

#: The period for storing automatically restored operation logs is 300 days at maximum.

However, if the disk space required for automatic restoration is less than Period for storing automatically restored operation logs (days) x 1.5 (GB), the guideline for the disk space should be Period for storing automatically restored operation logs (days) x 1.5 (GB).

The following shows a guideline for the disk space required when the number of automatically restored operation logs is 100,000,000 and 300,000,000.

With 100,000,000 operation logs

54.7 GB

With 300,000,000 operation logs

161.0 GB

When the number of automatically restored operation logs is 100,000,000 and 300,000,000, the operation logs can be stored in the database for the following period.

Number of managed computers	Guideline for the number of days during which the operation logs can be stored	
	100,000,000 operation logs (54.7 GB of disk space)	300,000,000 operation logs (161.0 GB of disk space)
500	4 months	1 year
1,000	2 months	6 months
2,000	1 month	3 months
5,000	2 weeks	1 months
10,000	1 week	3 weeks
30,000	3 days	1 week

Note: A month is calculated as 20 business days.

Use the following formula for estimating the disk space required when you manually restore the operation logs.

When you manually restore the operation logs for 3 months for 200 managed computers

90 days x 1.5 (GB) = 135 (GB)

Related Topics:

- A.6 Performance and Estimates

4.5.5 Guidelines for disk space requirements in the data folder for acquiring operation logs

To acquire operation logs, you need to add the following disk space to the data folder.

Number of managed computers	Required disk space (GB)	
	When the periodic export is disabled	When the periodic export is enabled
5,000	75	106
10,000	150	213
30,000	448	637

Note: The table above calculates the disk space required to store 2 weeks (5 business days per week) of operation logs.

Related Topics:

- A.6 Performance and Estimates

4.5.6 Guidelines for disk space requirements for revision history archive

The table below lists the guidelines for estimating the disk space requirements when outputting a revision history archive.

The values in this table assume the following scenario:

- The revision history archive will span five years.
- Over the course of five years, approximately 100 changes will be recorded for each managed device.

Number of devices	Required disk space (GB)
10,000	Approximately 10
30,000	Approximately 30

4.5.7 Guidelines for disk space requirements for revision history database

The table below lists the guidelines for estimating the disk space requirements of the revision history database.

The values in this table assume that the number of device information changes recorded daily per device is the total of the following. If the number of changes is likely to exceed this number, make sure that enough disk space is available to meet the requirements.

- Number of changes recorded in day-to-day operation: 14
- Number of invalid changes: 0.1 (one invalid change per device in 10 percent of devices)

Number of devices	Required disk space (GB)
10,000	Approximately 7
30,000	Approximately 11

4.5.8 Guidelines for recommended disk space

The following describes the guidelines for the recommended disk space for all data (including operation logs) managed by JP1/IT Desktop Management 2. These guidelines vary depending on the types of operation logs to be acquired.

When all operations are logged

Number of managed devices	Recommended disk space (GB)#1				
	1 year#2	2 years#2	3 years#2	4 years#2	5 years#2
100	214	222	230	238	246
500	220	228	236	244	252
1,000	236	252	268	284	300
2,000	281	313	345	377	409
3,000	343	391	439	487	535
5,000	464	544	624	704	784
10,000	825	985	1,145	1,305	1,465
30,000	2,048	2,528	3,008	3,488	3,968

#1: The value is based on the assumption that a constant amount of data is generated per day, and the data is accumulated every day according to an assumed environment.

#2: Operation log storage period. For calculation of the amount of data, one year is handled as 240 days (20 business days per month).

When only operations closely related to information leakage are logged

Number of managed devices	Recommended disk space (GB)#1				
	1 year#2	2 years#2	3 years#2	4 years#2	5 years#2
100	205	206	206	207	208
500	206	206	207	207	208
1,000	207	208	209	210	211
2,000	209	211	213	215	217
3,000	212	215	218	221	224
5,000	216	221	226	232	237
10,000	284	294	304	314	325
30,000	334	365	395	426	457

#1: The value is based on the assumption that a constant amount of data is generated per day, and the data is accumulated every day according to an assumed environment.

#2: Operation log storage period. For calculation of the amount of data, one year is handled as 240 days (20 business days per month).

The following table describes the assumed environment used for calculating the recommended disk space.

Item	Assumed environment
Device	• 100 types of groups, including department and location, are created. • The number of devices excluded from management is 15% of the number of managed devices. • 300 software products (installation software) are installed on one managed device. • One managed device has 300 Windows updates applied. • One managed device has 100 Windows updates that have not been applied yet.
Operation log	• If only operations closely related to information leakage are logged, 120 operation logs are acquired for one device. • If all operations are logged, 2,000 operation logs are acquired for one device. • 30 (days) is specified for **Period for storing automatically restored operation logs**. • Operation logs for 200 computers for 3 months (20 business days per month) are manually restored. However, if there are 100 managed computers, operation logs for 100 computers are manually restored. • Periodic export of the operation logs is not performed.
Asset	• The number of registered items of hardware asset information (excluding USB devices) is twice as many as the number of managed devices. • 100 items of hardware asset information (USB device) are registered. • 500 items of managed-software information are registered. • 100 items of software license information are registered. • 100 items of contract information are registered. We assume that many large files are not registered for each asset information item. To register many large files to be managed, allocate sufficient free space in addition to the disk space shown in the two tables above.
Distribution	10 GB of data is registered for packages.
Event	250 events are generated for one managed device per day.

Related Topics:

- A.6 Performance and Estimates

4.5.9 Acquiring operation logs when the connection destination of the agent is turned off

If a user performs an operation on a computer with the agent installed while the management server on which operation logs will be stored is turned off, operation logs are temporarily saved on the computer.

After that, when the management server is turned on, the operation logs saved on the computer are uploaded to the management server.

Important note

The operation logs for the number of days specified in the **Period for which prohibited operations and operation logs are kept on the user's computer** field under **Common settings for prohibited operations and operation logs** in the Security module can be temporarily stored on the computer. If the period expires, the operation logs are deleted, in the order of oldest to newest. Therefore, we recommend that you turn on the connection destination before old operation logs are deleted.

Tip

When the operation logs are acquired periodically, operation logs saved on the computer with the agent installed are also uploaded to the management server .

In addition, do not turn off the management server for a long period.

4.6 Analysis and Preparation before operation

Before starting system operation, examine the issues that must be specified during operation, including to whom a user account should be assigned, which devices should be managed, and how the managed devices should be grouped.

4.6.1 User account considerations

You need to carefully consider JP1/IT Desktop Management 2 user assignments. Specifically, consider for whom you will create user accounts and which permissions you will assign to the created user accounts.

You can assign appropriate permissions to a user account according to the purpose of the administrator who will use the account. The following describe which permissions should be assigned for the purpose of operation.

- To perform administrative operations by using JP1/IT Desktop Management 2:

  Assign system administrator permission.
- To add and edit a user account for JP1/IT Desktop Management 2:

  Assign user management permission.
- To view the managed information:

  No permissions need to be assigned (view permission is assigned by default).
- Assign tasks so as to limit the range of operations for JP1/IT Desktop Management 2 according to the tasks for which the administrators are responsible.

  There are five types of tasks: security control, asset management, device management, distribution management, and system configuration management.

In addition to permissions, an administration scope can also be assigned to a user account to limit that user to manage information only in that scope. Assign an administration scope if you do not want a user to change information outside the administration scope or if you want to divide management tasks by administration scope. By thus dividing work responsibilities among administrators, you can ensure efficient management of devices and hardware assets in the organization.

Tip

By creating multiple user accounts and assigning permissions according to the tasks of the users, you can ensure a proper division of responsibilities and effective internal controls among the administrators of a system.

Related Topics:

- 2.3.2 User account permissions
- 2.3.2 User account permissions
- 2.3.4 Task allocations for user accounts
- 2.3.5 Available operations by task allocation
- 2.3.6 Administration scopes for user accounts
- 2.3.7 Differences in operation windows when administration scopes are assigned
- 4.6.2 Creating user accounts for efficient internal controls

4.6.2 Creating user accounts for efficient internal controls

To provide efficient internal controls, you need to register user accounts to restrict the available functions according to the jobs of JP1/IT Desktop Management 2 users. The following table provides an example of a management structure that provides efficient internal controls.

Management structure	Role
System owner	Controls and manages the usage of the system in the organization. The system owner approves applications to use JP1/IT Desktop Management 2, but does not use JP1/IT Desktop Management 2.
User account manager	Manages JP1/IT Desktop Management 2 users. User management permission is assigned.
System administrator	Uses JP1/IT Desktop Management 2 to perform management tasks. System administrator permission is assigned.
Manager	Views managed information to check the management status of the organization. View permission is assigned.

In this structure example, only the user account manager can use JP1/IT Desktop Management 2 from the beginning. The system administrator and manager must apply to the system owner for the use of JP1/IT Desktop Management 2. When the system owner approves an application, the user account manager registers a user account with the necessary permissions assigned.

The following describes the basic procedure for registering a user account. By registering a user account in this way, whether the system is used in accordance with the task of the user can be determined objectively.

1. A user who wants to use JP1/IT Desktop Management 2 applies to the system owner.
   A system administrator who wants to perform management tasks or a manager who wants to view the managed information applies to the system owner for the use of JP1/IT Desktop Management 2.

2. The system owner approves the use of the product.

3. The system owner asks the user account manager to create a user account.

4. The user account manager creates a user account.
   System administrator permission is assigned to a system administrator. No permissions are assigned to a manager so that he or she can only view information.

5. The user account manager reports the result of user account creation to the system owner.

6. The user account manager informs the user that the account has been created.
   The system administrator or manager will be able to use JP1/IT Desktop Management 2 with restricted functions.

7. Periodical audit is performed to check the registration status of user accounts.
   Audit the application trail and the user account registration status to confirm that the system is being used correctly.

4.6.3 Analyzing management targets

JP1/IT Desktop Management 2 allows device management, security control, and asset management. The range of target devices varies depending on the management methods. Before starting operation, you need to determine which devices in the organization you want to manage.

In addition, you can use online management for computers that can be connected to the network, and use offline management for computers that cannot be connected to the network. For details about functional differences between online management and offline management, see (1) Functional differences between agent/agentless management.

Target devices for device management

For device management, you can view the device status and many types of information by collecting information from devices connected to the network. Examine the devices for which you want to view the current status in the organization.

Device management is applicable to devices that have IP addresses, such as computers with OSs, network printers, and routers. To perform device management, you must register the devices as JP1/IT Desktop Management 2 management targets. One license is used to manage one device.

You can search for any device having an IP address in the network to automatically collect information. Therefore, even if devices in a department are unknown, you can use JP1/IT Desktop Management 2 to collect information for the devices in the organization and add them as management targets. For devices without IP addresses, such as offline computers, use offline management or manage them as assets.

Peripheral devices for computers, such as a mouse and keyboard, can be managed as part of device information by entering information for the peripheral devices as additional information. Therefore, no licenses are used for managing peripheral devices.

If you do not want to use JP1/IT Desktop Management 2 to manage some devices in the organization, register them as exclusion targets. For example, if you only want to manage the devices which are subject to security control, register devices such as network printers and routers as exclusion targets. This allows you to collect information only from the managed devices.

Device management targets are determined as follows:

- Devices to be managed by collecting information:
  Register the devices as management targets. One managed device uses one licence.
- Devices not to be managed:
  Register the devices as exclusion targets (uses no license).

Devices subject to security control

For security control, you can view the security status of devices and take corrective actions based on the information collected from the managed devices. Examine the devices for which you want to maintain security.

Security control is applicable to managed computers running Windows.

By installing agents in computers, you can judge and diagnose the security status and take security measures.

Agentless computers can also be subject to security control, provided that administrative share is enabled and you can log on as a member of the Administrators group. Note, however, that you can judge and diagnose the security status of an agentless computer only within the range of device information that can be acquired. Security judgement and diagnosis are not possible for some information. There are also functional restrictions. For example, the auto enforce function and the software startup suppression function cannot be used.

Security control targets are determined as follows:

- To automatically apply security measures:
  Computers with agents installed are subject to security control.
- To judge and diagnose the security status:
  Computers running Windows are subject to security control. Functions are restricted on agentless computers.

Target devices for asset management

For asset management, you can manage the status of devices owned by the organization (hardware assets), no matter whether they are connected to the network. Analyze the devices which you want to manage as assets in the organization. No licenses are used for managing hardware assets.

Asset management is applicable to all devices owned by the organization. Because you can register any asset information, you can manage peripheral devices and devices without IP addresses.

Of the devices owned by the organization, register the devices you want to manage as hardware assets with asset numbers assigned. By registering the devices as hardware assets, you can manage the asset status (indicating whether the asset is in use or in stock), user name, contact phone number, and related contract information, in addition to asset numbers.

Hardware asset information is automatically registered for devices that are added asJP1/IT Desktop Management 2 management targets. To manage devices as assets rather than adding them as management targets, you must register hardware asset information manually.

(1) Managing device information for online managed computers

To correctly manage device information in the organization where devices increase or decrease on a daily basis, you need to periodically perform a search and register all devices to be managed. The managed device information must be kept up to date.

To manage device information, you need to decide on a search range, search schedule, and whether to install agents on computers discovered by a search. You also need to set up an operation schedule to collect and update device information for computers.

Analyzing device search requirements

Consider the following items related to device search.

- Search range

  Decide the ranges for device searches. Because the IP addresses to be searched for are specified during setup, determine the ranges of IP addresses of the devices to be searched for.

  You can specify multiple search ranges. We recommend that you specify only ranges of IP addresses used in the organization. Because connection is attempted to all IP addresses in the specified range, if you specify a search range that contains unused IP addresses, a long time will be required until the search completes.

- Search schedule

  Decide when to perform device searches. If you plan to perform device searches on a regular basis, decide the search start time and the date. You can set a schedule by specifying a day of the week and time to perform a search, for example, at 8:00 on the first Monday of every month.

  Turned-off devices cannot be discovered by a search. Therefore, for the first week after installation of JP1/IT Desktop Management 2, set up the system to repeatedly perform searches so that all devices will be discovered. When all necessary devices have been registered, set up a search schedule based on a consideration of how frequently devices are installed in the organization.

- Setting and allocation of authentication information

  To collect information such as the device type and OS during a search, you need to register authentication information used for searches. A search uses two types of authentication information: SNMP and Windows administrative share.

  SNMP authentication information

    Register a community name for using SNMP to connect a device.

If a community name has not been set in the network, `public` is set as the community name. Because authentication information with `public` assigned is registered by default, you do not need to register SNMP authentication information if no community name has been set.

Authentication information for Windows administrative share

Register an ID and password used to access Windows administrative share.

You can specify the registered authentication information to be used for each search range. If the computer authentication information varies for different search ranges, you need to register the necessary authentication information and set it for each search range.

If no authentication information is registered, you cannot collect device information during a search, but can only confirm the existence of devices.

- Operation on discovered devices

  Decide which action should be performed when a new device is discovered by a device search. The following actions can be performed.

  - Automatically add the discovered devices as management targets

    Computers that are recognized by a search as Windows OS devices are automatically added as management targets.

  - Automatically install agents on discovered devices

    When an agent is installed on a computer, that computer is automatically added as a management target and becomes subject to security control.

    To install an agent on a computer, authentication information for Windows administrative share must be registered and allocated.

Deciding collection and update intervals for device information

Decide how to collect and update device information during operation. How device information should be updated varies depending on whether an agent is installed on a managed computer.

- For a computer with an agent installed

  The agent collects computer information, and then reports it to the management server on a regular basis. This allows the computer information retained by the management server to be refreshed automatically.

  In addition to automatic collection, you can collect computer information at any time.

- For an agentless computer

  An agentless computer cannot report information to the management server automatically. Therefore, the device information on an agentless computer is configured to be collected and updated on a regular basis. By default, the device information is collected once every hour.

  If there are many agentless computers and collecting information places load on the network, specify a collection interval that is appropriate for your environment.

More detailed information can be collected and managed for a computer with an agent installed than for an agentless computer. Consider installing agents. Also, consider how to update device information.

(2) Applying security measures to online managed computers

Decide how to set security policies considering the organization's security rules. Also determine the judgment schedule based on the security policies, and set the calculation targets and storage period for reports created as a result of security diagnosis.

Applying security policies

By default, the default policy is applied to the managed computers. If there is only one set of rules in the organization, you can change the security policy settings for all computers by editing the default policy. If some computers require special security policies, mainly use the default policy and create special security policies.

In addition, decide security policy details (security configuration items and action items).

Deciding security judgment items and automatic application of security measures

Decide which judgement items should be set for a security policy based on the organization's rules, and determine which security measures should be automatically applied to violations.

Deciding actions to be taken against security policy violations

Decide the action to be taken if a security policy violation is found. You can select from the following actions.

- Notify the user of a security policy violation.
- Deny network connection of the computer that has a security problem.

Setting up the security judgment schedule

The security status is determined at a regular interval based on the specified security policy. Use the Settings module to specify the time of security status judgment appropriate for operations.

Considerations related to calculation of security diagnostic reports

The results of a security status judgment can be calculated in a security diagnostic report. Decide the calculation period and storage period for security diagnostic reports.

- Calculation period

  You can check the security status using periodic security diagnostic reports in addition to checking the current status. You can specify the period as weekly, monthly, quarterly, half yearly, or yearly. Use the Settings module to specify the calculation start date appropriate for the operation in the organization.

- Storage period

  You need to decide how long the calculated security diagnostic reports will be stored. You can specify the storage period in a range from 1 to 10 years.

(3) Managing asset information

You can manage a variety of assets owned by the organization. Consider the management target for each type of asset information.

Hardware assets

Information about the devices, such as computers, servers, printers, network devices, and USB devices, can be managed as hardware asset information. In addition to detailed asset information, you can manage the status indicating that the asset is in use, in stock, or disposed of. Thus, you can see the status of the hardware assets in the organization.

Determine which hardware assets owned by the organization you want to manage by using JP1/IT Desktop Management 2. Then, provide information on the assets.

> **Tip**
>
> If you have an asset register at hand, you can register the asset information by importing the asset register.

Software licenses

You can manage information about the software licenses owned by the organization. Computers permitted to use them can also be managed.

To manage the software licenses, register information about software license certificates. Provide the certificates for the software licenses owned by the organization.

Managed software

You can register a software product corresponding to a software license to manage the license used for each software product. In addition to managing the total number of licenses, you can allocate a license to each computer to find computers that use licenses without permission.

You must confirm in advance which software products currently in use correspond to which software licenses.

Contracts

You can register contract information about hardware assets and software licenses, such as support contracts, rental contracts, and lease contracts, and then manage the contract information associated with asset information. Because you can view information about the contracts that are about to expire, you can create a work schedule.

To manage contract information, register information about contract documents. Provide contract documents related to the hardware assets and software licenses owned in the organization.

Handling management items

You can create original management items as additional management items. You can also add options to the existing management items. If you want to individually manage information in the organization, you must first determine which management items should be created.

> **Tip**
>
> Before you attempt to import and register asset information, confirm the management items contained in the data to be imported. To manage items that do not exist in JP1/IT Desktop Management 2, you need to create management items before importing asset information.

4.6.4 Creating groups

You can manage devices and hardware assets in groups. First, you need to determine what type of grouping to use, and how you wish to create the groups.

When you create groups, you can perform the following tasks at the group level:

- Assign security policies
- Assign a computer to perform distribution
- Define the scope of reports (excluding user-defined groups)
- Assign agent configurations (excluding user-defined groups)

The following table describes the types of group and how each group type is managed.

Type	Management method
Device type	Computers are grouped based on operating system information collected from the computer. Devices other than computers are grouped automatically based on their device type.
Network	Computers are grouped by network segment based on IP address information collected from the computer.

Type	Management method
Department	Computers are automatically grouped based on the department and location information collected from the computer. The administrator can also manually assign computers to groups. When linking with Active Directory, the department information managed by Active Directory can be reflected directly to the group configuration.
Location	
User-defined	Devices are assigned to groups automatically based on the conditions set by the system administrator.

The following describes the matters you must consider when creating groups:

1. Types of group

   In the following circumstances, devices must be managed in user-defined groups. When using user-defined groups, you also need to consider the structure of the groups.

   - You want to manage groups using the value of an added management item as the allocation criteria
   - You want to manage groups using added management items and system groups (device type, network, department, or location) as the allocation criteria

   By default, the relevant groups are not created automatically when you group devices by department and location. You need to decide the structure of the groups.

   When you group devices by device type and network, groups are created automatically based on the information collected from devices. In this case, you do not need to consider the group structure.

2. Group structure

   When using user-defined groups, consider the criteria you want to use to allocate devices to groups.

   Department and location groups can be managed in a tree structure. Consider what group structure would be appropriate in light of the departmental framework of your organization and how devices are physically distributed throughout it. When linking with Active Directory, consider whether to incorporate the group configuration managed by Active Directory as department information.

3. Creating groups

   User-defined groups are created by the system administrator, who sets the conditions for allocating devices to the groups. For details about how to create user-defined groups, see (20) Creating groups. For details about the structure of user-defined groups, see (22) Overview of user-defined groups.

   There are two methods to create groups of departments and locations:

   Group creation by collecting device information

   Groups are created based on the user information collected from computers. To collect user information from computers, the department and location configurations must be set in advance in the Settings module on the management server. Note that user information can only be collected from computers with agents installed.

   You can also use the group configuration managed by Active Directory as department information. To do so, enable the import of group configurations when you configure Active Directory linkage in the Settings module.

   You can also automatically group computers based on the registry information collected from the computers.

   Group creation by the administrator

   You can group computers manually by defining the department and location configuration in the Settings module on the management server.

   Tip

   During initial setup, we recommend that you group devices automatically based on the collected device information. Manual grouping should be used to modify an existing group configuration, rather than during initial setup.

4.6.5 Analysis of network monitoring requirements

To prevent information leaks and virus infections caused by unauthorized devices brought into the network, use network monitoring to prevent unauthorized devices from being connected to the organization's network.

You must determine the network monitoring methods, the networks to be monitored, and the devices permitted for network connection.

Determining the network monitoring method

There are two network monitoring methods as described below. Decide which method you should use.

Blacklist method

This method specifies the devices that are prohibited from connecting to the network. This blocks network connection of the registered devices. Other devices are permitted to connect to the network. Use this method if you want to generally permit network connection and prohibit network connection only when an unauthorized device is found.

When using the blacklist method, we recommend that you enable all automatic updates of the network control list. By doing so, you can ensure that no superfluous information remains on the network control list. If you enable automatic updates only for add operations, superfluous information remains in the network control list, creating a need for manual maintenance by the system administrator.

For details about how to configure automatic update of the network control list, see the description of editing the automatic update of the network filter list in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

Whitelist method

This method specifies the devices permitted for network connection in advance. The registered devices can connect to the network. Network connection attempted from any other devices is automatically blocked. Use this method if you want to ensure robust security for network connection of devices.

When using the whitelist method, by enabling all automatic updates of the network control list, you can automatically prevent sharing of NICs (including wireless LAN cards). However, depending on exactly when automatic updates are enabled, devices might be prevented from accessing the network. If you enable automatic updates only for add operations, you can prevent NIC sharing by making maintenance of the network control list the responsibility of the system administrator.

For details about how to configure automatic update of the network control list, see the description of editing automatic update settings in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

Tip

You can specify the monitoring method for each network segment.

Deciding the network segments to be monitored

Because a network monitor is installed in each network segment, you must decide which network segments in the organization will be monitored.

To monitor the network, you must install computers with the network monitor enabled in the target network segments. A single computer with the network monitor enabled can monitor multiple network segments if that computer can use multiple network cards to connect to multiple networks. Network monitoring takes effect as long as the network monitor is running. Therefore, ensure that the network monitor is enabled on a computer that runs 24 hours a day and on which an agent can be installed.

Deciding the devices subject to network connection control

Devices you should decide vary depending on the network monitoring method.

For the blacklist method:

Determine the devices that are to be prohibited from connecting to the network. Check the IP addresses and MAC addresses used for registering the devices manually.

For the whitelist method:

Use the network search function or install agents to discover all devices to be permitted for network connection. Note that if the network monitor is enabled on a computer, devices that exist in that network segment will automatically be discovered.

Tip

Use one of the following methods to register the devices subject to network connection control.

- Use the network search function or network monitor to discover devices (devices are automatically registered).
- Connect a computer with an agent installed (devices are automatically registered).
- An administrator registers devices manually.

Tip

Because the whitelist method requires you to extract all devices that will be permitted for network connection, operation is difficult at the beginning. You can also use the blacklist method to monitor the network in an early stage of operation, and then change the method to the whitelist method after all devices have been extracted.

Tip

When you use the network monitor, all computers permitted for network connection must be registered as management targets. Devices other than computers need not be management targets.

Quarantine communication

You can set up a device to which devices blocked from the network can connect. Consider the devices appropriate for the operation methods of the organization.

For example, you might set up a security measurement server. This allows computers that have been automatically blocked due to insufficient security measures to connect to the management server and security measurement server. You can also configure the computers to use a troubleshooting tool from the security measurement server and then automatically connect to the network when the security is ensured.

4.6.6 Analyzing periodic maintenance needs

We recommend that you perform the following maintenance during operation. Decide when maintenance should be performed.

- Back up operation data

Back up operation data including the database and data files. If a disk error occurs, information on the management server might be lost or the management server might no longer operate.

Therefore, create a backup on a regular basis during operation. If an error occurs in the management server, you can use the backup to restore the state that existed when the backup was created.

- Reorganize the database

  Long term operation of the database might cause problems such as fragmented areas, degraded storage efficiency, and reduced access speed. To prevent such problems, a function that reorganizes the database is provided. By reorganizing the database, you can change the storage configuration without changing the data contents, thus providing more efficient performance.

  As a standard, reorganize the database before the database space usage reaches 80%.

Decide when and at what interval you should back up operation data and reorganize the database. To create a backup or reorganize the database, you need to stop the management server. Therefore, when creating a schedule, choose a day of the week and time when the management server is not used.

Tip

We recommend that you create a backup or reorganize the database on a regular basis.

Use one of the following methods to perform maintenance on the management server.

- Anytime you wish

  You can manually perform maintenance anytime your wish by using the database manager or by executing a command.

- Scheduled maintenance

  Register the command as a Windows task, and then set a schedule to execute the command automatically.

To perform maintenance by using the database manager:

1. From the **Start** menu on the management server, start the database manager.

2. In the dialog box that appears, select the menu item you want to execute.

3. Follow the instructions in the database manager window to perform maintenance.

Maintenance is completed.

To perform maintenance by using commands:

1. Use the `stopservice` command to stop the management server.

2. Perform maintenance.

   - To back up operation data:

     Use the `exportdb` command to create a backup.

   - To reorganize the database:

     Use the `reorgdb` command to reorganize the database.

3. Use the `startservice` command to start the management server.

Maintenance is completed.

Important note

If the management server is in a cluster configuration, use the cluster software function to start and stop cluster resources on the management server.

If the management server is not in a cluster configuration, you can also use the `exportdb` or `reorgdb` command with the `-a` option specified to perform maintenance. In this case, perform only step 2 above. Steps 1 and 3 are automatically performed.

Tip

If an error occurs on the management server, you can restore the data by using the `importdb` command with the backup data specified as an argument. You can also back up, restore, and reorganize the database by using the database manager.

Appendixes

A. Miscellaneous Information

This appendix provides miscellaneous information about using JP1/IT Desktop Management 2.

A.1 List of folders

Folders created on the management server

The following table shows the folders that are created on the management server when JP1/IT Desktop Management 2 - Manager is installed.

Folder name	Description
JP1/IT Desktop Management 2-Manager-installation-folder	JP1/IT Desktop Management 2 data folder
%WINDIR%\Temp\JDNINST	Folder for log files which are output during installation

The following table shows the folders that are created in *JP1/IT Desktop Management 2-Manager-installation-folder*.

Folder name	Description
log\	Folder to which log files output during installation are copied
mgr\	Root folder for the management server
mgr\backup\	Default backup folder
mgr\bin\	Executable file folder
mgr\conf\	Environment definition file folder
mgr\db\	Database installation folder
mgr\dbclt\	Folder for the installer of the database's ODBC driver
mgr\definition	Linkage definition file folder
mgr\doc\	Online manual folder
mgr\download\	Installation set folder
mgr\endorsed\	Java standard library replacement file folder
mgr\gui\	J2EE application folder
mgr\license\	License file folder
mgr\log\	Trace log folder
mgr\nma\	Network monitor agent folder
mgr\ospatch\	Updated program information file folder
mgr\script\	Agent script file folder
mgr\Setup_Input\	Database setup input file folder
mgr\Setup_Input_HA\	Folder for the database setup input files used for a cluster configuration
mgr\temp\	Temporary data folder
mgr\tools\	Tool folder

Folder name	Description
mgr\troubleshoot\	Default troubleshooting information folder
mgr\uCPSB\	Application server installation folder

The following table shows the folders that are created during installation or setup of JP1/IT Desktop Management 2 - Manager (other than in the installation folder).

Folder name	Description
%ProgramFiles%\Hitachi\HNTRLib2\	Trace library installation folder
All-User-profile-application-data-folder \Hitachi\jp1itdmm\Database\#	JP1/IT Desktop Management 2 data folder
All-User-profile-application-data-folder \Hitachi\jp1itdmm\LocalData\#	Local disk work folder
program-menu-of-the-system\JP1_IT Desktop Management 2 - Manager\	Program folder.

#: This folder name is set by default when the product is provided. The folder is created during setup.

Folders created for the remote installation manager

The following table shows the folders that are created on a computer on which Remote Install Manager is installed.

Folder name	Description
Remote Install Manager-installation-folder	Folder for the remote installation manager data
%WINDIR%\Temp\JDNINST	Folder for log files that are output during installation

The following table shows the folders that are created in *Remote Install Manager-installation-folder*.

Folder name	Description
log\	Folder to which log files output during installation are copied
mgr\	Root folder for Remote Install Manager
mgr\bin\	Executable file folder
mgr\dbclt\	Folder for the installer of the database's ODBC driver
mgr\license\	License file folder
mgr\RMTINS\	Folder for Remote Install Manager-related files
mgr\temp\	Temporary data folder
mgr\troubleshoot\	Default troubleshooting information folder

The following table shows the folder (except the installation folder) that is created when Remote Install Manager is installed or set up.

Folder name	Description
program-menu-of-the-system\JP1_IT Desktop Management 2 - Manager\	Program folder

A.2 List of services and processes

The tables below list the JP1/IT Desktop Management 2 services and corresponding service processes. They also provide a short description of the services and note whether the services start automatically.

List of JP1/IT Desktop Management 2 - Manager services

Service name	Service display name	Service process name	Description	Automatic startup of the service
JP1_DTNAVI_AGCTRL	JP1_ITDM2_Agent Control	*JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\bin\jdnagcadm.exe	Agent control service	Yes
JP1_DTNAVI_MGRSRV	JP1_ITDM2_Service	*JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\bin\jdnmsservice.exe	Manager service	Yes
JP1_DTNAVI_WEBCON	JP1_ITDM2_Web Container	*JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\bin\jdnwebcon.exe	Application server service	Yes
JP1_DTNAVI_WEBSVR	JP1_ITDM2_Web Server	*JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\uCPSB\httpsd\httpsd.exe	Web server service	Yes
HiRDBEmbeddedEdition_JE1	JP1_ITDM2_DB Service	*JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\db\BIN\pdservice.exe	Management server database service	Yes
HiRDBClusterService_JE1	JP1_ITDM2_DB Cluster Service	*JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\db\BIN\pdsha.exe	Cluster service of the management server database	No
Hntr2Service	Hitachi Network Objectplaza Trace Monitor 2	%Program files%\Hitachi\HNTRLib2\bin\hntr2srv.exe	Log output service	No

Legend: Yes: The service starts automatically, No: Does not start automatically

Note that no services start automatically in a cluster configuration because services are manipulated by using the cluster software functions.

List of JP1/IT Desktop Management 2 - Network Monitor services

Service name	Service display name	Service process name	Description	Automatic startup of the service
NXNetMonitor	JP1_ITDM2_Network Monitor	%ProgramFiles%\Hitachi\jp1itdmn\nma\bin\nxnmsvc.exe	Network monitor service	Yes

Legend: Yes: The service starts automatically

List of JP1/IT Desktop Management 2 - Agent services

Service name	Service display name	Service process name	Description	Automatic startup of the service
jdngsrv	JP1_ITDM2_Agent Service	%SystemRoot%\system32\jdngsrv.exe	Agent services	Yes

Service name	Service display name	Service process name	Description	Automatic startup of the service
jdngsmcsrv	JP1_ITDM2_Agent Monitor Control	*Job Management Partner 1/IT Desktop Management 2-Agent-installation-folder* \bin\jdngsmcsrv.exe	Operation monitoring service	Yes
jdngrcagent.exe	JP1_ITDM2_Agent Remote Control	*Job Management Partner 1/IT Desktop Management 2-Agent-installation-folder* \bin\jdngrcagent.exe	Remote control agent service	Yes

Legend: Yes: The service starts automatically

The following table lists and describes the resident processes on a computer on which JP1/IT Desktop Management 2 - Manager is installed. Processes are shown in alphabetical order of their names.

List of processes

Process name	Function	Whether the process is resident
cjstartsv.exe	Application server process	Yes
cprfd.exe	Application server process	Yes
httpsd.exe	Web server function process	Yes
jdnagcadm.exe	Service process	Yes
jdnagcmain.exe	Service process	Yes
jdngschserv.exe	Service process	Yes
jdngsrvmain.exe	Service process	Yes
jdnmscontroller.exe	Service process	Yes
jdnmsplugincontroller.exe	Service process	Yes
jdnmssecurityctrl.exe	Service process	Yes
jdnmssecuritysplit.exe#	Service process	Yes
jdnmsservice.exe	Service process	Yes
jdnwebcon.exe	Application server process	Yes

Legend: Yes: Resident process

#: This process is resident only if you select **16GB** for **Cache size when accessing the database** in the server configuration when you set up the management server.

List of database processes

Process name	Function	Whether the processes are resident (Number of resident processes)	Number of processes
pdservice.exe	HiRDB service process that controls the process server	Yes	1
pdprcd.exe	Process server process that manages HiRDB-related processes	Yes	1

Process name	Function	Whether the processes are resident (Number of resident processes)	Number of processes
pdrsvre.exe	Post-processing process that handles post-processing of an abnormally-terminated process	Yes	1 to 3
pdmlgd.exe	Message log server process that controls message output	Yes	1
pdrdmd.exe	System manager process that manages startup and stoppage of units and connected users	Yes	1
pdstsd.exe	Status server process for input and output of the status files for units	Yes	1
pdlogd.exe	Log server process that controls log-related processes and acquisition of system logs	Yes	1
pdscdd.exe	Scheduler process that assigns transactions to single server processes	Yes	1
pdtrnd.exe	Transaction server process that controls transactions	Yes	1
pdtrnrvd.exe	Transaction recovery process that controls settlement and recovery of a transaction	Yes (1)	1 to 673
pd_buf_dfw.exe	Deferred write process that writes data to the database storage disk	Yes	1
pdlogswd.exe	Log swap process that assigns and releases system log-related files, manages input and output of those files, and acquires synchronization point dumps	Yes	1
pdsds	Single server process that handles SQL processing	Yes (20)	1 to 350
pd*xxx*#	Processes other than pdsds, including utility processes and the database's internal processes	No	--

Legend: Yes: The process is resident. No: The process is not resident. --: The number of processes depends on the process.

#: *xxx* is a character string that contains 3 to 8 characters.

A.3 Port number list

This section describes the port numbers used by JP1/IT Desktop Management 2.

JP1/IT Desktop Management 2 - Manager port number list

Management server

Port number for management server	Connection direction	Connected to [**port number**]	Protocol	Use
31080	←	Administrator's computer [**ephemeral**]	TCP	Used for communication from an administrator's computer to a management server when the operation window is referenced or used. This port number is also used for communication from Remote Installation Manager or Packager installed on the administrator's computer to a management server.

Port number for management server	Connection direction	Connected to [**port number**]	Protocol	Use
31000	←	Agent or relay system [**ephemeral**]	TCP	Used for communication from an agent or relay system to a management server
Ephemeral	→	agent or relay system [**31001**]	TCP	Used for communication from a management server to an agent or relay system during distribution using Remote Installation Manager
31006 to 31009, 31011, 31012	None	None	TCP	Used for JP1/IT Desktop Management 2 internal processing
31010	←	• Remote Installation Manager [**ephemeral**] • Asset Console (jamTakeITDM2Info.exe) [**ephemeral**]	TCP	Used for communication from Remote Installation Manager or Asset Console to a management server, or internal processing
Ephemeral	→	Agent or relay system [**31014**]	TCP	Used for communication from a management server to an agent or relay system to distribute jobs by multicasting
31015	←	Agent or relay system [**ephemeral**]	TCP	Used for communication from an agent or relay system to a management server for requesting retransmission during multicast distribution
31021	←	• Remote Installation Manager [**ephemeral**] • Agent [**ephemeral**] • Relay system [**ephemeral**] • Packager [**ephemeral**]	TCP	Used for communication from Remote Installation Manager, agent, relay system, and Packager to a management server during distribution using Remote Installation Manager
Ephemeral	→	Agent [**16992**]	TCP	Used for controlling the power source of a computer that uses AMT

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, in the setup, change them to port numbers that are not used.

If a management server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if you install JP1/IT Desktop Management 2 - Manager in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Administrator's computer (Remote Installation Manager)

Port number for administrator's computer	Connection direction	Connected to [**port number**]	Protocol	Use
Ephemeral	→	Management server [**31010 and 31021**]	TCP	Used for communication from Remote Installation Manager to a management server during distribution using Remote Installation Manager
Ephemeral#	← →	Management server [ephemeral#]	TCP	Used for Remote Installation Manager internal processing

#: The following describes how to fix the port numbers used for connecting the database to the agent.

To fix the port number of the management server (connection destination):

1. Execute the `stopservice` command to stop the services on the management server.
2. Use a text editor to open the `pdsys` file stored in *JP1/IT Desktop Management 2 - Manager-installation-folder*\mgr\db\CONF.
3. Add `set pd_service_port =` *port-number*. For *port-number*, specify the port number you want to use.

   Example: To specify 10000 as the port number, enter as follows:

   ```
   set pd_service_port = 10000
   ```
4. Execute the `startservice` command to restart the services on the management server.

To fix the port numbers of Remote Installation Manager (connection destination):

For receiving ports, the OS automatically assigns port numbers by default. Ten or more receiving ports are used.

1. Stop Remote Installation Manager and other applications for JP1/IT Desktop Management 2.
2. Use a text editor to open the `HiRDB.ini` file stored in *Remote-Install-Manager-installation-folder*\mgr\dbclt.

   If Remote Install Manager and the management server are installed in the same computer, `HiRDB.ini` is stored in *JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\db\CONF\emb.
3. For `PDCLTRCVPORT=`, specify the range of port numbers you want to use in the *port-number-port-number* format. Note that the range of port numbers is not set if you do not specify anything or specify `0` after `PDCLTRCVPORT=`, By default, the range of port numbers is not set.

   Example: To specify 10000-10500 as the range of port numbers, enter as follows:

   ```
   PDCLTRCVPORT=10000-10500
   ```
4. Start Remote Installation Manager and other applications for JP1/IT Desktop Management 2.

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, in the setup, change them to unused port numbers.

If the administrator's server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if you install Remote Install Manager in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Port number list for a relay system

Port number for relay system	Connection direction	Connected to [**port number**]	Protocol	Use
31001	←	Management server [**ephemeral**]	TCP	Used for communication from a management server to a relay system during distribution using Remote Installation Manager
31002	←	Agent [**ephemeral**]	TCP	Used for communication from an agent to a relay system during distribution using Remote Installation Manager
31014	←	Management server [**ephemeral**]	TCP	Used for communication from a management server to a relay system to distribute jobs by multicasting
31015	←	Agent [**ephemeral**]	TCP	Used for communication from an agent to a relay system for requesting retransmission during multicast distribution

Port number for relay system	Connection direction	Connected to [**port number**]	Protocol	Use
Ephemeral	→	Management server [**31021**]	TCP	Used for communication from a relay system to a management server during distribution using Remote Installation Manager
Ephemeral	→	Agent [**16992**]	TCP	Used for controlling the power source of a computer that uses AMT

Port number list for a controller and remote control agent

Controller or remote control agent [port number]	Connection direction	Connected server [port number]	Protocol	Use
Remote control agent [31016]	←	Controller [ephemeral]	TCP	Used for window operation from a controller to a remote control agent
Remote control agent [31017]	←	Controller [ephemeral]	TCP	Used for transferring files from a controller to a remote control agent
Remote control agent or controller [31018] (when used as a chat server)	← →	Remote control agent or controller [ephemeral]	TCP	Used for chat
Remote control agent [ephemeral]	→	Controller [31019]	TCP	Used for requesting a remote connection from a remote control agent to a controller
Remote control agent [ephemeral]	→	Controller [31020]	TCP	Used for callback file transfer from a remote control agent to a controller

If a computer with a controller installed or a computer that is remotely controlled controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if a controller and remote control agent are installed in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, follow the steps below to change them to port numbers that are not used.

- Port number for a controller

  Specify port numbers in the **Options** dialog box of the controller.
- Port number for a remote controller agent

  Specify port numbers in the **Remote control settings** view used for agent configuration.
- Port number for the chat functionality

  In the **Chat** window, select **Options**, and in the displayed dialog box, in the **Connect** tab, specify the port numbers.

JP1/IT Desktop Management 2 - Agent port number list

Agent port number	Connection direction	Connected server [port number]	Protocol	Use
31001	←	Management server [ephemeral]	TCP	Used for communication from a management server to the agent
16992	←	Management server [ephemeral]	TCP	Used for controlling the power source of a computer that uses AMT

Agent port number	Connection direction	Connected server [port number]	Protocol	Use
Ephemeral	→	Relay system [**31002**]	TCP	Used for communication from an agent to a relay system during distribution using Remote Installation Manager
31014	←	Management server or relay system [**ephemeral**]	TCP	Used for communication from a management server or relay system to an agent to distribute jobs by multicasting
Ephemeral	→	Management server or relay system [**31015**]	TCP	Used for communication from an agent to a management server or relay system for requesting retransmission during multicast distribution
Ephemeral	→	Management server [**31021**]	TCP	Used for communication from an agent to a management server system during distribution using Remote Installation Manager

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, when setting up a management server, change them to port numbers that are not used.

If a computer with an agent installed controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if an agent is installed in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

If networks between JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Agent control ports by using Windows Firewall, specify firewall settings to enable the ports in the above table.

Port numbers for agentless devices

For agentless devices, the port numbers for Windows administrative shares or SNMP are used depending on the authentication status of the devices.

A.4 Lists of parameters

This section describes the parameters used for installation and setup, and the parameters of the Settings module.

(1) Parameters used for installation

JP1/IT Desktop Management 2 - Manager installation

The following tables list and describe the parameters used for installing JP1/IT Desktop Management 2 - Manager.

Installation type

Item	Description	Specifiable values	Default
Installation Type	Select the installation method.	• Quick installation • Custom installation	Quick installation

User registration (for custom installation)

Item	Description	Specifiable values	Default
User Name	Specify the name of the user who uses the product.	No limit	User name that was set during OS installation
Company Name	Specify the name of the company that uses the product.	No limit	Company name that was set during OS installation

Installation folder (for quick installation)

Item	Description	Specifiable values	Default
JP1/IT Desktop Management 2 - Manager Installation Folder	Specify the installation folder.	A path consisting of 40 or fewer characters#1	C:\Program Files\Hitachi \jp1itdmm\ Note, however, that if the OS is a 64-bit version of Windows, the default folder is the folder specified for the %ProgramFiles(x86)% environment variable (if the OS is installed on the C drive, C: \Program Files (x86)\Hitachi \jp1itdmm\).
Database folder	Specify the folder in which the database is created.	A path consisting of 100 or fewer characters#2	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm\

#1: Available characters are single-byte alphanumeric characters, single-byte spaces, periods (.), parentheses, underscores (_), and backslashes (\).

#2: Available characters are single-byte alphanumeric characters, single-byte spaces, hash marks (#), periods (.), parentheses, at marks (@), and backslashes (\).

Setting up the database (for quick installation)

Item	Description	Specifiable values	Default
User ID	Specify the ID of the user who uses the database.	A character string of 8 or fewer characters#	itdm2m
Password	Specify the password for the user ID.	A character string of 28 or fewer characters#	(Blank)
Confirm password	Re-enter the specified password for confirmation.		

#: Available characters are single-byte alphanumeric characters beginning with an alphabet.

Installation folder (for custom installation)

Item	Description	Specifiable values	Default
JP1/IT Desktop Management 2 - Manager Installation Folder	Specify the installation folder.	A path consisting of 40 or fewer characters#	C:\Program Files\Hitachi \jp1itdmm\ Note, however, that if the OS is a 64-bit version of Windows, the default folder is the folder specified for the %ProgramFiles(x86)% environment variable (if the OS is installed on the C drive, C: \Program Files (x86)\Hitachi \jp1itdmm\).

#1: Available characters are single-byte alphanumeric characters, single-byte spaces, periods (.), parentheses, underscores (_), and backslashes (\).

Custom installation (for custom installation)

Item	Description	Specifiable values	Default
Component to Install	Select the component to be installed and the installation method[#1].	- Manager[#2] A component that provides main functions of JP1/IT Desktop Management 2, such as function management and security status management - Remote Install Manager[#3] A component that provides GUI functionality for distribution management that uses the remote installation manager This component can be installed on a computer that is different from the Manager's computer. In such a case, install Remote Install Manager whose version is the same as Manager.	All components

#1: To install the component, click the icon on the left of the component name, and then select from the pull-down list. If you select **This feature will not be available.** in the pull-down list of the component name, the icon will change to the x icon.

#2: When you install Manager, you also need to install Remote Install Manager. If you have selected **This feature will not be available.** in the pull-down list of Remote Install Manager, you cannot install Manager.

#3: To install Remote Install Manager on a computer that is different from the Manager's computer, select **This feature will not be available.** in the pull-down list of Manager.

Installation completed

Item	Description	Specifiable values	Default
Setup[#1]	Select whether to start setup after installation.	Selected Setup is started. Not selected Setup is not started.	Selected.
Automatic update of components[#2]	Specify whether to automatically distribute components (such as agents and network monitor agents) registered on the management server to computers if the components are updated.	Selected Components are updated automatically. Not selected Components are not updated automatically.	Selected.
Register components as a distribution package[#2]	Specify whether to create component packages, which allow you to install updated components by using the distribution function.	Selected Packages are created. Not selected Packages are not created.	Not selected.

#1: Displayed if custom installation of Manager is performed.

#2: Displayed if setup is unnecessary when an overwrite installation is performed. In a cluster system, this item is displayed on the primary server.

JP1/IT Desktop Management 2 - Agent installation

The following tables list and describe the parameters used for installing JP1/IT Desktop Management 2 - Agent from the provided media.

Installation type

Item	Description	Specifiable values	Default
Installation Type	Select the installation method.	• Quick installation • Custom installation	Quick installation

Installation folder (for custom installation)

Item	Description	Specifiable values	Default
JP1/IT Desktop Management 2 - Agent Installation Folder	Specify the installation folder.	A path consisting of 104 or fewer characters#	C:\Program Files\Hitachi \jp1itdma\ Note, however, that if the OS is a 64-bit version of Windows, the default folder is the folder specified for the %ProgramFiles(x86)% environment variable (if the OS is installed on the C drive, C: \Program Files (x86)\Hitachi \jp1itdmm\).

#: Available characters are single-byte alphanumeric characters, single-byte spaces, periods (.), parentheses, colons (:), underscores (_), and backslashes (\).

Types of components to be installed (for custom installation)

Item	Description	Specifiable values	Default
Types of components to be installed	Specify the types of components to be installed.	• Agent • Relay system	Agent

Components to be installed (for custom installation)

Item	Description	Specifiable values	Default
Components to be installed	Select the component and its sub components to be installed, and the installation method#1.	• Agent or relay system#2 (the type specified in the **Types of components to be installed** dialog box) • Packager • Automatic Installation Tool	Agent or relay system (the type specified in the **Types of components to be installed** dialog box)

#1: Select the installation method from the pull-down list that is displayed by clicking the icon on the left of the component name. If you select **This feature will not be available.** in the pull-down list, the icon will change to the x icon.

#2: The remote control agent is a subcomponent of an agent or relay system.

(2) Setup parameters

The following tables list and describe the parameters for setting up a management server and agent.

Setup of a management server

Setup selection

Item	Description	Specifiable values	Default
Setup type	Select the setup type.	• Reconfiguration • Database upgrade • Server reconfiguration	If the database does not need to be upgraded: Reconfiguration If the database needs to be upgraded: Database upgrade

Database settings (for setting change)

Item	Description	Specifiable values	Default
Change the password for accessing the database	Specify whether to change the password for accessing the database.	Selected The password is changed. Not selected The password is not changed.	Selected
Current password	Specify the current password for the user ID.	A character string of 28 or fewer characters#	(Blank)
New password	Specify the new password for the user ID.		
Confirm new password	Re-enter the specified new password for confirmation.		

#: Available characters are single-byte alphanumeric characters. The first character must be an alphabetic character.

Cluster environment

Item	Description	Specifiable values	Default
Use JP1/IT Desktop Management 2 - Manager in a cluster configuration	Specify whether to use the management server in a cluster configuration.	Selected Used in a cluster environment Not selected Not used in a cluster environment	Not selected
Type	Select the type.	• Primary system • Standby system	Primary system
Logical host name	Specify a domain name.	A character string of 255 or fewer single-byte characters	(Blank)
Logical IP address	Specify an IP address.	An IPv4 IP address	(Blank)
Configuration file to be imported	Specify a configuration file to be imported.	A setup file name consisting of 255 or fewer characters (`*.conf`)	(Blank)

Database settings (for initial setting)

Password setting

Item	Description	Specifiable values	Default
User ID	Specify the user ID for accessing the database.	A character string of 8 or fewer characters#	itdm2m
Password	Specify the password for the user ID.	A character string of 28 or fewer characters#	(Blank)
Confirm password	Re-enter the specified password for confirmation.		

#: Available characters are single-byte alphanumeric characters. The first character must be an alphabetic character.

Address and cache settings

Item	Description	Specifiable values	Default
IP address for accessing the database	Specify the IP address of the management server for accessing the database.	An IPv4 IP address	An IP address acquired by a Windows function#1
Cache size when accessing the database#2	Select the cache size used when accessing the database.	• 1 GB • 16 GB	16 GB

#1: The first acquired IP address if multiple IP addresses are set for the management server (for example, when multiple network cards are used).

#2: Displayed only when the 64-bit version of OS is used on the computer on which JP1/IT Desktop Management 2 - Manager has been installed.

Folder settings

Item	Description	Specifiable values	Default
Database folder#1	Specify the folder in which database information is stored. For a cluster configuration, specify a folder on a shared disk.	A path consisting of 120 or fewer characters#2	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm\Database\db\
Data folder#1	Specify the folder in which data used by the management server is stored. For a cluster configuration, specify a folder on the shared disk.	A path consisting of 120 or fewer characters#2	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm\Database\data\
Local data folder#1	Specify a folder for the data area on a local disk. Note that a path to a shared disk cannot be specified.	A path consisting of 120 or fewer characters#2	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm\LocalData\
Database extraction folder#1	Specify the folder in which a database is temporarily saved.	A path consisting of 120 or fewer characters#2	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm\Database\dbtemp\

#1: The database folder, data folder, local data folder, and database extraction folder cannot be the same and cannot have a parent-child relationship with each other.

#2: Available characters are single-byte alphanumeric characters, single-byte spaces, hash marks (#), periods (.), parentheses, at marks (@), and backslashes (\).

Database upgrade settings

Item	Description	Specifiable values	Default
Type	Select the type.	- Primary system - Standby system	Primary system
Configuration file to be imported	Specify the setup file copied from the primary node.	A setup file name consisting of 255 or fewer characters (`*.conf`)[#2]	(Blank)
Database folder[#1]	Specify the folder in which database information is stored. For a cluster configuration, specify a folder on the shared disk.	A path consisting of 120 or fewer characters[#2]	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm \Database\db\
Database extraction folder[#1]	Specify the folder in which a database is temporarily saved.	A path consisting of 120 or fewer characters[#2]	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm \Database\dbtemp\

#1: The database folder, data folder, local data folder, and database extraction folder cannot be the same and cannot have a parent-child relationship with each other.

#2: Available characters are single-byte alphanumeric characters, single-byte spaces, hash marks (#), periods (.), parentheses, at marks (@), and backslashes (\).

Operation log settings

Item	Description	Specifiable values	Default
Use Operation log	Specify whether to acquire operation logs from computers with agents installed.	Selected Operation logs are acquired. Not selected Operation logs are not acquired.	For quick installation: Not selected For custom installation: Not selected
Store the operation logs	Specify whether to store the operation logs.	Selected Operation logs are stored. Not selected Operation logs are registered in the database, but not stored.	For quick installation: Not selected For custom installation: Selected
Operation log backup folder[#1]	Specify the folder in which the operation logs are stored.	A path consisting of 120 or fewer characters[#2]	(Blank)
Username[#3]	Specify the user name used for accessing the operation log backup folder.	A character string of 158 or fewer single-byte characters	(Blank)
Password	Specify the password for the user name.	A character string of 30 or fewer single-byte characters	(Blank)
Number of managed nodes	Specify the number of devices to be managed.	50 to 30000	For quick installation: 50 For custom installation: 200
Maximum number of days for which the operation logs are to be stored in the database	Specify the maximum number of days for which the operation logs are to be stored in the database. For example, specify100 for this item, if	30 to 500	60

Item	Description	Specifiable values	Default
Maximum number of days for which the operation logs are to be stored in the database	operation logs for 100 days are to be stored in the database.#4	30 to 500	60
Operation log database folder#5	Specify the database folder in which operation logs are stored.	A path consisting of 120 or fewer characters#6	*All-User-profile-application-data-folder*\Hitachi\jp1itdmm \Database\oplogdb
Capacity to be added to the cache#7	Specify the capacity, to be added to the database cache, for improving retrieval performance of operation logs.	0 to 16	0

#1: You can also specify a folder on a network drive. To specify a network drive, use UNC format.

#2: Available characters are single-byte alphanumeric characters, single-byte spaces, hash marks (#), periods (.), parentheses, at marks (@), backslashes (\), and hyphens (-).

#3: To specify a domain user, use *domain-name\user-name* format.

#4: The specified number of days cannot be decreased once it is specified.

#5: If the number of managed computers is in the range from 10,000 to 30,000, Hitachi recommends that you use a physical disk dedicated to the operation log database.

#6 : Available characters are single-byte alphanumeric characters, single-byte spaces, hash marks (#), periods (.), parentheses, at marks (@), and backslashes (\).

#7: Displayed only when the 64-bit version of OS is used on a computer on which JP1/IT Desktop Management 2 - Manager has been installed. For the 32-bit version of OS, 0 is set.

Revision history archive output settings

Item	Description	Specifiable values	Default
Regularly output and save the revision history archive	Specify whether to regularly output the revision history for archival purposes.	Selected A revision history archive is regularly output. Not selected A revision history archive is not regularly output.	Not selected
Output folder for the revision history#1	Specify the folder in which the output revision history archive is stored.	A path consisting of 120 or fewer characters#2	(Blank)
User name#3	Specify the user name used for accessing the output folder.	A character string of 158 or fewer single-byte characters	(Blank)
Password	Specify the password for the user name.	A character string of 30 or fewer single-byte characters	(Blank)

#1: A folder on the network drive can also be specified. Use the UNC format to specify the network drive.

#2: Available characters are single-byte alphanumeric characters, single byte spaces, hash marks (#), periods (.), parentheses (()), at marks (@), backslashes (\), and hyphens (-).

#3: Use the *domain-name\user-name* format to specify a domain user.

Port number settings

Item	Description	Specifiable values	Default
Port number for accepting connections from the administrator's computer	Specify the port number used to connect to the management server from the administrator's	2 to 49151	31080

Item	Description	Specifiable values	Default
Port number for accepting connections from the administrator's computer	computer by using an operation window.	2 to 49151	31080
Port number for accepting connections from agents	Specify the port number used to connect to the management server from agents.	5001 to 49151	31000
Port number for agent startup requests	Specify the port number used to connect to agents from the management server.	5001 to 49151	31001
Port numbers used by the server	Specify the start value of the 11 consecutive port numbers used for management server internal processing.	5001 to 49141	31002
Port number used for remote control	Specify the start value of the five consecutive port numbers used by the remote control function.	5001 to 49147	31016

Settings for address resolution

Item	Description	Specifiable values	Default
Specify the type of information that determines the connection-target computer for inter-host communication.		- Host name - IP address	Host name
Address resolution method#1	Specify the addresses resolution method upon job creation or execution.	- Use the Windows network IP addresses are acquired from the Windows network upon job creation or execution.#2 - Use device information and system configuration information IP addresses are acquired only from the system configuration information of JP1/IT Desktop Management 2 upon job creation or execution.#3	Use the Windows network
When the address of the job destination cannot be resolved#1	Specify whether to treat a job for which address resolution for the destination failed during job execution as an error.	- Treat as an error. - Do not treat as an error.	Do not treat as an error.

#1: Specify this item when **Host name** is selected as the type of information that determines the communication-target computer (which is called the *ID key for operation*).

#2: The `hosts` file or name server is used for address resolution. If address resolution fails, IP addresses are acquired from the system configuration information of JP1/IT Desktop Management 2.

#3: The IP addresses in the system configuration information of JP1/IT Desktop Management 2 must be always maintained in the correct state. In an environment in which jobs are created and executed while the name server is stopped (for example, during the night), even if you select **Use the Windows network**, address resolution might fail and jobs might not be created. However, if you select **Use device information and system configuration information**, you do not have to wait until address resolution fails.

Other settings

Item	Description	Specifiable values	Default
Currency unit setting	Specify the unit of money displayed in an operation window.	A character string of 10 or fewer single-byte characters	Currency unit set in the system
Control the network bandwidth on the management server	Specify whether to set the maximum transfer rate for sending packages from the management server to agents by using the ITDM-compatible distribution function.	Selected The maximum transfer rate from the management server is set. Not selected The maximum transfer rate from the management server is not set.	Not selected
Maximum transfer rate	Specify the maximum transfer rate for sending packages.	2 to 1024	2
Number of consecutive login failures before the account is locked	Specify the number of consecutive login failures that are allowed before the account is locked.	0 to 10	0
Number of days until the password expires	Specify the expiration date of the password for the login user.	0 to 999	180
Suppress operations on asset information from the operation window	Specify whether to suppress operations on asset information from the operation window, for asset management from Asset Console.	Selected Operations on asset information from the operation window are suppressed. Not selected Operations on asset information from the operation window are not suppressed.	Not selected

End of setup

Item	Description	Specifiable values	Default
Register components[#1]	Specify whether to register components such as agents and network monitor agents on the management server.	Selected The programs are registered. Not selected The programs are not registered.	Selected
Automatic update of components[#2]	Specify whether to automatically distribute components, such as agents and network monitor agents, registered on the management server to computers if the components are updated.	Selected Components are updated automatically. Not selected Components are not updated automatically.	Selected
Register components as distribution packages[#2]	Specify whether to create component packages, which allow you to install updated components by using the distribution function.	Selected Packages are created. Not selected Packages are not created.	Not selected

#1: Displayed when the first startup is started manually.

#2: Displayed when startup is started as an extension process of installation.

Setup for distribution by using Remote Installation Manager

Communication

Item	Description	Specifiable values	Default
JP1/IT Desktop Management 2 - Manager (management server)	Specify the port number, of the management server, that is used for distribution using Remote Installation Manager.	0 to 65535	31021
JP1/IT Desktop Management 2 - Agent (Relay System)	Specify the port number, of the relay system, that is used for distribution using Remote Installation Manager.	0 to 65535	31002
Perform interval transmissions	Specify whether a file is divided by the specified unit and transmitted at the specified interval when a file transmission to agents and relay systems occurs.	Selected Interval transmissions are performed. Not selected Interval transmissions are not performed.	Not selected
Number of continuous transmission buffers#	Specify the number of buffers that are used for one file transmission.	0 to 4294967295	0
Transfer interval#	Specify the interval between transmissions (transmission suspension period) when interval transmissions are performed.	0 to 4294967295	1000

#: If 0 is specified, interval transmissions are not performed.

Server customization options

Item	Description	Specifiable values	Default
Number of JP1/IT Desktop Management 2 - Agent instances that can connect to the management server concurrently	Specify the maximum number of the following systems that can connect to the management server concurrently: • Agents • Relay systems • Remote Installation Managers • Packagers	4 to 100	30
Number of JP1/IT Desktop Management 2 - Agent instances that can execute jobs concurrently#1	Specify the maximum number of the following systems that can execute jobs concurrently: • Agents • Relay systems • Remote Installation Managers • Packagers	0 to 100	20

Item	Description	Specifiable values	Default
Specify when jobs will be deleted#2	Specify whether to delete jobs immediately after the job definitions and execution statuses are deleted. If jobs are not deleted immediately, specify the time the jobs are to be deleted.	Selected Jobs are not deleted immediately. If this option is selected, also specify the time the jobs are to be deleted. 00:00 to 23:59 Not selected Jobs are deleted immediately.	Not selected
Monitor the startup of JP1/IT Desktop Management 2 - Agent	Specify whether to change the job execution status to startup failure and report it to the managing server if a job is not executed because an agent or relay system is not running.	Selected Whether the agents and relay systems are running is monitored and reported to the managing server. Not selected Whether the agents and relay systems are running is not monitored.	Selected
Break down the reason for a starting failure	Specify whether to break down the reason for a starting failure and report it to the managing server when the startup of an agent or relay system fails.	Selected The reason for a starting failure is broken down and reported to the managing server. Not selected The reason for a starting failure is not broken down.	Not selected
Monitor file transfer errors of JP1/IT Desktop Management 2 - Agent	Specify whether to change the job execution status to communication error and report it to the managing server when a job of one of the following job types falls into a communication error during file transfer with an agent or relay system: • Install package • Send package, allow client to choose • Transfer package to relay system • Acquire collected files from relay system • Get system information from client • Hold report • Hold-report release	Selected File transfer errors are monitored and reported to the managing server. Not selected File transfer errors are not monitored.	Selected

#1: If 0 is specified for this item, startup messages are not sent to the target system. In other words, if 0 is set, job execution from Remote Installation Manager and startup of agents using agent control are no longer available.

#2: In general, because many agents are managed in distribution management, deleting job definitions and execution status requires long time for deleting the database. This might cause problems in operations, or place a load on main business operations. You can avoid this problem by delaying deletion of jobs and deleting such jobs at the same time when it is convenient.

Multicast distribution

Item	Description	Specifiable values	Default
Multicast distribution	Specify the port number that is used for multicast distribution of jobs.	0 to 65535	31045
Multicast distribution (when retransmission is required)#1	Specify the port number that is used for a request for resending of jobs by multicast distribution.	0 to 65535	31015
Allow jobs to be sent by multicast distribution#2	Specify this item to send jobs for which multicast distribution is specified, to agents and relay systems by multicast distribution.	Selected Jobs are to be sent by multicast distribution. Not selected Jobs are not to be sent by multicast distribution.	Not selected
Multicast address	Specify the multicast address assigned to the distribution-destination multicast group#3.	224.0.1.0 to 239.255.255.255	238.255.0.1
Size of one packet	Specify the size of a packet used when a job is distributed.	1 to 60	40#4

#1: Because multicast distribution uses the UDP protocol, resending of packets occurs during distribution. Therefore, you must set the port number used for a request for resending.

#2: If you use a router that does not support IP multicast, do not select this option. If you do so, the distribution method is switched to unicast distribution, and it takes time until job distribution finishes.

#3: A multicast group must contain the agents that connect to the management server and the relay systems. If the multicast address for the distribution-destination agents and the relevant relay systems is different from the multicast address specified here, jobs are sent by unicast distribution to the agents and relay systems.

#4: The value of 40 KB is efficient enough for 100BASE communication lines. If the communication line is 10BASE, specify 4 KB. Note that, if the packet size is too large, multicast distribution might fail and change to unicast distribution from the middle of distribution.

Log options

Item	Description	Specifiable values	Default
Record the results of jobs#1	Specify whether to record the execution results of jobs for which no IDs are specified in Remote Installation Manager.	Selected The execution results of jobs for which no IDs are specified are recorded in Remote Installation Manager. Not selected The execution results of jobs for which no IDs are specified are not recorded in Remote Installation Manager.	Selected
Record result if the job is	Specify the execution status of the jobs to be recorded.	Error Only the jobs whose execution status is Error are recorded in Remote Installation Manager. Error, Completed The jobs whose execution status is Error or	Error, Completed

Item	Description	Specifiable values	Default
Record result if the job is	Specify the execution status of the jobs to be recorded.	Completed are recorded in Remote Installation Manager.	Error, Completed
Record the results of ID group jobs#2	Specify whether to record the execution results of jobs (for each client) for which IDs are specified.	Selected The execution results of jobs (for each client) for which IDs are specified are recorded. Not selected The execution results of jobs (for each client) for which IDs are specified are not recorded.	Selected
Record result if the ID group job is	Specify the execution status of the jobs to be recorded.	Error, Finished Jobs whose execution status is Error or Finished are recorded in Remote Installation Manager. Error, Finished, Completed Jobs whose execution status is Error, Finished, or Completed are recorded in Remote Installation Manager.	Error, Finished, Completed

Note: You can reduce the required disk capacity by recording necessary execution results only. If the large amount of execution results of finished jobs remain, Remote Installation Manager might be slower. Therefore, Hitachi recommends that you record only the jobs whose execution status needs to be checked.

#1: The execution status of the following jobs cannot be automatically deleted even after the jobs finish:

- *Send package, allow client to choose* jobs
- *Get system information from client* jobs for which the execution date on agents has been specified
- *Get software information from client* jobs for which the execution date on agents has been specified

#2: For the execution results of an agent that belongs to the IDs managed by the relay system, this setting is enabled for all job types. For the execution results of an agent that belongs to the IDs managed by the managing server, this setting is disabled for the following jobs, and all execution statuses are recorded in the managing server:

- *Send package, allow client to choose* jobs
- *Get system information from client* jobs for which the execution date on agents has been specified
- *Get software information from client* jobs for which the execution date on agents has been specified

System configuration

Item	Description	Specifiable values	Default
Synchronize changes to the system configuration	Specify whether to automatically apply the changes in the system configuration information of JP1/IT Desktop Management 2 to the system configuration information of the relay system.	Selected The changes in the system configuration information are automatically applied to the system configuration information of the lower system.	Selected

Item	Description	Specifiable values	Default
Synchronize changes to the system configuration	Specify whether to automatically apply the changes in the system configuration information of JP1/IT Desktop Management 2 to the system configuration information of the relay system.	Not selected The changes in the system configuration information are not automatically applied to the system configuration information of the lower system.	Selected
Save deletion history	Specify whether to save the history of deleting a host from the system configuration information of JP1/IT Desktop Management 2.	Selected The history of deleting a host from the system configuration information is saved. Not selected The history of deleting a host from the system configuration information is not saved.	Not selected

Event service

Item	Description	Specifiable values	Default
Enable the event service	Specify whether to use the JP1/Base event service to report the execution results of jobs and errors in JP1/IT Desktop Management 2 as JP1 events to JP1/IM.	Selected JP1 events are reported to JP1/IM. Not selected JP1 events are not reported to JP1/IM.	Not selected
Send job end event - At completion	Specify whether to report that all jobs for all destinations have normally finished.	Selected That all jobs for all destinations have normally finished is reported. Not selected That all jobs for all destinations have normally finished is not reported.	Not selected
Send job end event - At error	Specify whether to report that an error occurred in a job.	Selected That an error occurred in a job is reported. Not selected That an error occurred in a job is not reported.	Not selected
Send instruction end event - At completion	Specify whether to report that all instructions have normally finished.	Selected That all instructions have normally finished is reported. Not selected That all instructions have normally finished is not reported.	Not selected

Item	Description	Specifiable values	Default
Send instruction end event - At error	Specify whether to report that an error occurred in an instruction.	Selected That an error occurred in an instruction is reported. Not selected That an error occurred in an instruction is not reported.	Not selected

The types of jobs whose execution results can be reported to JP1/IM are shown below. For these jobs, the execution results of jobs can also be reported by more detailed unit (instruction). An instruction is the minimum unit of a job created by JP1/IT Desktop Management 2, and is created for each destination and for each distributed software program. For example, if a job is created that distributes two software programs to each of two destinations, four instructions are created for the job.

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

Error Handling

Item	Description	Specifiable values	Default	File names#
Generations of log file to be saved	Specify the maximum number of generations that are to be saved for each log.	1 to 999	5	Not applicable
MAIN file	Specify the number of lines on which MAIN log entries are output.	500 to 9,999	700	MAIN.LOG
USER file	Specify the number of lines on which USER log entries are output.	500 to 9,999	700	• BUILD.LOG • SCRIPT.LOG • USER.LOG
COMPO file	Specify the number of lines on which COMPO log entries are output.	500 to 9,999	700	• API.LOG • ATRFILE.LOG • BSAPI.LOG • CLTPROTO.LOG • DEFAULT.LOG • EXCFILE.LOG • MNGFILE.LOG • RDBMENTE.LOG • SERVICE.LOG • SRVSOCK.LOG • STSFILE.LOG • WSH.LOG
FUNC file	Specify the number of lines on which FUNC log entries are output.	500 to 9,999	2000	• AMTAPI.LOG • CLIENT.LOG • CLTDEL.LOG • DCMAMT.LOG • DISCVRY.LOG

Item	Description	Specifiable values	Default	File names#
FUNC file	Specify the number of lines on which FUNC log entries are output.	500 to 9,999	2000	• DLL.LOG • INVENTRY.LOG • MLTPROTO.LOG • MONRST.LOG • MONTRACE.LOG • NDGMENT.LOG • PSM.LOG • SCHEDULE.LOG • SCHTRACE.LOG • SERVER.LOG • SITE.LOG • SRVAPI.LOG • SRVLOCK.LOG • USER_CLT.LOG • WRAPPER.LOG
LONG file	Specify the number of lines on which LONG log entries are output.	500 to 9,999	700	• DUMP.LOG • NODE.LOG • NODEOPR.LOG • RDBSRV.LOG • USERINV.LOG
Type of Event Viewer message	Specify the type of messages that are output to Windows NT's Event Viewer.	Error Error messages are output. Error, Warning Error messages and warning messages are output. Error, Warning, Information Error messages, warning messages, and information messages are output.	Error	Not applicable

#: For log files that are not listed here, the number of log generations to be managed and the number of log entries cannot be set.

The capacity of each log file can be calculated by the following formula:

log-file-size (bytes) = (*header-size* + (*size-of-an-entry* x *number-of-entries*)) x (*number-of-generations* + 1)

header-size:

17 bytes

size-of-an-entry:

192 bytes (except LONG log entries) or 300 bytes (LONG entries)

Audit Log

Item	Description	Specifiable values	Default
Units in which the audit log is to be output	Specify the unit in which the audit log is to be output.	• Output for each job • Output for each command#	Output for each job

#: Note that, if **Output for each command** is selected, the capacity of the output audit log might greatly consumes free disk space.

Setup of a relay system

Connection-destination settings

Item	Description	Specifiable values	Default
Communicate with the higher system	Specify whether to connect to the management server.	Selected Connected to the management server. Not selected Not connected to the management server.	Selected
Host name or IP address	Specify the host name or IP address of the management server to connect to.[#1]	Host name[#2] or IPv4 IP address	Host name or IP address of the management server
Port number of management server	Specify the port number that is used when an agent connects to the management server.	5001 to 49151	31000

#1: If, in the settings for address resolution during management server setup, you specified a host name as the node identification key for operation, specify a host name here. If you specified an IP address, specify an IP address here.

#2: Specify the name using a character string of 255 or fewer characters.

Communication settings

Item	Description	Specifiable values	Default
Network Adapter Settings button	Click this button to set the priority among the communication lines used by JP1/IT Desktop Management 2 in an environment that has multiple network adapters (multiple LAN connections).	None	None

Network adapter settings

Item	Description	Specifiable values	Default
Specify the priority in which network adapters should be used	Specify whether to set the priority among network adapters for use when there are multiple network adapters.	Selected The priority among network adapters is set. Not selected The priority among network adapters is not set.	Not selected
Automatically update network adapter information upon service startup or connection	Specify whether network adapter information is automatically updated upon service startup or connection.	Selected Network adapter information is automatically updated. Not selected Network adapter information is not automatically updated.	Selected

Setup of an agent

Connection-destination settings

Item	Description	Specifiable values	Default
Communicate with the higher system	Specify whether to connect to the following higher systems: • Management server • Higher system for distribution	Selected Connected to the higher systems. Not selected Not connected to the higher systems.	Selected
Host name or IP address	Specify the host name or IP address of the management server to connect to.#1	Host name#2 or IPv4 IP address	Host name or IP address of the management server
Port number of management server	Specify the port number that is used when an agent connects to the management server.	5001 to 49151	31000

#1: If, in the settings for address resolution during management server setup, you specified a host name as the node identification key for operation, specify a host name here. If you specified an IP address, specify an IP address here.

#2: Specify the name using a character string of 255 or fewer characters.

Communication settings

Item	Description	Specifiable values	Default
Network Adapter Settings button	Click this button to set the priority among the communication lines used by JP1/IT Desktop Management 2 in an environment that has multiple network adapters (multiple LAN connections).	None	None

Network Adapter Settings

Item	Description	Specifiable values	Default
Specify the priority in which network adapters should be used	Specify whether to set the priority among network adapters for use when there are multiple network adapters.	Selected The priority among network adapters is set. Not selected The priority among network adapters is not set.	Not selected
Automatically update network adapter information upon service startup or connection	Specify whether network adapter information is automatically updated upon service startup or connection.	Selected Network adapter information is automatically updated. Not selected Network adapter information is not automatically updated.	Selected

If you upgrade Job Management Partner 1/IT Desktop Management 2, the existing configuration items are displayed without changes, and the default values are displayed for new configuration items.

(3) User account parameters

The following table lists and describes the parameters in the **Account Management** view that opens from **User Management** in the Settings module.

Item	Description	Specifiable values	Default
User Account	Set the user account for JP1/IT Desktop Management 2.	User account	System
User ID	Specify the user ID used to log in to an operation window.	A character string of 64 or fewer single-byte characters#1	(Blank)
Password	Specify the password for the user ID.	A character string of 32 or fewer single-byte characters#2	(Blank)
Retype Password	Enter the password again.	A character string of 32 or fewer single-byte characters#2	(Blank)
User Name	Specify the user account name.	A character string of 128 or fewer characters	(Blank)
E-mail	Specify the email address of the user account user.	Email character string	(Blank)
Description	Enter a description of the user account.	A character string of 1,024 or fewer characters	(Blank)
System Administrator#3	Specify whether to assign system administrator permission to the user account.	Selected System administrator permission is assigned. Not selected System administrator permission is not assigned.	Not selected
User Management#3	Specify whether to assign user account management permission to the user account.	Selected User account management permission is assigned. Not selected User account management permission is not assigned.	Not selected
Security management	Specify whether to set security management as a task for the user account.	Selected Security management is set as a task for the user account. Not selected Security management is not set as a task for the user account.	Selected
Asset management	Specify whether to set asset management as a task for the user account.	Selected Asset management is set as a task for the user account. Not selected Asset management is not set as a task for the user account.	Selected
Device management	Specify whether to set device management as a task for the user account.	Selected Device management is set as a task for the user account.	Selected

Item	Description	Specifiable values	Default
Device management	Specify whether to set device management as a task for the user account.	Not selected Device management is not set as a task for the user account.	Selected
Distribution management	Specify whether to set distribution management as a task for the user account.	Selected Distribution management is set as a task for the user account. Not selected Distribution management is not set as a task for the user account.	Selected
System configuration management	Specify whether to set system configuration management as a task for the user account.	Selected System configuration management is set as a task for the user account. Not selected System configuration management is not set as a task for the user account.	Not selected
Set the administration scope for this user account	Specify whether to set an administration scope for the user account.	Selected An administration scope is set for the user account. Not selected No administration scope is set for the user account.	Not selected
Administration scope	Specify the administration scope.	Groups in the department	Not set.
Status	Displayed only when the user account has been locked. If **Disabled** has been selected, you cannot log in to JP1/IT Desktop Management 2.	Enabled You can unlock the user account. Disabled The user account has been locked.	Disabled

#1

Available characters are single-byte alphanumeric characters and the following symbols:

Exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), parentheses, asterisks (*), plus signs (+), commas (,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), less-than signs (<), equal signs (=), more-than signs (>), question marks (?), at marks (@), square brackets, carets (^), underscores (_), grave accent marks (`), curly brackets, vertical bars (|), swung dashes (~), and single-byte spaces

#2

Observe the following rules when setting a password for the user account.

- Use 8 to 32 characters.
- Use single-byte alphanumeric characters and the following symbols:

  Exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), parentheses, asterisks (*), plus signs (+), commas(,), hyphens (-), periods (.), forward slashes (/), colons (:), semicolons (;), less-than signs (<), equal signs (=), more-than signs

(>), question marks (?), at marks (@), square brackets, carets (^), underscores (_), grave accent marks (`), curly brackets, vertical bars (|), swung dashes (~), and single-byte spaces

- Use a combination of two or more types of characters.
- Use a character string that is different from the user ID.
- When changing the password, use a different character string from the current one.

#3

If neither **System Administrator** nor **User Management** is selected, view permission is assigned to the user account.

(4) Agent parameters

The following tables list and describe the parameters in the **Add Agent Configuration** and **Edit Agent Configuration** dialog boxes that open from the **Agent Configuration and Installation Set Creation** view in the Settings module.

Basic settings

Item		Description	Specifiable values	Default
Management server	Host name or IP address	Specify the host name or IP address of the management server that the agent connects to.	Host name[#1] or IPv4 address	Host name or IP address of the management server
	Port number	Specify the port number that the agent uses to connect to the management server.	5001 to 49151	Port number specified for **Port number for Agent connection** in the **Port Number Settings** dialog box during management server setup
Higher-level system for distribution that uses Remote Install Manager[#2]	System type	Specify the higher-level system for distribution using Remote Installation Manager. In the following cases, make sure to specify **Management server**: • When you create an agent setting that is to be assigned to the relay system. • When you edit the default agent setting.	• Management server • Relay system	Management server
	Host name or IP address	Specify the host name or IP address of the higher-level system for distribution using Remote Installation Manager. In the following cases, make sure to specify the host name or IP address of the management server: • When you create an agent setting that is to be assigned to the relay system. • When you edit the default agent setting.	Host name[#3] or IPv4 address	Host name or IP address of the management server
	Port number for distribution (for the management server)	Specify the port number that is used when the agent connects to the management server for distribution.	1 to 65535	Port number specified for **IT Desktop Management 2 - Manager (management server)** of **Port numbers** under **Related to Communications** in the **Setup for Distribution by Using Remote Install**

Item		Description	Specifiable values	Default
Higher-level system for distribution that uses Remote Install Manager[#2]	Port number for distribution (for the management server)	Specify the port number that is used when the agent connects to the management server for distribution.	1 to 65535	**Manager** dialog box during management server setup
	Port number for distribution (for the relay system)	Specify the port number that is used when the agent connects to the relay system for distribution.	1 to 65535	Port number specified for **IT Desktop Management 2 - Manager (Relay System)** of **Port numbers** under **Related to Communications** in the **Setup for Distribution by Using Remote Install Manager** dialog box during management server setup
Communicate with the higher-level system		Specify whether the agent communicates with the higher-level system.	Selected The agent communicates with the higher-level system. Select the check box to manage computers online. Not selected The agent does not communicate with the higher-level system. Clear the check box to manage computers offline.	Selected
Periodically notify the higher system of the information collected from the computer		Specify whether to periodically notify the higher system of the information collected from the computer.	Selected Information is periodically sent to the higher system. Not selected Information is not sent to the higher system.	Selected
Monitoring interval - Security items (minutes)		Specify the monitoring interval for updates of device information related to agent security.	1 to 9999	10
Monitoring interval - Other information (minutes)		Specify the monitoring interval for updates of device information other than agent security.	1 to 9999	60
Flow Control		Specify whether to use flow control to limit how much data the ITDM-compatible distribution function can transfer per hour when transferring packages to agents from the management server. Use this parameter for compatibility with the JP1/IT Desktop Management settings. If you do not need compatibility with JP1/IT Desktop Management, select OFF.	ON Flow control is used. Specify, in the range from 30 to 99 (99 by default), the maximum percentage of network bandwidth the distribution function can use per hour. OFF Flow control is not used.	OFF
Perform polling based on the system startup[#4]		Specify whether to perform polling based on the system startup.	Selected Polling is performed based on the system startup.	Selected

Item	Description	Specifiable values	Default
Perform polling based on the system startup#4	Specify whether to perform polling based on the system startup.	Not selected Polling is not performed based on the system startup.	Selected
Polling timing	Select, from the drop-down list, when polling is to be performed at system startup.#5	Before the client starts When the agent starts, polling is performed, and then downloaded packages are installed.#6 After the client starts When the agent starts, downloaded packages are installed, and then polling is performed.#7	Before the client starts
Polling method	Specify the polling method.	Perform polling one time (only when the system starts) Polling is performed only once when the system starts. You can select **Perform polling on every system startup** or **Perform polling only during the first system startup (once a day)** from the drop-down list only when you select **Before the client starts** for **Polling timing**. Periodically perform polling on every system startup Polling is performed at a specified interval. Specify the interval in the range from 1 to 720 minutes.	Periodically perform polling on every system startup (30 minutes)
Polling start time	Specify the time to wait before polling is started after the system starts, and the timing of startup of polling.	Start polling during system startup Polling is started at the same time the system starts. Start polling at the specified timing Polling is started at an arbitrary timing after the agent starts, until the specified time (seconds) has passed. Specify the time, in the range from 1 to 300 seconds (1 second by default), until which polling is to be started.#8 Start polling at the specified timing Polling is started after the specified time period (seconds) has passed after the agent starts. Specify the time in the range from 1 to 7200 seconds (1 second by default).	Start polling during system startup

Item	Description	Specifiable values	Default
Perform polling at the specified time	Specify whether to perform polling once a day at the specified time.	Selected Polling is performed at the specified time. Not selected Polling is not performed at the specified time.	Not selected
Execution time	Specify the time polling is to be executed.	00:00 to 23:59	00:00
Detection of change in JP1/IT Desktop Management 2 - Agent	Specify whether to display an event indicating that the contents of the JP1/IT Desktop Management 2 - Agent installation folder have been changed.	Selected An event is displayed. Not selected An event is not displayed.	Selected
Customize Installation Options#9	Specify the path into which the agent is to be installed.	A character string of 64 or fewer characters#10	%ProgramFiles%\Hitachi \jp1itdma

#1: Specify the host name using a character string of 255 or fewer characters.

#2: The value set for this item is always the same as the value for the higher-level system that is displayed in **Higher-level system to be polled** of **Communication settings** as the first-priority higher-level system.

#3: Specify the host name using a character sting of 64 or fewer characters. Available characters are single-byte alphanumeric characters, periods (.), and hyphens (-).

#4: If you execute a job after setting the timing of software execution to **Execute the next time the system starts**, select the **Perform polling based on the system startup** check box.

#5: If the agent is not started during job execution, you can use this setting to control the timing for installing packages for which **Install when system starts** is set.

#6: If a package with **Install when system starts** specified has already been registered in the managing server, the package is installed immediately after it is downloaded due to the polling upon system startup. Therefore, installation is completed during one system startup. If the **ITDM2_Startup** folder has been created, the programs registered in the **ITDM2_Startup** folder are started after the packages with **Install when system starts** specified are installed. If you want the startup of the programs registered in the **ITDM2_Startup** folder to be performed earlier, specify **After the client starts**.

#7: The packages that have already been downloaded are installed when the system starts, but the packages that are downloaded later due to polling and with **Install when system starts** specified are installed next time the system starts.

#8: When this setting has been specified, even if multiple agents start at the same time, they do not try to connect to the higher system at the same time, which can distribute the load on the network. Setting a larger value for this item can reduce the load when the system performance is not sufficient for the number of agents connected to the higher system, or when too much load is placed on the network.

#9: This item is displayed only when the default agent is set.

#10: Available characters are single-byte alphanumeric characters, single-byte spaces, percent signs (%), periods (.), parentheses, backslashes (\), and underscores (_).

Password settings

Item		Description	Specifiable values	Default
Settings to protect agents	Setting Password Protection will prevent end users from modifying agent configuration and uninstallation	Specify whether to set a password to prevent users from changing the agent setup settings or performing uninstallation.	Selected A password is requested upon agent setup and uninstallation. Not selected No password is requested upon agent setup and uninstallation.	Selected
	Password	Specify the password that will be requested upon agent setup or uninstallation.	A character string of 1 to 128 ASCII characters	(Blank)
	Confirm password	Re-enter the specified password for confirmation.		
Settings to protect information from external storage media#	Use a password to protect information sent using external storage media.	Specify whether to set a password to protect information in external storage media from users.	Selected A password is requested to retrieve information from external storage media. Not selected No password is requested to retrieve information from external storage media.	Not selected
	Password	Specify the password that will be requested when information in external storage media is retrieved.	A string of 1 to 128 ASCII characters	(Blank)
	Confirm password	Re-enter the specified password for confirmation.		
Protection settings for registering USB devices	Protect USB Device Registration with Password	Specify whether to set a password to prevent the user from registering a USB device.	Selected A password is requested to register a USB device. Not selected No password is requested to register a USB device.	Not selected
	Password	Specify the password that will be requested to register the USB device.	A string of 1 to 128 ASCII characters	(Blank)
	Confirm password	Re-enter the specified password for confirmation.		

#: If the version is upgraded from JP1/IT Desktop Management earlier than 10-01 to JP1/IT Desktop Management 2, the password specified for **Settings to protect agents** is automatically set.

Relay system settings

Item			Description	Specifiable values	Default
Settings of the system where IDs will be registered	Managemen t server	Host name or IP address	As the host name or IP address of the higher system where IDs will be registered, the host name or IP address specified for	None	None

Item			Description	Specifiable values	Default
Settings of the system where IDs will be registered	Management server	Host name or IP address	**Management server** of **Basic settings** is displayed.	None	None
	System where IDs will be registered	System type	Select the type of system where IDs will be registered.	• Management server • Relay system	Relay system
		Host name or IP address	Specify the host name or IP address of the system selected by **System type** of **System where IDs will be registered**.[#1] If you selected **Relay system** for **System type** of **System where IDs will be registered** when creating an agent setting to be assigned to the relay system, Hitachi recommend that you specify `localhost`.	Host name[#2] or IPv4 address	localhost
Specify ID Key for Operations			Select the ID key for operations (information for identifying a computer) that is used for distribution using Remote Installation Manager.	• Host name When you create or execute a job, select **Use the Windows network** or **Use the system configuration information of IT Desktop Management 2** from the drop-down list as the address resolution method. (The default is **Use the Windows network**.) • IP address	Host name or IP address that was specified in the **Settings for Address Resolution** dialog box during management server setup
Settings to send notifications to JP1/IT Desktop Management 2 - Manager	Transmission timing for processing result files		Specify the timing of sending notification files received from lower systems to the managing server.	• Immediately • Periodically	Immediately
	Receive jobs and transmit result file processing in parallel		Specify whether the relay system will execute reception of jobs (download) and transmission of notification files (upload) in parallel during communication with the connected higher system (management server).	Selected Reception of jobs and transmission of processing result files are performed in parallel. Not selected Reception of jobs and transmission of processing result files are not performed in parallel.	Selected
	Notify JP1/IT Desktop Management 2 - Manager of the status of the split distribution executed on the lower JP1/IT Desktop Management 2 - Agent		Specify whether to notify the higher system of the state of progress of the split distribution (of packages) being executed on the lower system.	Selected Notification of the state of progress of the split distribution is sent to the higher system. Not selected Notification of the state of progress of the split distribution is not sent to the higher system.	Not selected

Item		Description	Specifiable values	Default
Processing settings for the relay system	Number of JP1/IT Desktop Management 2 - Agents that can be connected to the relay system concurrently	Specify the number of agents that can be connected to the relay system concurrently.	4 to 9999	50
	Number of job download requests for JP1/IT Desktop Management 2 - Agents	Specify the number of agents to be executed concurrently[#3] when a job is executed.	Specify the number of job download requests to be executed concurrently Specify the number of jobs to be executed concurrently in the range from 1 to 9999. Do not execute job download requests Because the startup message is not sent to agents, startup of agents using job execution or client control is not available.	Specify the number of job download requests to be executed concurrently (20)
	Job management file cache	Specify the upper limit of the cache size[#4] on the relay system's memory for the executed job information (management files).	Specify the upper limit of the cache size Specify the upper limit of the cache size on the memory in the range from 1 to 1,000,000 KB. Do not cache Executed job information (management files) is not cached.	Specify the upper limit of the cache size (100,000 KB)
	Monitor the startup of JP1/IT Desktop Management 2 - Agent when a job is executed	Specify whether to change the job execution status to **Startup failure** and report it to the managing server when a job is not executed because the agent is not running.	Selected The execution status of ID jobs that normally finished on the agent is reported to the relay system. Not selected The execution status of ID jobs that normally finished on the agent is not reported to the relay system.	Selected
	Subdivide the cause of startup failures	Specify whether to subdivide the cause of agent's startup failures and report it to the managing server.	Selected The cause of startup failures is subdivided. Not selected The cause of startup failures is not subdivided.	Selected

#1: If, during the setup for the management server, you specified a host name as the ID key for operations specified in **Settings for Address Resolution**, specify a host name here. If you specified an IP address, specify an IP address here.

#2: Specify the host name using a character string of 64 or fewer single-byte characters.

#3: Specifically, this number is the number of startup messages that the managing server sends to agents at one time. If the number of agents on which jobs are executed is larger than the specified value, the jobs are divided and executed based on this specified value. If 0 is specified, startup messages are not sent to the lower system, so that execution of jobs initiated by the higher system and startup of the destination using client control will not be available. Note that you must specify the size of a file to be distributed, considering the network performance. If the size is too large (10 MB or more), the network load might increase even with a few agent connections.

#4: If the total size of management files exceeds its upper limit, the throughput of job processing will decrease. Hitachi recommends that you specify an appropriate value for the upper limit of cache size of management files based on the scale of your operation environment, in order to prevent any decrease in throughput of job processing. Use the formula below to calculate the guideline value to be specified, by entering the estimated values for individual elements. If the cache size exceeds its upper limit due to an increase in the number of management files, delete the management file that is least referenced, and then cache a new management file. If **Do not cache** is selected, the job management files on a disk are accessed every time agents request polling, so replying to the agents might be delayed.

Cache size for management files (KB) = number of executed jobs stored in the relay system x number of destinations for each job x number of packages for each job (for remote installation jobs) x 1 KB

User notification settings

Item		Description	Specifiable values	Default
Settings to shut down and restart the computer#1	For user computers, display a dialog box that instructs the user to shut down or restart the computer	Specify whether the user's computer accepts the administrator's instructions for shutdown and restart of the computer.	Selected The user's computer accepts the administrator's instructions for shutdown and restart of the computer. Not selected The user's computer does not accept the administrator's instructions for shutdown and restart of the computer.	Selected
	Computer shutdown or restart timing	Specify the timing the user's computer starts shutting down or restarting when an update program or a program that requires restarting is distributed.	Automatically start if no response is received from the user within the specified period Shutdown or restart is automatically started. Specify the time to wait until the automatic startup begins in the range from 1 to 1440 minutes.#2 Follow the response of the user in the dialog box that instructs the user to shut down or restart the computer Neither shutdown nor restart is started until the user responds.	Automatically start if no response is received from the user within the specified period (3 minutes)
Display Settings on User Computers	When an action item user is notified of a message	Specify whether to display a balloon tip on the user's computer when the user receives a message that is set as the security determination result in Action Items for a security policy.	Displayed (balloon tip) A balloon tip is displayed on the user's computer. Hidden A balloon tip is not displayed on the user's computer.	Displayed (balloon tip)

Item		Description	Specifiable values	Default
Display Settings on User Computers	When users are instructed to restart the computer	Specify whether to display a balloon tip on the user's computer when restart of the computer is required due to application of security policies or software.	Displayed (balloon tip) A balloon tip is displayed on the user's computer. Hidden A balloon tip is not displayed on the user's computer.	Displayed (balloon tip)
	When a user input window is displayed	Specify whether to display, on the user's computer, the message indicating that the system administrator requests input of user information.	Displayed (user input screen) The window for entering user information is displayed on the user's computer. Displayed (balloon tip) A balloon tip is displayed on the user's computer. Hidden Neither the window for entering user information nor a balloon tip is displayed on the user's computer.	Displayed (balloon tip)
	When distributing packages (ITDM-compatible distribution)	Select whether to display a balloon tip on the user's computer when software distribution is performed.	Displayed (balloon tip) A balloon tip is displayed on the user's computer. Hidden A balloon tip is not displayed on the user's computer.	Displayed (balloon tip)
Display settings for notification dialog boxes	Display when a job fails	Specify whether the notification dialog box is displayed on the user's computer when a job fails.	Selected The notification dialog box is displayed on the user's computer. Not selected The notification dialog box is not displayed on the user's computer.	Not selected
	If a shortcut file that failed to start from **ITDM2_Startup** exists, display a message asking whether to delete the shortcut file	Specify whether to display a confirmation dialog box for deletion of icons and shortcut files that have been registered in the **ITDM2_Startup** folder and cannot be executed.#3	Selected A confirmation dialog box is displayed for deletion of icons and shortcut files that cannot be executed. Not selected The confirmation dialog box is not displayed for deletion of icons and shortcut files that cannot be executed.	Not selected

#1: This setting is ignored if the computer is the relay system.

#2: A confirmation dialog box is displayed on the user's computer until the time specified here passes.

#3: You might not be able to execute a program because the execution file of the program registered in the **ITDM2_Startup** folder has already been uninstalled. In such a case, you can set to display a confirmation dialog box asking whether to delete icons and shortcut files that cannot be executed.

Job settings

Item		Description	Specifiable values	Default
Display settings for dialog boxes indicating that a job is being processed	Display a dialog box indicating that processing is in progress	Specify whether to display a dialog box indicating that download or installation is being processed on the agent.	Selected A dialog box indicating that download or installation is being processed is displayed. Not selected A dialog box indicating that download or installation is being processed is not displayed.	Selected
	Display a dialog box indicating that a package is being downloaded	Specify whether to display a dialog box indicating that a package is being downloaded.	Selected A dialog box indicating that a package is being downloaded is displayed. Not selected A dialog box indicating that a package is being downloaded is not displayed.	Selected
	Displayed dialog box	Specify the type of dialog box indicating that download processing is in progress.	Default dialog box The dialog box provided by JP1/IT Desktop Management 2 by default is displayed. Dialog box specified by the program The specified program created by a user for displaying a dialog box is started and the corresponding dialog box is displayed.	Default dialog box
	Display a dialog box indicating that a package is being installed	Specify whether to display a dialog box indicating that a package is being installed.	Selected A dialog box indicating that a package is being installed is displayed. Not selected A dialog box indicating that a package is being installed is not displayed.	Selected
	Displayed dialog box	Specify the type of dialog box indicating that installation processing is in progress.	Default dialog box The dialog box provided by JP1/IT Desktop Management 2 by default is displayed. Dialog box specified by the program The specified program created by a user for displaying a dialog box is started and the corresponding dialog box is displayed.	Default dialog box
	Display the dialog box in the forefront	Specify whether to display the dialog box in the foreground, to indicate that installation processing is in progress.	Selected The dialog box indicating that installation processing is in	Not selected

Item		Description	Specifiable values	Default
Display settings for dialog boxes indicating that a job is being processed	Display the dialog box in the forefront	Specify whether to display the dialog box in the foreground, to indicate that installation processing is in progress.	progress is displayed in the foreground. Not selected The dialog box indicating that installation processing is in progress is not displayed in the foreground.	Not selected
	Program to display dialog boxes	Specify the name of a program to display dialog boxes when **Dialog box specified by the program** is selected as the type of dialog boxes to be displayed.	The path to a program (a program file whose extension is exe) created by a user for displaying dialog boxes.[#1]	(Blank)
Settings to perform a retry when a remote installation or remote collection fails	Perform a retry	Specify whether to perform a retry when an error occurs while remote installation or remote collection of user programs or data is in progress.	Selected A retry is performed. Not selected No retry is performed.	Selected
	Retry count	Specify the retry count that is allowed.	1 to 100	10
	Retry interval	Specify the retry interval.	Periodically perform retries Specify the interval in the range from 1 to 3600 (seconds). Immediately perform retries The specified number of retries are performed without interval.	Periodically perform retries (1 second)
Settings for split distribution of packages	Split packages to be distributed[#2]	Specify whether to split and distribute a package if it is larger than the size specified here.	Selected A package is split into the size specified here and distributed. Not selected A package is distributed without being split.	Selected
	Split size	Specify the size a package is to be split. This split size is applied to each package to be distributed.	When specified in KB: 1 to 2097151 When specified in MB: 1 to 2047	2097151KB
	Transmission suspension period	Specify the interval (suspension period) between split distributions of a package.	1 to 1440	60
Installation waiting time settings	Time to wait for a response from the installer	Specify the maximum time to wait for the response from the installer during remote installation of a Hitachi program product. If no response is received when the specified time expires, an error is reported to the higher system.	180 to 7200	1800
Settings to permit job holds[#3]	Permit users to hold jobs	Specify whether to have the user select whether to execute a job transmitted from the higher system.	Selected The user selects whether to execute the job.[#4]	Not selected

Item		Description	Specifiable values	Default
Settings to permit job holds[#3]	Permit users to hold jobs	Specify whether to have the user select whether to execute a job transmitted from the higher system.	Not selected The user does not select whether to execute the job.	Not selected
	Timing to release job holds	Specify the timing to release temporary job holds when whether to execute jobs is selected by the user.	Automatically release job holds if no user response is received within the specified period Specify the time (in the range from 1 to 1800 seconds) to wait until job holds are released.[#5] Do not release job holds until a user response is received Execution of jobs is held until the response from the user is received.[#6]	Automatically release job holds if no user response is received within the specified period (180 seconds)
Settings to suppress notifications	Suppress notifications on jobs waiting to be installed and collected	Specify whether to suppress notifications on jobs waiting to be installed or collected, to the higher system.[#7]	Selected Notifications to the higher system are suppressed. Not selected Notifications to the higher system are not suppressed.	Not selected
Interval transmission settings	Perform interval transmissions	Specify whether to split a file by the specified unit and transmit the split files at the interval during file transmission to an agent.	Selected Interval transmissions are performed. Not selected Interval transmissions are not performed.	Not selected
	Number of continuous transmission buffers	Specify the number of buffers to be used for one file transmission.	1 to 4294967295	1
	Transmission interval	Specify the interval (suspension period) between interval transmissions.	1 to 4294967295	1000

#1: A program created by a user for displaying dialog boxes does not have to display a dialog box. However, it must satisfy the conditions below, including parameters and the window name. Even if the specified user program does not display a dialog box correctly due to an error in the settings, or other reason, the processing continues regardless of the user program's behavior.

The specification format of the arguments that are passed to a program for displaying dialog boxes is shown below. Refer to this format when you create a user program.

Format

```
parameter-1 parameter-2 parameter-3 parameter-4
```

parameter-*1*

Specify whether to always display dialog boxes on top (1 single-byte character).

1: Dialog boxes are not displayed on top.

2: Dialog boxes are always displayed on top.

parameter-*2*

Specify the type of dialog box being processed (1 single-byte character).

1: Dialog box during download

2: Dialog box during installation

parameter-*3*

Package ID (1 to 44 single-byte characters)

parameter-*4*

Package name (1 to 50 single-byte characters)

Example

The following are examples for specifying individual types of dialog boxes:

- Dialog box during download

```
1 1 package-ID package-name
```

- Dialog box during installation (when it is not displayed on top)

```
1 2 package-ID package-name
```

- Dialog box during installation (when it is always displayed on top)

```
2 2 package-ID package-name
```

Window name of the dialog box to be displayed

The window name must be the ones shown below. If you set a window name other than these, you will not be able to hide the dialog box. For the katakana in the window name, specify single-byte kana characters.

- Dialog box during download
  IT Desktop Management 2 - Download
- Dialog box during installation
  IT Desktop Management 2 - Installation

JP1/IT Desktop Management 2 issues the PostMessage function (with WM_CLOSE specified) to direct the user program to stop displaying the dialog box, and then issues the TerminateProcess function to stop the user program process.

#2: Select this check box when you want to reduce the network load. Note that, even if a package for which split distribution is set is distributed, split distribution is not performed if this check box is cleared.

#3: This setting is ignored for the relay system.

#4: When a job is transmitted from the higher system, the **JP1/IT Desktop Management 2 Job Suspended** dialog box is displayed, and the user can select whether to execute the job. If the user does not want to execute the job immediately, execution of the job can be temporarily suspended. Note that only the **Install package** jobs in the GUI installation mode can be suspended unless the execution date (installation date and time of the package, or execution date and time of the job) is specified.

#5: The specified number of seconds is displayed (as the remaining time until the execution) in the **JP1/IT Desktop Management 2 Job Suspended** dialog box. If the value becomes 0, the displayed job is automatically executed, and the dialog box closes.

#6: The **JP1/IT Desktop Management 2 Job Suspended** dialog box remains displayed until the user operates on the dialog box.

#7: Usually, the display of the **Job status** window changes at each notification because there is a time gap until completion (or failure) of installation or collection is reported to the higher system after completion of job distribution. However, completion or failure might be reported immediately after notifications on jobs waiting to be installed and collected. If you suppresses notifications, you can reduce the network load (traffic of 170 bytes (340 bytes for ID jobs) for each notification), You can also reduce update processing for the job status on the higher system. You can suppress the following types of jobs:

- Install package
- Collect files from client
- Collect files from client to relay system

When the above types of jobs are executed, notifications are suppressed if both *Job specification* and *Suppression condition* in the following table are satisfied.

Job specification			Suppression condition
Installation date/time	Install when system starts	GUI installation mode	
Yes[#1]	No	No	The specified date and time had passed when distribution of the job was completed.
No	Yes	No	• **Before the system starts** has been set for **Polling timing** on the agent. • The job was distributed during polling at system startup.
Yes	Yes	No	• **Before the system starts** has been set for **Polling timing** on the agent. • The job was distributed during polling at system startup. • The specified date and time had passed when distribution of the job was completed.
No	No	Yes[#2]	Logon to the agent had finished when distribution of the job was completed.
Yes	No	Yes[#2]	• The specified date and time had passed when distribution of the job was completed. • Logon to the agent had finished when distribution of the job was completed.
No	Yes	Yes[#2]	• **Before the system starts** has been set for **Polling timing** on the agent. • The job was distributed during polling at system startup. • Logon to the agent had finished when distribution of the job was completed.
Yes	Yes	Yes[#2]	• **Before the system starts** has been set for **Polling timing** on the agent. • The job was distributed during polling at system startup. • The specified date and time had passed when distribution of the job was completed. • Logon to the agent had finished when distribution of the job was completed.

Legend: Yes: Specified. No: Not specified.

#1: The *Collect files from client* and *Collect files from client to relay system* jobs are not subject to suppression.

#2: Only the *Install package* jobs are subject to suppression.

Communication settings

Item		Description	Specifiable values	Default
Settings to perform polling for multiple higher systems[#1]	Perform polling for multiple higher systems	Specify whether to perform polling (monitoring of directions from the managing server) for multiple higher systems when the managing server can execute a job using multiple paths.[#2] The following higher systems can be set for the polling targets: • Management server • Relay system Do not set to perform polling for multiple higher systems in the following cases: • When you create an agent setting to be assigned to the relay system • When you edit the default agent setting	Selected Polling is performed for multiple higher systems. To add a higher system to the polling targets, click the **Add** button. Then, in the displayed dialog box, specify the host name or IP address, type, and priority of the higher system. The added higher systems are displayed in **Higher-level system to be polled** in the order of a priority.[#3] Not selected Polling is not performed for multiple higher systems.	Not selected
	Type of polling for multiple higher systems	Select, from the drop-down list, the type of polling to be performed when the relay system (the polling-target higher system) cannot be connected due to a failure.	Hot standby Polling is performed for higher systems displayed in **Higher-level system to be polled** in the order of higher priority, and then a higher system that can be connected is regarded as the polling-target higher system.[#4] To add a higher system to the polling targets, click the **Add** button. Then, in the displayed dialog box, specify the host name or IP address, type, and priority of the higher system. Select the type of polling at system startup (the first polling) from the following three types: • Poll all higher systems when the system starts • Poll only higher systems whose priority is 1 when the system starts • Poll higher systems according to their priority when the system starts Multiple hosts Polling is performed for all higher systems.	Hot standby (Poll all higher systems when the system starts)
Communication protocol for receiving execution requests	Use the received IP address for connections with higher systems[#5]	Specify whether to allow connection to the higher system even when name resolution for the higher system is not available.	Selected Connection to the higher system is available because when an execution request is received from the higher system, the IP address of the	Selected

Item		Description	Specifiable values	Default
Communication protocol for receiving execution requests	Use the received IP address for connections with higher systems[#5]	Specify whether to allow connection to the higher system even when name resolution for the higher system is not available.	higher system in that request information is saved. Not selected Connection to the higher system is not available when name resolution for the higher system is not available.	Selected
Communication error settings	Timing to assume that a communication error occurred	Specify whether the agent will wait for responses from communication software and assume that a communication failure occurred if no response is received.	Assume that a communication failure occurred if no response is received from communication software within the specified period Specify the time to wait for responses from communication software in the range from 1 to 120 minutes.[#6] Do not monitor responses from communication software Responses from communication software is not monitored.	Assume that a communication failure occurred if no response is received from communication software within the specified period (5 minutes)
Settings to perform retries when an error occurs	Perform a retry when a socket connection establishment error occurs, and when a file transmission error occurs	Specify whether to perform a retry when a socket connection establishment fails or when a communication error occurs during file transmission from the higher system to the agent.[#7]	Selected A retry is performed. Not selected No retry is performed.	Selected
	Retry count	Specify the number of retries that are allowed when a socket connection establishment fails or when a communication error occurs during file transmission.	1 to 999	5
	Retry interval	Specify the retry interval (in seconds) for when a socket connection establishment fails or when a communication error occurs during file transmission.	1 to 7200	5
Non-transmitted processing result files	Retransmit non-transmitted processing result files to higher systems	Specify whether to retry a transmission when there is a notification file that has not been sent to the higher system.	Selected A retry is performed. Not selected No retry is performed.	Selected
	Retry count	Specify whether to specify the retry count of transmissions when there is a notification file that has not been sent to the higher system.	Specify Specify the retry count in the range from 1 to 300. Do not limit Retries are repeated until all notification files have been transmitted.	Specify (2)
	Retry interval	Specify the retry interval (in seconds) for transmissions when there is a notification file that has	60 to 3600	300

Item			Description	Specifiable values	Default
Non-transmitted processing result files	Retry interval		not been sent to the higher system.[#8]	60 to 3600	300
Multicast distribution settings (distribution by Remote Installation Manager)	Use the multicast address to transmit jobs		Specify whether to use the multicast address to transmit jobs during distribution using Remote Installation Manager.	Selected The multicast address is used to transmit jobs during distribution using Remote Installation Manager. Not selected The multicast address is not used to transmit jobs during distribution using Remote Installation Manager.	Not selected
	Multicast address		Specify the multicast address that is to be used to transmit jobs for which multicast distribution is specified. Specify the multicast address that has been set for the connection-destination higher system.[#9]	224.0.1.0 to 239.255.255.255	238.255.0.1
	Upper limit of the job transmission packet size		Specify the size of a packet used for distribution of jobs.	1 to 60	40[#10]
	Use the multicast address to receive jobs		Specify whether to use the multicast address to receive jobs during distribution using Remote Installation Manager.	Selected The multicast address is used to receive jobs during distribution using Remote Installation Manager. Not selected The multicast address is not used to receive jobs during distribution using Remote Installation Manager.	Not selected
	Port number	Normal reception	Specify the port number used to receive jobs during multicast distribution.	1 to 65535	The port number specified for **Multicast distribution** of **Port numbers** under **Multicast Distribution** in the **Setup for Distribution by Using Remote Install Manager** dialog box during the management server setup
		Reception for retransmissions	Specify the port number used when retransmissions of packets occur during multicast distribution.[#11]	1 to 65535	The port number specified for **Multicast distribution (when retransmission is required)** of **Port numbers** under **Multicast Distribution** in the

Item			Description	Specifiable values	Default
Multicast distribution settings (distribution by Remote Installation Manager)	Port number	Reception for retransmissions	Specify the port number used when retransmissions of packets occur during multicast distribution.[#11]	1 to 65535	**Setup for Distribution by Using Remote Install Manager** dialog box during the management server setup
	Multicast address		Specify the multicast address that is to be used to receive jobs for which multicast distribution is specified. Specify the multicast address that is set for the connection-destination higher system.[#9]	224.0.1.0 to 239.255.255.255	238.255.0.1

#1

This setting is ignored for the relay system.

#2

Usually, the agent receives a direction from the managing server and executes the requested processing. However, no directions might be received as a result of, for example, a communication error, or the agent not running. In such a case, the agent can use polling to receive directions. If you use client control, Hitachi recommends that you use polling. If you use a low-speed WAN, you can reduce unnecessary data transmissions and receptions by not using polling.

#3

The higher system with the highest priority displayed in **Higher-level system to be polled** is always the same as the one specified in **Higher-level system for distribution that uses Remote Install Manager** of **Basic settings**.

#4

If the connection to the polling-target higher system becomes unavailable, polling is performed for the higher systems in the order of higher priority, and then a new polling-target higher system is determined.

#5

- This setting is not necessary if the ID key for operations is an IP address.
- If the higher system is a cluster system, connection with the higher system might not be correctly established.
- In an environment in which the higher system uses multiple network adapters, connection with the higher system might not be correctly established.

#6

You can monitor the agent's processing, such as downloading files.

#7

If a retry is performed, the file transmission resumes from the point where the file transmission was suspended. Thus, you can reduce unnecessary traffic because the part of the file that has already been transmitted before the communication error will not be transmitted again. Note that the retry count and retry interval that are specified here are enabled for unicast distribution only.

#8

For the retry interval for transmissions when there is a notification file that has not been sent to the higher system, specify an appropriate value according to the system requirements. For example, for a security audit system (for which information from clients is immediately required), specify a small value.

#9

If you set for this item the multicast address that is set for the connection-destination higher system, this system will be registered in the multicast group that was set as the distribution destination of the higher system.

#10

A value of 40 KB is efficient enough for 100BASE communication lines. If the communication line is 10BASE, specify 4 KB. Note that, if the packet size is too large, multicast distribution might fail and change to unicast distribution from the middle of distribution.

#11

Because multicast distribution uses the UDP protocol, resending of packets occurs during distribution. Therefore, you must set the port number used for a request for resending.

Startup settings

Item	Description	Specifiable values	Default
Create the startup folder (**ITDM2_Startup**) for only IT Desktop Management 2[#1]	Specify whether to create the ITDM2_Startup folder that is used to move the programs registered in the Windows **Startup** group.[#2]	Selected The ITDM2_Startup folder is created. Not selected The ITDM2_Startup folder is not created.	Not selected
Move startup programs into the **ITDM2_Startup** folder	If you create the ITDM2_Startup folder, specify whether to automatically move the programs registered in the Windows **Startup** group to the ITDM2_Startup folder on the agent.	Selected The programs registered in the Windows **Startup** group are automatically moved to the ITDM2_Startup folder. To move a specific program to the ITDM2_Startup folder, click the **Add** button. Then, in the displayed dialog box, specify the program. The specified program is displayed in **Startup program (shortcut file) to be moved**. Not selected The programs registered in the Windows **Startup** group are not automatically moved to the ITDM2_Startup folder.	Not selected

#1: The **ITDM2_Startup** folder has not been created by default.

#2: If you move the programs registered in the Windows **Startup** group to the ITDM2_Startup folder, you can avoid installation failure of packages for which **Install when system starts** is set. This installation failure is caused by the conflict between the installation of packages for which **Install when system starts** is set and the startup of the programs registered in the Windows **Startup** group on the agent.

AMT Settings

Item	Description	Specifiable values	Default
Allow IDE Redirection	Specify whether to use the AMT IDE redirection function to use the remote CD-ROM function during remote control.	Selected The remote CD-ROM function is used.	Not selected

Item	Description	Specifiable values	Default
Allow IDE Redirection	Specify whether to use the AMT IDE redirection function to use the remote CD-ROM function during remote control.	Not selected The remote CD-ROM function is not used.	Not selected
Allow Remote KVM	Specify whether to use the AMT remote KVM function to enable remote control of computers via RFB connection.	Selected Remote control of computers via RFB connection is enabled. Not selected Remote control of computers via RFB connection is disabled.	Not selected
Password	Specify the password required for using the remote KVM function of the destination computer.	A character string of 8 or fewer single-byte characters#	(Blank)
Retype Password	Enter the specified password again for confirmation.	A character string of 8 or fewer single-byte characters#	(Blank)
Confirm permission for the connection to the user.	Specify whether to display a confirmation dialog box during connection to a computer.	Selected A confirmation dialog box is displayed during connection to the computer. Not selected No confirmation dialog box is displayed during connection to the computer.	Selected
Display time of dialog (seconds)	Specify how long (seconds) the connection confirmation dialog box is displayed.	10 to 4095	300
Session Timeout (minutes)	Select whether a timeout occurs when the computer cannot be connected to.	Do A timeout occurs. Specify, in the range from 1 to 255, the wait time (minutes) that can elapse before a timeout occurs. Not Do A timeout does not occur.	Not Do
Default Screen	Select the display to be used when the destination computer has a dual display.	• Primary • Secondary	Primary

#

You need to use at least one character for each of the following types:

- Uppercase letter
- Lowercase letter
- Number
- Symbols other than ", comma (.), and colon (:)

Remote control settings

Item		Description	Specifiable values	Default
Activation Process	Remote Control Agent Starts Automatically	Specify whether to automatically start Remote Control Agent when the agent starts.	Selected Remote Control Agent starts automatically. Not selected Remote Control Agent does not start automatically.	Selected
	Display Icon in Taskbar	Specify whether to display an icon on the Windows taskbar when Remote Control Agent is running.	Selected An icon is displayed. Not selected An icon is not displayed.	Selected
	Allow end user to terminate the remote control session in Agent	Specify whether to allow the user to terminate Remote control Agent.	Selected The user is allowed to terminate Remote Control Agent. Not selected The user is not allowed to terminate Remote Control Agent.	Not selected
After Disconnecting Remote Control		Select the processing to be performed when connection between Remote Control and the management server is disconnected.	• Keep Remote Control Agent Running • Terminate Remote Control Agent	Keep Remote Control Agent Running
Connection Settings	Remote Control Port	Specify the port number used for the standard connection.	1 to 65532	The port number specified for **Remote Control port number** in the **Port Number Settings** dialog box during the management server setup
	RFB Port	Specify the port number used for the RFB connection.	1 to 65535	5900
Request Server	Connection Destination	Specify the default destination used when a computer requests connections.	Host name# or IPv4 address	Host name or IP address of the management server
File Transfer	Select whether to allow file transfer between the management server and computers.		• Deny File Transfer • Allow File Transfer	Allow File Transfer
	Read File From Agent	Specify whether to allow reading files from the computer during file transfer.	Selected Reading files from the computer is allowed. Not selected Reading files from the computer is not allowed.	Selected
	Write File to Agent	Specify whether to allow writing files to the computer during file transfer.	Selected Writing files to the computer is allowed.	Selected

Item		Description	Specifiable values	Default
File Transfer	Write File to Agent	Specify whether to allow writing files to the computer during file transfer.	Not selected Writing files to the computer is not allowed.	Selected
Chat	Start the chat server when remote control agent starts	Specify whether to start the chat server when Remote Control Agent starts.	Selected The chat server is started. Not selected The chat server is not started.	Not selected
	Display Icon in Taskbar	Specify whether to display an icon on the Windows taskbar when the chat server is running.	Selected An icon is displayed. Not selected An icon is not displayed.	Selected
	Open chat window when chat client connects chat server	Specify whether the **Chat** window opens automatically when another computer establishes a chat connection while the chat server is running.	Selected The **Chat** window opens automatically. Not selected The **Chat** window does not open automatically.	Not selected
Settings of allowed controllers	Allowed Controller List	Specify the computer allowed for remote control connection.	Host name or IPv4 address	None
User Authentication	Allowed Use List	Specify the authentication information that the controller will be asked for during remote control connection.	Windows authentication information or any authentication information (user name and password)	None
Connection Confirmation	Display user-response dialog box on user computers	Specify whether to display a confirmation dialog box for remote control during connection from the management server.	Selected A confirmation dialog box is displayed during connection. Not selected A confirmation dialog box is not displayed during connection.	Not selected
	Dialog box display	Specify the display period of a confirmation dialog box that asks the user for permission for remote control.	Specify the display period Specify, in the range from 1 to 180 seconds, the display period of a confirmation dialog box that asks the user for permission for remote control. Keep the dialog box displayed until a response is received A dialog box remains displayed until user response is received.	Specify the display period (10 seconds)
	When no user response is received	Select the operation to be performed when the user	• Connect • Do not connect	Connect

Item		Description	Specifiable values	Default
Connection Confirmation	When no user response is received	does not respond to the confirmation dialog box that asks the user for permission for remote control.	- Connect - Do not connect	Connect
Connection Mode		Select the connection mode to be allowed by the destination computer.	- Exclusive - Shared - View	Shared

#

Specify the host name using a character string of 255 or fewer characters.

(5) Installation set parameters

The following tables list and describe the parameters in the **Installation Set Creation** dialog box that opens from **Agent Configuration and Installation Set Creation** view in the Settings module.

Installation folder settings

Item	Description	Specifiable values	Default
Installation folder	Specify the path name to the folder in which JP1/IT Desktop Management 2 - Agent is to be installed.	A path consisting of 104 or fewer characters#	%ProgramFiles%\Hitachi \jp1itdma

#: Available characters are single-byte alphanumeric characters, single-byte spaces, periods (.), parentheses, colons (:), underscores (_), and backslashes (\).

Account settings

Item	Description	Specifiable values	Default
Set the account to install Agent.	Specify whether to set account information required for users who do not have administrator permissions to install agents.	Selected The account information required for users who do not have administrator permissions to install agents is set. Not selected The account information required for users who do not have administrator permissions to install agents is not set.	Not selected
Administrative Account Name	Specify an account (user name) who has administrator permissions.	A character string of 276 or fewer single-byte characters	(Blank)
Password	Specify the password for the account (user name) who has administrator permissions.	A character string of 128 or fewer single-byte characters	(Blank)
Confirm password	Re-enter the specified password for confirmation.		

Component settings

Item	Description	Specifiable values	Default
Component to be installed	Specify the type of component to be installed (whether the component is to be installed as an agent or relay system).	- JP1/IT Desktop Management 2 - Agent (agent) - JP1/IT Desktop Management 2 - Agent (relay system)	Agent
Remote control agent	Specify whether to install Remote Control Agent.	Selected Remote Control Agent is installed. Not selected Remote Control Agent is not installed.	Not selected

Settings for the registration-destination ID

Item	Description	Specifiable values	Default
Registration-destination ID	Specify the ID for agent registration (the group used for receiving jobs from the managing server). You can create an ID by entering the ID name in the dialog box opened by clicking the **Register** button.	A character string of 32 or fewer characters	(Blank)

Settings for the file to be deployed

Item	Description	Specifiable values	Default
Files to be deployed	Specify the files to be deployed upon agent installation (and the deploy-destination folder) in the dialog box opened by clicking the **Add** button.	Files to be deployed A character string of 100 or fewer characters Deploy-destination folder A character string of 255 or fewer single-byte characters	(Blank)

Settings for the file to be automatically executed

Item	Description	Specifiable values	Default
Files to be automatically executed	Specify the program that is to be automatically executed after agent installation, the files required for automatic execution, and the arguments# in the dialog box opened by clicking the **Add** button.	The name of the program to be automatically executed, and the name of files required for automatic execution A character string of 100 or fewer characters File path A character string of 255 or fewer single-byte characters	(Blank)

#: Specify each argument by using a character string of 127 or fewer characters.

Settings for an overwrite installation

Item	Description	Specifiable values	Default
Perform an overwrite installation of the agent	Specify whether to perform an overwrite installation if an agent has already been installed.	Selected An overwrite installation is performed. Not selected An overwrite installation is not performed.	Selected
Register the agent to the specified **registration-destination ID**	Specify whether to register the agent to the specified ID upon overwrite installation.	Selected The agent is registered to the specified ID upon overwrite installation. Not selected The agent is not registered to the specified ID.	Selected
Deploy the files specified in **Files to be deployed**	Specify whether to deploy the files specified in **Files to be deployed** upon overwrite installation.	Selected The files specified in **Files to be deployed** are deployed upon overwrite installation. Not selected The files specified in **Files to be deployed** are not deployed.	Selected
Execute the files specified in **Files to be automatically executed**	Specify whether to execute the files specified in **Files to be automatically executed** upon overwrite installation.	Selected The files specified in **Files to be automatically executed** are executed upon overwrite installation. Not selected The files specified in **Files to be automatically executed** are not executed.	Selected

(6) Parameters for configuring Active Directory searches

The following tables list and describe the parameters in the **Active Directory** view displayed from the **Configurations** view in the Settings module.

Discovery Schedule

Item	Description	Specifiable values	Default
Auto Discovery Schedule	Specify whether to set a schedule to perform searches regularly.	Selected Searches are performed regularly according to a schedule. Not selected Regular searches are not performed.	Selected
Start At	Specify the start time for searches.	00:00 to 23:59	23:00
Repeat Interval	Specify the unit of the interval at which you want to perform searches.	• Daily • Weekly • Monthly	Daily

Item	Description	Specifiable values	Default
Repeat	Specify details of the repeat interval.	The specifiable values depend on the item selected for **Repeat Interval**. For Daily: 1 to 31 For Weekly: Sunday to Saturday For Monthly: You can specify the date (1 to 31), or the week of the month (first to fourth or last) and the day of the week (Sunday to Saturday).	1

Discovery Option

Item	Description	Specifiable values	Default
Auto-Manage Discovered Nodes	Specify whether to automatically register discovered Windows computers as management targets.	Selected The discovered computers are automatically registered as management targets. Not selected The discovered computers are not automatically registered as management targets.	Selected
Auto-Install Agent	Specify whether to automatically install agents on Windows computers discovered by a search.	Selected Agents are automatically installed on the discovered computers. Not selected Agents are not automatically installed on the discovered computers.	Not selected

Notification of Discovery Completion

Item	Description	Specifiable values	Default
Report to	Set the user account to which an email is sent when the search is completed.	Registered user accounts	None

(7) Parameters for configuring network searches

The following tables list and describe the parameters in the **IP Address Range** view displayed from the **Configurations** view in the Settings module.

Search range settings

Item	Description	Specifiable values	Default
IP Address Range	Set the search range used for a network search.	A search range	Management server segment#

Item	Description	Specifiable values	Default
Discovery Range Name	Specify the name of the search range.	A name consisting of 255 or fewer characters	New search range name
From	Specify an IPv4 IP address as the start value of the search range.	An IPv4 IP address	(Blank)
To	Specify an IPv4 IP address as the end value of the search range.	An IPv4 IP address	(Blank)
Credentials Used	Specify the authentication information used to search the specified range.	Any All the registered authentication information items are used. Select Select the authentication information you want to use.	Any

#: For the management server segment, the range of IP addresses in the network segment that contains the management server is specified, and **Any** is selected for **Credentials Used**.

Credentials Used

Item	Description	Specifiable values	Default
Credentials Used	Set the authentication information used for a network search.	Authentication information	SNMP standard#1
Credential Name	Specify the name used for managing authentication information.	A name consisting of 255 or fewer characters	New authentication name
Protocol	Select the type of authentication information.	• SNMP • Windows	SNMP
Port#2	Specify the port number used by SNMP.	1 to 65535	161
Community Name#2	Specify the community name.	A name consisting of 255 or fewer single-byte characters	(Blank)
User ID#3	Specify the user ID with which Windows administrative shares can be authenticated. To specify a domain user for authentication, use *user-ID@FQDN* (FQDN: Fully Qualified Domain Name) or *domain-name\user-ID* format. For FQDN, specify a full domain name without omitting host and subdomain names. For example: `User001@PC001.hitachi.com`.	An ID consisting of 276 or fewer characters	(Blank)
Password#3	Specify the password for the user ID.	A password consisting of 127 or fewer single-byte characters	(Blank)
Retype Password#3	Specify the password again.	A password consisting of 127 or fewer single-byte characters	(Blank)

#1: For SNMP standard, **SNMP** is selected for **Protocol**, `161` is specified for **Port**, and `public` is specified for **Community Name**.

#2: Displayed when **SNMP** is selected for **Protocol**.

#3: Displayed when **Windows** is selected for **Protocol**.

Discovery Schedule

Item	Description	Specifiable values	Default
Auto Discovery Schedule	Specify whether to set a schedule to perform searches regularly.	Selected Searches are performed regularly according to a schedule. Not selected Regular searches are not performed.	Not selected
Start At	Specify the start time for searches.	00:00 to 23:59	12:00
Repeat Interval	Specify the unit of the interval at which you want to perform searches.	• Daily • Weekly • Monthly	Daily
Repeat	Specify details of the repeat interval.	The specifiable values depend on the item selected for **Repeat Interval**. For Daily: 1 to 31 For Weekly: Sunday to Saturday For Monthly: You can specify the date (1 to 31), or the week of the month (first to fourth or last) and the day of the week (Sunday to Saturday).	1

Discovery Option

Item	Description	Specifiable values	Default
Auto-Manage Discovered Nodes	Specify whether to automatically register discovered Windows computers as management targets.	Selected The discovered computers are automatically registered as management targets. Not selected The discovered computers are not automatically registered as management targets.	Selected
Auto-Install Agent	Specify whether to automatically install agents on Windows computers discovered by a search.	Selected Agents are automatically installed on the discovered computers.	Not selected

Item	Description	Specifiable values	Default
Auto-Install Agent	Specify whether to automatically install agents on Windows computers discovered by a search.	Not selected Agents are not automatically installed on the discovered computers.	Not selected

Notification of Discovery Completion

Item	Description	Specifiable values	Default
Report to	Set the user account to which an email is sent when the search is completed.	Registered user accounts	None

(8) Agentless management parameters

The following table lists and describes the parameters in the **Agentless Management** dialog box that opens from the **Agent** view in the Settings module.

Item	Description	Specifiable values	Default
Auto Monitoring Schedule	Select whether to collect device information from agentless devices regularly.	Selected Device information is collected from agentless devices. Not selected Device information is not collected from agentless devices.	Selected
Update Interval	Specify the interval for collecting device information from agentless devices.	1 to 24	1

(9) Security schedule parameters

The following table lists and describes the parameters in the **Security Schedule** view that opens from the Settings module.

Item	Description	Specifiable values	Default
Judgment Time	Specify the time at which the computer security status is determined.	00:00 to 23:59	00:00
Judgment Interval (days)	Specify the interval (number of days) at which the security status is determined.	1 to 31	1

(10) Operation log settings parameters

The following tables list and describe the parameters in the **Operation Log Settings** view in the Settings module.

Automatic restoration of operation logs

Item	Description	Specifiable values	Default
Automatically restore operation logs	Specify whether to automatically restore the operation logs that are received.	Selected Operation logs are automatically restored. Not selected Operation logs are not automatically restored.	Selected
Period for storing automatically restored operation logs	Specify the period for which automatically restored operation logs are to be stored in the operation log database.	1 to 300#	30

#: The maximum specifiable value is the value obtained by subtracting the manually restored days from the value specified in **Maximum number of days for which operation logs are to be stored in the database** during management server setup.

Export of operation logs

Item	Description	Specifiable values	Default
Periodically export operation logs	Specify whether to periodically export the operation logs that are received.	Selected Operation logs are exported periodically. Not selected Operation logs are not exported.	Not selected

(11) Parameters for configuring automatic update of the network control list

The following table lists and describes the parameters in the **Automatic Updates on Network Filter List** view displayed from the **Network Filter Settings** view via the **Network Access Control** view of the Settings module.

Automatic Updates on Network Filter List

Item	Description	Specifiable values	Default
Enable all automatic updates	Select whether to enable automatic updating of the network control list.	Selected Automatic updating of the network control list is enabled for all operations. Not selected Automatic updating of the network control list is enabled for add operations only.	Not selected

(12) AMT parameters

The following tables list and describe the parameters in the **AMT Settings** view that opens from **Inventory** in the Settings module.

Credentials Used

Item	Description	Specifiable value	Default
User ID	Enter the user ID used for connecting to AMT of a managed computer.	A string of no more than 64 ASCII characters that does not include control characters.	(Blank)
Password	Specify the password for the user ID.	A string of no more than 64 ASCII characters that does not include control characters.	(Blank)
Retype Password	Enter the password again for confirmation.	A string of no more than 64 ASCII characters that does not include control characters.	(Blank)

Password for administrative privileges

Item	Description	Specifiable value	Default
Password	Set the password for administrative privileges for AMT.	A string of 8 to 32 ASCII characters (0x20 to 0x7E)#1. The password must contain at least one lowercase letter, one uppercase letter, one numeral, and one symbol#2.	(Blank)
Retype Password	Enter the password again for confirmation.	A string of 8 to 32 ASCII characters (0x20 to 0x7E)#1. The password must contain at least one lowercase letter, one uppercase letter, one numeral, and one symbol#2.	(Blank)

#1: You cannot specify colons (`:`), commas (`,`), or double quotation marks (`"`).

#2: You cannot specify underscores (_).

(13) Revision history configuration parameters

The table below shows the parameters in the **Revision History Settings** view displayed from the **Device** view in the Settings module.

Collection of revision history

Item	Description	Specifiable values	Default
Collect revision history	Specify whether to collect a revision history for device information.	Selected A revision history of device information is collected. Not selected A revision history of device information is not collected.	Not selected

Revision History Collection Targets

Item	Description	Specifiable values	Default
Device Inventory	Select the device information for which to acquire revision history.	Selected A revision history is kept for the selected item. Not selected A revision history is not kept for the item.	All device information is selected

(14) Parameters for the report duration and start date

The following table lists and describes the parameters in the **Duration and Start Date** view that opens from **Reports** in the Settings module.

Item	Description	Specifiable values	Default
Select the storage duration of the report.	Specify the storage duration of reports.	1 year to 10 years	5 years
Select the start day of week.	Specify the start day of the week on which reports are calculated.	Sunday to Saturday	Monday
Select the start day of month.	Specify the start day of the month on which reports are calculated.	1 to 31	1
Select the start month of year.	Specify the start month of the year on which reports are calculated.	January to December	April

(15) Summary report parameters

The following tables list and describe the parameters in the **Summary Report Notifications** view that opens from **Reports** in the Settings module.

Daily Summary

Item	Description	Specifiable values	Default
Select Daily Summary recipients	Select the user ID to which you want to send daily summaries. If an email address has not been specified, enter the email address.	Email character string	The user account specified in the **Account Management** view is displayed.

Weekly Summary

Item	Description	Specifiable values	Default
Select Weekly Summary recipients	Select the user ID to which you want to send weekly summaries. If an email address has not been specified, enter the email address.	Email character string	The user account specified in the **Account Management** view is displayed.

Monthly Summary

Item	Description	Specifiable values	Default
Select Monthly Summary recipients	Select the user ID to which you want to send monthly summaries. If an email address has not been specified, enter the email address.	Email character string	The user account specified in the **Account Management** view is displayed.

(16) Event notification parameters

The following tables list and describe the parameters in the **Event Notifications** view that opens from **Events** in the Settings module.

Select the category and severity of events about which you want to be notified by email:

Item	Description	Specifiable values	Default
Critical, Warning, and Information	Select the severity (**Critical**, **Warning**, and **Information**) of events for which you want to send notification emails.	Selected Event notification emails are sent. Not selected Event notification emails are not sent.	Only **Critical** is selected.
Security	Set events related to security management, such as changes and allocation of policies, judgement results, action results, and startup suppression.	Selected Notification emails for the selected events. Not selected Event notification emails are not sent.	All categories under **Critical** are selected.
Suspicious Operations	Set events related to suspicious operations, such as detection of emails with attachments, detection of file upload to a Web server or FTP server, and detection of copying or moving of files to external media.		
Assets	Set events related to asset management, such as asset registration, change of the asset status, and addition or deletion of software licenses.		
Distribution (ITDM-compatible)	Set events related to ITDM-compatible distribution functions, such as installation and uninstallation of software, and distribution of files.		
Inventory	Set events related to device management, such as addition and deletion of software, and addition and deletion of computer accounts.		
Settings	Set events related to settings, such as discovery of devices, addition of management targets, and agent distribution.		
Error	Set events related to errors that occur in functions.		

Select recipients:

Item	Description	Specifiable values	Default
Select recipients	Select the user IDs to which you want to send event notification emails. If an email address has not been specified, enter the email address.	Email character strings	User account specified in the **Account Management** view

Interval of notification

Item	Description	Specifiable values	Default
Interval of notification	Specify the interval (number of minutes) at which event notifications are sent.	1 to 1440	30

(17) Mail server parameters

The following table lists and describes the parameters in the **SMTP Server** view that opens from **General** in the Settings module.

SMTP Server Settings

Item	Description	Specifiable values	Default
Host Name	Enter the host name of the SMTP server.	The host name of the SMTP server	(Blank)
Secure Connection	Select the security protection used for communication with the SMTP server.	• Plain • TLS	Plain
Port	Specify the port number of the SMTP sever.	1 to 65535	25
Source E-mail	Specify the source email address of notification emails.	Email character string	(Blank)
Use Authentication	Select **Use Authentication** to use the user authentication function (SMTP Authentication) on the SMTP server.	Selected SMTP authentication is used. Not selected SMTP authentication is not used.	Not selected.
User ID	Enter the user ID used for user authentication.	User ID used for user authentication	(Blank)
Password	Specify the password for the user ID.	Password for the user ID	(Blank)
Retype Password	Enter the password again for confirmation.	Password for confirmation	(Blank)

(18) Active Directory parameters

The following table lists and describes the parameters in the **Active Directory** view that opens from **General** in the Settings module.

Item	Description	Specifiable values	Default
Get Department Hierarchy Information	Specify whether to acquire the organization hierarchy from Active Directory and apply it to the group configuration of the department.	Selected Organization hierarchy information managed by Active Directory is applied to the group configuration of the department. Not selected Organization hierarchy information managed by Active Directory is not applied to the group configuration of the department.	Not selected
Domain Name	Specify the domain name of the Active Directory server.	A character string of 0 to 255 ASCII characters that does not include the following. Domain names cannot begin with a period (.). • ASCII control characters	(Blank)

Item	Description	Specifiable values	Default
Domain Name	Specify the domain name of the Active Directory server.	- Single-byte spaces, exclamation marks (!), double quotation marks ("), hash marks (#), dollar signs ($), percent signs (%), ampersands (&), parentheses, asterisks (*), plus signs (+), commas (,), single quotation marks ('), forward slashes (/), colons (:), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), question marks (?), at marks (@), left square brackets ([), backslashes (\\), right square brackets (]), carets (^), grave accent marks (`), left curly brackets ({), vertical bars (|), right curly brackets (}), and swung dashes (~)	(Blank)
Host Name	Specify the host name of the Active Directory server (fully modified domain name).	A character string of 0 to 255 ASCII characters that does not include control characters	(Blank)
Port	Enter the port number used for connecting to the Active Directory server.	1 to 65535	389
User ID	Enter the user ID used for connecting to the Active Directory server.	A character string of 0 to 276 ASCII characters that does not include control characters	(Blank)
Password	Specify the password for the user ID.	A character string of 0 to 64 ASCII characters that does not include control characters	(Blank)
Retype Password	Enter the password again for confirmation.	A character string of 0 to 64 ASCII characters that does not include control characters	(Blank)
Root OU	Enter the domain name and OU names separated by slashes (/) to specify the path to the root organizational unit (OU) for which you want to acquire information. The entered values are not case sensitive. For example, when the domain name is `hitachi.co.jp` and the OU names are `general affairs department` and `general affairs section`, enter `hitachi.co.jp/general affairs department/general affairs section`. The domain name must be entered. OU names are optional. When you acquire information on a department, the hierarchy under the path specified here is applied to the group configuration of the department.	A character string of 0 to 256 ASCII characters that does not include control characters	(Blank)
TLS	Specify whether to enable TLS (Transport Layer Security) communication.	Selected TLS is enabled. Not selected TLS is not enabled.	Not selected

(19) Support service parameters

The following tables list and describe the parameters in the **Product Update** view that opens from **General** in the Settings module.

Customer Support configuration

Item	Description	Specifiable values	Default
Enable Product Update	Specify whether to acquire the latest Windows update information from the support service sites.	Selected Connect to the support service site. Not selected Do not connect to the support service site.	Not selected
URL	Specify the URL of the support service site.	No restrictions	https://www.hitachi-support.com/jp1itdm
Download User ID	Specify the authentication ID of the Web server.	No restrictions	(Blank)
Password	Specify the password for the download user ID.	No restrictions	(Blank)
Retype Password	Enter the password again for confirmation.	No restrictions	(Blank)
Start At	Specify the time at which to connect to the support service.	00:00 to 23:59	The time when the setup for the management server was completed, rounded up to the nearest hour.#
Repeat Interval	Select **Daily**, **Weekly**, or **Monthly** as the unit of the interval at which you want to establish a connection.	• Daily • Weekly • Monthly	Daily
Repeat	Specify details of the repeat interval.	The specifiable values depend on the item selected for **Repeat Interval**. For Daily: 1 to 31 For Weekly: Sunday to Saturday For Monthly: You can specify the date (1 to 31), or the week of the month (first to fourth, or last) and the day of the week (Sunday to Saturday)	1
Specify users to receive Product Update notification e-mails.	Select the user IDs to which you want to send updates in the update list. If an email address has not been specified, enter the email address.	Email character string	User accounts specified in the **Account Management** view

#: For example, if the setup time is 10:30, the download starts at 11:00.

Proxy Server configuration

Item	Description	Specifiable values	Default
Use Proxy Server	Select this option when using a proxy server.	Selected A proxy server is used. Not selected A proxy server is not used.	Not selected

Item	Description	Specifiable values	Default
IP Address	Enter the IP address of the proxy server.	An IPv4 IP address	(Blank)
Port	Enter the port number of the proxy server.	1 to 65535	(Blank)
User ID	Enter the user ID used for connecting to the proxy server.	A user ID used for connecting to the proxy server	(Blank)
Password	Specify the password for the user ID.	The password for the user ID	(Blank)
Retype Password	Enter the password again for confirmation.	The password for confirmation	(Blank)

(20) MDM linkage parameters

The following tables list and describe the parameters in the **MDM Linkage Settings** view that opens from **General** in the Settings module.

MDM Linkage Settings

Item	Description	Specifiable values	Default
MDM setting name	Specify the name of the setting.	A character string of 255 or fewer characters	(Blank)
MDM system	Select the MDM system you want to connect to.	• MobileIron	(Blank)
Host name of MDM server	Specify the common name (CN) assigned to the server certificate of the MDM system. If you are using MobileIron, specify the CN in FQDN format.	A character string of 255 or fewer characters	(Blank)
Port number of MDM server	Specify the port number used for connecting to the MDM system.	1 to 65535	(Blank)
URL	Specify the URL of the MDM system.	A character string of 0 to 2,083 characters	(Blank)
User ID	Specify the user ID used to log in to the MDM system.	A character string of 276 or fewer characters	(Blank)
Password	Specify the password used to log in to the MDM system.	A character string of 128 or fewer characters	(Blank)
Retype Password	Enter the password again for confirmation.	A character string of 128 or fewer characters	(Blank)

Proxy Server configuration

Item	Description	Specifiable values	Default
Use Proxy Server	Select this option when using a proxy server.	Selected A proxy server is used. Not selected A proxy server is not used.	Not selected
IP Address	Enter the IP address of the proxy server.	An IPv4 IP address	(Blank)
Port	Enter the port number of the proxy server.	1 to 65535	(Blank)

Item	Description	Specifiable values	Default
User ID	Enter the user ID used for connecting to the proxy server.	A user ID used for connecting to the proxy server	(Blank)
Password	Specify the password for the user ID.	The password for the user ID	(Blank)
Retype Password	Enter the password again for confirmation.	The password for confirmation	(Blank)

Collection Schedule

Item	Description	Specifiable values	Default
Start At	Specify the time at which information is collected from the MDM system.	00:00 to 23:59	(Blank)
Repeat Interval	Select **Daily**, **Weekly**, or **Monthly** as the unit of the interval at which you want to collect information.	• Daily • Weekly • Monthly	Daily
Repeat	Specify details of the repeat interval.	The specifiable values depend on the item selected for **Repeat Interval**. For Daily: 1 to 31 For Weekly: Sunday to Saturday For Monthly: You can specify the date (1 to 31), or the week of the month (first to fourth or last) and the day of the week (Sunday to Saturday).	1

(21) JP1/NETM/NM - Manager linkage parameters

The following table lists and describes the parameters in the **JP1/NETM/NM - Manager Link Settings** view displayed by clicking **Edit** for **JP1/NETM/NM - Manager Link Settings** in the **Network Filter Settings** view via the **Network Access Control** view of the Settings module.

Item	Description	Specifiable values	Default
Link with JP1/NETM/NM - Manager	Specify whether to link with JP1/NETM/NM - Manager.	Selected The system links with JP1/NETM/NM - Manager. Not selected The system does not link with JP1/NETM/NM - Manager.	Not selected

A.5 Lists of properties

The following table lists and describes the properties that can be set by the configuration file. Note that the settings in the configuration file are applied after the JP1/IT Desktop Management 2 service is restarted.

Property	Description	Setting value	Default
Capacity_OplogDBPathWarningThreshold	Warning threshold of the free space of the operation log database folder	0 to 1,048,576 MB	10% of the estimated size of the operation log database
Capacity_OplogDBPathErrorThreshold	Error threshold of the free space of the operation log database folder	0 to 1,048,576 MB	3% of the estimated size of the operation log database
Capacity_OplogBKPathWarningThreshold	Warning threshold of the free space of the operation log storage folder (when periodic export is disabled)	0 to 1,048,576 MB	The seven days total of the guideline values of the disk space required for the operation log storage folder
Capacity_OplogBKPathErrorThreshold	Error threshold of the free space of the operation log storage folder (when periodic export is disabled)	0 to 1,048,576 MB	The three days total of the guideline values of the disk space required for the operation log storage folder
Capacity_OplogBKPathWarningThreshold_ExportEnabled	Warning threshold of the free space of the operation log storage folder (when periodic export is enabled)	0 to 1,048,576 MB	The seven days total of the guideline values of the disk space required for the operation log storage folder
Capacity_OplogBKPathErrorThreshold_ExportEnabled	Error threshold of the free space of the operation log storage folder (when periodic export is enabled)	0 to 1,048,576 MB	The three days total of the guideline values of the disk space required for the operation log storage folder
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportDisabled	Warning threshold of the free space of the data folder (when operation log is enabled and periodic export is disabled)	0 to 1,048,576 MB	50% of the guideline value of the disk space required for the data folder used as the operation log buffer + 3,072 MB
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportDisabled	Error threshold of the free space of the data folder (when operation log is enabled and periodic export is disabled)	0 to 1,048,576 MB	30% of the guideline value of the disk space required for the data folder used as the operation log buffer + 500
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportEnabled	Warning threshold of the free space of the data folder (when operation log is enabled and periodic export is enabled)	0 to 1,048,576 MB	50% of the guideline value of the disk space required for the data folder used as the operation log buffer + 3,072 MB
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportEnabled	Error threshold of the free space of the data folder (when operation log is enabled and periodic export is enabled)	0 to 1,048,576 MB	30% of the guideline value of the disk space required for the data folder used as the operation log buffer + 500

Property	Description	Setting value	Default
State_AfterAgentUninstalling#	Specifies whether uninstallation of JP1/IT Desktop Management 2 - Agent is treated as disposal of a device, or as uninstallation of JP1/IT Desktop Management 2 - Agent.	0: Treated as an uninstallation. 1: Treated as disposal of a device.	0
Report_Data_MakeTime	Time for creating totalization data for the report	00:00 to 23:59	23:00
Report_Digest_MakeTime	Time for creating a digest report	00:00 to 23:59	06:00
DB_MentenanceTime	Time for database maintenance	00:00 to 23:59	05:00
ChangeHistory_GetTime	Time for acquiring the revision history	00:00 to 23:59	00:00
OpLog_DB_DeleteTime	Time for maintenance of the operation log database in which operation logs were automatically acquired	00:00 to 23:59	01:00

#

If no uninstallation notification can be received from an agent, the device information is not changed as is done in older versions. In such a case, take actions as necessary (for example, by deleting the device information).

A.6 Performance and Estimates

This section describes memory requirements, disk space requirements, and prerequisite CPUs for each system component of the product.

Related Topics:

- (1) Memory requirements
- (2) Disk space requirements
- (3) Prerequisite CPUs

(1) Memory requirements

The following describes the memory requirements for each system component of the product.

- Management server
- Computer that displays operation windows
- Administrator's computer with Remote Installation Manager installed
- Administrator's computer with a remote control controller installed
- Computer used as a relay system
- Managed computer

Management server

Item	Operating environment
Memory usage	When the number of managed computers is 10,000 or fewer: 7,065.4 MB When the number of managed computers is 10,000 to 30,000: 24,958.6 MB

Item	Operating environment
Memory usage	If you added the capacity of the database cache to improve the performance of the operation log search function, the value specified for addition (a maximum of 16 GB) must be added.
Installed memory	An amount of installed memory equal to or greater than the sum of the following values is required: • When the number of managed computers is 5,000 or fewer: 2.0 GB or more • When the number of managed computers is 5,000 to 10,000: • Minimum value 2.0 GB • Recommended value 8.0 GB • When the number of managed computers is 10,000 to 30,000: • Minimum value 16.0 GB • Recommended value 32.0 GB • If you specified a value for **Capacity to be added to the cache** during management server setup to improve the performance of the operation log search function, the specified value (a maximum of 16 GB) must be added.

Note: If the number of managed computers is 5,000 to 10,000, at least a 32-bit version of the OS must be used on the management server. Hitachi recommends that you use 64-bit version of the OS. If the number of managed computers is 10,000 to 30,000, use a 64-bit version of the OS. If the number of managed computers is 5,000 or more, and you want to collect operation logs, use a 64-bit version of the OS.

Computer that displays operation windows

Item	Operating environment
Memory usage	No memory is used by JP1/IT Desktop Management 2.
Installed memory	2.0 GB or more

Administrator's computer with Remote Installation Manager installed

Item	Operating environment
Memory usage	The required value can be calculated from the following formula: 20 + 0.002 x a MB a: number of displayed data items The number of displayed data items is the total of the data items (shown below) that are displayed in Remote Installation Manager windows. If you want to display more than one of the same windows, multiply the number of data items by the number of those windows. • **System Configuration** window Host information (relay system, agent) • System information for each system • Installed packages for each agent • **Destination** window • ID (new host, asset management item condition) Destination corresponding to each grouping information set (path, agent) • Host group (IP address, new host, OS type, additional management item of hardware asset information, department, installation location) Destination corresponding to each grouping information set (path, agent) • Installed packages for each agent

Item	Operating environment
Memory usage	• **Job Definition** window Folders, Job Definition • **Package** window Cabinet, Package • **Job Status** window Folder, Job (destination for each job, package for each job)
Installed memory	2.0 GB or more

Administrator's computer with a remote control controller installed

Item	Operating environment
Memory usage	The sum of the following values: • Basic function (remote control): (10 x number of connections) MB • File transfer function: 4 MB • Chat server function: (4 + (0.2 x number of connections)) MB • Chat client function: (4 + (0.4 x number of connections)) MB
Installed memory	An amount of installed memory equal to or greater than the sum of the following values is required: • Recommended memory size for each OS • Memory usage multiplied by 0.5 and then truncated to the nearest multiple of 8

Computer used as a relay system

Item	Operating environment
Memory usage	The sum of the following values: • Basic functions (device information collection, distribution, and remote control) (always resident): 58 MB • Operation logging function (resident when the function is enabled): 34 MB for a 32-bit OS, or 43 MB for a 64-bit OS • Network monitor function (resident when the function is enabled): 2 MB + (10 x number of network segments to be monitored) MB • The value calculated from the following formula: 28 + 0.018 x (a + 8) + (b x 0.001) a: Number of concurrently connected computers The value specified for **Number of JP1/IT Desktop Management 2 - Agents that can be connected to the relay system concurrently** under **Processing settings for the relay system** in the window displayed from **Relay system settings** of the agent configurations b: Cache size of the management file Calculate the value by using the following formula: Cache size of the management file (KB) = number of jobs that are saved in the relay system and executed by the higher system x number of destinations for each job x number of packages for each job (for remote installation jobs) x 1 KB
Installed memory	An amount of installed memory equal to or greater than the sum of the following values is required: • Recommended memory size for each OS • Memory usage multiplied by 0.5, and then truncated to the nearest multiple of 8

Managed computer

Item	Operating environment
Memory usage	Computer with an agent installed The sum of the following values: • Basic functions (device information collection, distribution, and remote control) (always resident): 58 MB • Operation logging function (resident when the function is enabled): 34 MB for a 32-bit OS, or 43 MB for a 64-bit OS • Network monitor function (resident when the function is enabled): 2 MB + (10 x number of network segments to be monitored) MB Agentless computer 22 MB
Installed memory	An amount of installed memory equal to or greater than the sum of the following values is required: For agent-installed computers: • Recommended memory size for each OS • Memory usage multiplied by 0.5, and then truncated to the nearest multiple of 8 For agent-less computers: Recommended memory size for each OS + 16 MB

(2) Disk space requirements

The following describes the disk space requirements for each system component of the product.

- Management server
- Computer that displays operation windows
- Administrator's computer with Remote Installation Manager installed
- Administrator's computer with a remote control controller installed
- Computer used as a relay system
- Managed computer

Management server

Item	Operating environment
Installation drive (program size)	When the number of managed computers is 10,000 or fewer: 2.5 GB or more When the number of managed computers is 10,000 to 30,000: 17.5 GB or more If you added the capacity of the database cache to improve the performance of the operation log search function, the value specified for addition (a maximum of 16 GB) must be added.
Drive of the database storage folder (database capacity)	When the number of managed computers is 10,000 or fewer: The required space is equal to or greater than the sum of the following values: • Basic function: 20 GB • Operation logging function: Data capacity appropriate for the operation[#1]

Item	Operating environment
Drive of the database storage folder (database capacity)	- Revision history function: Data capacity appropriate for the operation#2 When the number of managed computers is 10,000 to 30,000: The required space is equal to or greater than the sum of the following values: - Basic function: 60 GB - Operation logging function: Data capacity appropriate for the operation#1 - Revision history function: Data capacity appropriate for the operation#2
Drive on which the data folder is stored	A value equal to or greater than the sum of the following values: - Basic functions: 320 MB - The sum of the sizes of all distribution packages - The sum of the sizes of attached files for hardware assets, contracts, and licenses - The capacity required for operation logs You must estimate the data capacity#3 appropriate for the operation.
Drive of the operation log backup folder	You must estimate the data capacity#4 appropriate for the operation.
Drive on which the revision history output folder is stored	You must estimate the data capacity#5 appropriate for the operation.

#1: For details about the data capacity required for the operation log database, see 4.5.4 Guidelines for disk space requirements for the operation log database. If the number of managed computers is in the range from 10,000 to 30,000, Hitachi recommends that you use a dedicated physical disk for the operation log database.

#2: For details about the data capacity required for the revision history database, see 4.5.7 Guidelines for disk space requirements for revision history database.

#3: For details about the data capacity required for the data folder, see 4.5.5 Guidelines for disk space requirements in the data folder for acquiring operation logs.

#4: For details about the data capacity required for the operation log storage folder, see 4.5.3 Guidelines for disk space requirements for operation log backup folder.

#5: For details about the data capacity required for the revision history output folder, see 4.5.6 Guidelines for disk space requirements for revision history archive.

To use the distribution function, the following additional free disk space is required.

For distribution using Remote Installation Manager

Item	Operating environment
Drive with JP1/IT Desktop Management 2 - Manager installed	1.0 x number of packages x number of agents + number of packages x 0.3 (KB)
Drive on which the data folder is stored	Total package size after compression + number of packages x 2 (KB)

For ITDM-compatible distribution

Item	Operating environment
Drive with JP1/IT Desktop Management 2 - Manager installed	Free disk space more than twice the package size (before compression)
Drive on which the data folder is stored	
System drive	Free disk space for the package (before compression)

To automatically update the component, the following additional free disk space is required.

Item	Operating environment
Drive with JP1/IT Desktop Management 2 - Manager installed	500 MB
Drive on which the data folder is stored	
System drive	

Computer that displays operation windows

JP1/IT Desktop Management 2 does not require disk space.

Administrator's computer with Remote Installation Manager installed

Item	Operating environment
Installation drive (program size)	24 MB or more

Administrator's computer with a remote control controller installed

Item	Operating environment
Installation drive (program size)	20 MB or more

Computer used as a relay system

Item	Operating environment
Installation drive (program size)	The required space is equal to or greater than the sum of the following values: • Basic functions (inventory collection, distribution, and remote control): 71 MB • Operation logging function: 120 MB • Network monitor function: 2 MB + (55 x number of network segments to be monitored) MB

If Remote Install Manager is used for distribution, the free space described in the following table is also required.

Item	Operating environment
Drive with a relay system installed	(80 + total package size after compression + number of packages x number of agents under the relay system / 1024) MB

If a relay system is updated by automatic update, the free space described in the following table is also required.

Item	Operating environment
Drive with a relay system installed	200 MB
Drive on which the data folder is stored	
System drive of a computer with a relay system agent installed	

Managed computer

Item	Operating environment
Installation drive (program size)	*For agentless operation:* JP1/IT Desktop Management 2 does not require disk space.
	For agent operation: A value equal to or greater than the sum of the following values: • Basic functions (inventory collection, distribution, and remote control): 71 MB • Operation logging function: 120 MB + 260 KB x retention period (days) • Network monitor function: 2 MB + (55 x number of network segments to be monitored) MB

To use the distribution function, the following additional free disk space is required.

- For distribution using Remote Installation Manager

Item	Operating environment
Drive with an agent installed	Free disk space more than three times the package size (before compression)

- For ITDM-compatible distribution

Item	Operating environment
Drive with an agent installed	• When the package type is **Software Installation**: Free disk space more than twice the package size (before compression to a ZIP file) • When the package type is **File Distribution**: Free disk space more than triple the package size (before compression to a ZIP file)
System drive of a computer with an agent installed	Free disk space for the package (before compression to a ZIP file)

To update an agent automatically, the following additional free disk space is required.

Item	Operating environment
Drive with an agent installed	50 MB
System drive of a computer with an agent installed	

To update a network agent automatically, the following additional free disk space is required.

Item	Operating environment
Drive with an agent installed	20 MB
System drive of a computer with an agent installed	

When an agentless computer uses Windows administrative shares for authentication, executable programs are sent to execute functions. At least 2.5 MB of free disk space is required to store the executable programs.

Computer used as a packager

Item	Operating environment
Drive with an agent installed	7 MB + free disk space more than twice the package size (before compression)

Computer running Automatic Installation Tool

Item	Operating environment
Drive with an agent installed	6 MB

Related Topics:

- 4.5 Examining the database

(3) Prerequisite CPUs

This section describes the prerequisite CPUs for each system component of the product.

- Management server
- Computer that displays operation windows
- Administrator's computer with Remote Install Manager installed
- Administrator's computer with a remote control controller installed
- Computer used as a relay system
- Managed computer

Management server

When the number of managed computers is 5,000 or fewer:

A 32-bit or 64-bit processor at 2.0 GHz or higher

When the number of managed computers is 5,000 to 10,000:

- Minimum requirements
  A 32-bit or 64-bit processor at 2.0 GHz or higher
- Recommended requirements
  A 32-bit or 64-bit 4-core processor at 2.0 GHz or higher

When the number of managed computers is 10,000 to 30,000:

- Minimum requirements
  Intel Xeon (4-core) processor at 2.5 GHz or higher x 2
- Recommended requirements
  Intel Xeon (4-core) processor at 3.0 GHz or higher x 2

Computer that displays operation windows

- A hyper-threading technology processor equivalent to Intel Pentium 4 or higher
- A processor equivalent to Intel Core 2 or higher

Administrator's computer with Remote Installation Manager installed

- Minimum requirements
  A processor at 1 GHz
- Recommended requirements
  A processor at 2 GHz or higher

Administrator's computer with a remote control controller installed

Computer OS	Operating environment
Windows 8.1	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows 8	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2012	A 64-bit processor at 1.4 GHz or higher
Windows 7	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2008	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher
Windows Vista	A 32-bit or 64-bit processor at 800 MHz or higher
Windows Server 2003	A 32-bit or 64-bit processor at 133 MHz or higher
Windows XP	A 32-bit processor at 300 MHz or higher

Computer used as a relay system

Computer OS	Operating environment
Windows 8.1	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows 8	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2012	A 64-bit processor at 1.4 GHz or higher
Windows 7	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2008	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher
Windows Vista	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher
Windows Server 2003	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher
Windows XP	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher

Managed computers

Agentless computers

No restrictions on CPUs.

Computers on which agents will be installed

Computer OS	Operating environment
Windows 8.1	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows 8	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2012	A 64-bit processor at 1.4 GHz or higher
Windows 7	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2008	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher
Windows Vista	A 32-bit or 64-bit processor at 800 MHz or higher
Windows Server 2003	A 32-bit or 64-bit processor at 133 MHz or higher
Windows XP	A 32-bit processor at 300 MHz or higher

Computer on which the network monitor is enabled

Computer OS	Operating environment
Windows 8.1	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows 8	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2012	A 64-bit processor at 1.4 GHz or higher
Windows 7	A 32-bit or 64-bit processor at 1.0 GHz or higher
Windows Server 2008	A 32-bit processor at 1.0 GHz or higher, or a 64-bit processor at 1.4 GHz or higher
Windows Server 2003	A 32-bit or 64-bit processor at 133 MHz or higher

A.7 List of limit values

For some items that can be managed by JP1/IT Desktop Management 2, there are restrictions on the number of items that can be registered and on the specifiable values. The tables below show the limit values for each item. The tables below use the following legend.

Legend: --: Not applicable

Security module

Function	Item	Limit value	Default	Description
Security Policy	Security Policy	There is no upper limit.	2 items	By default, *Default policy* and *Recommended security policy* are registered. The assumed maximum number of registered security policies is 80 for a 32-bit OS, and 140 for a 64-bit OS, including those above.
Security Configuration Items for Security Policy	Mandatory Software	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 100, including those registered for Unauthorized Software.
	Unauthorized Software	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 100, including those registered for Mandatory Software.
	Unauthorized Windows Service	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 30.
	User-defined security settings in user definitions	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 30.
	Blocked Software	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 100, including those registered for Mandatory Software.
Windows Update	Number of displayed items	There is no upper limit.	0	--

Function	Item	Limit value	Default	Description
Windows Update	Programs that can be added to Windows Updates manually	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 1,000.
Computer Security Status	Windows updates not applied for one device	There is no upper limit.	--	The assumed maximum number of items that can be registered is 100.
	Mandatory software not installed for one device	There is no upper limit.	--	The assumed maximum number of items that can be registered is 50.
	Unauthorized software installed for one device	There is no upper limit.	--	The assumed maximum number of items that can be registered is 50.
	Number of accounts that can be confirmed in the OS security settings for one device	1 to 50	--	--
	Number of services that can be confirmed in the service security settings for one device	1 to 30	--	--
USB device information	Information about files collected from a USB device for one device	1 to 10,000 items	--	--
Operation Logs	Number of displayed items	There is no upper limit.	0	--

Note: Even for items that have no upper limit, registering a huge amount of information might affect performance. For example, search performance might be degraded.

Assets module

Function	Item	Limit value	Default	Description
Hardware Asset	Hardware Asset Information	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 37,500 for a 32-bit OS, and 112,500 for a 64-bit OS. In the above number, the assumed maximum number of items that can be

Function	Item	Limit value	Default	Description
Hardware Asset	Hardware Asset Information	There is no upper limit.	0 item	registered for USB devices is 2,000 for a 32-bit OS, and 6,000 for a 64-bit OS.
	Asset Status	0 to 100 items can be added in addition to the default.	4 items	By default, **Unconfirmed**, **In Stock**, **In Use**, and **Disposed** are registered for Asset Status. These items are the same as those of the Settings module.
	Planned Asset Status	0 to 100 items can be added in addition to the default.	3 items	By default, **In Stock**, **In Use**, and **Disposed** are registered for Planned Asset Status. These items are the same as those of **Asset Status**, except for **Unconfirmed**.
	Device Type	0 to 100 items can be added in addition to the default.	11 items	By default, **PC**, **Server**, **Storage**, **Network Device**, **Printer**, **Smart Device**, **Peripheral Device**, **USB Device**, **Display**, **Other**, and **Unknown** are registered for Device Type. These items are the same as those of the Settings module.
	Number of items for Export Columns	1 to 200	8 items	By default, **Device Type**, **Asset #**, **Device Name**, **Manufacturer**, **Asset Status**, **Planned Asset Status**, **Planned Date**, and **Last Tracked Date** are selected for Export Columns.
Software License	Software License	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 5,000 for a 32-bit OS, and 15,000 for a 64-bit OS.
	License Type	0 to 100 items can be added in addition to the default.	2 items	By default, **Install License** and **Other** are registered for License Type. These items are the same as those of the Settings module.
	License Status	0 to 100 items can be added in addition to the default.	2 items	By default, **In Use** and **Expired** are registered for License Status. These items are the same as those of the Settings module.
	Planned License Status	0 to 100 items can be added in addition to the default.	2 items	By default, **In Use** and **Expired** are registered for Planned License Status. These items are the same as those of **License Status**.
	Number of items for Export Columns	1 to 200	11 items	By default, the following items are selected for Export Columns: **License #**, **License Name**, **License Type**, **Total Licenses**, **License Total**, **Assigned License Total**, **Remaining License Total**, **License Status**, **Planned License Status**, **Planned Date**, **Last Tracked Date**.
Managed Software	Managed Software	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 100 for a 32-bit OS, and 200 for a 64-bit OS.

Function	Item	Limit value	Default	Description
Managed Software	Number of items for Export Columns	1 to 10	7 items	By default, **Managed Software Name**, **Manufacturer**, **License Type**, **License Total**, **Number of Used Licenses**, and **Remaining License Total** are selected for Export Columns.
Contract	Contract Information	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 8,750 for a 32-bit OS, and 26,250 for a 64-bit OS.
	Contract Type	0 to 100 items can be added in addition to the default.	5 items	By default, **Lease**, **Rent**, **Maintenance**, and **Support**, **Fixed** are registered for Contract Type. These items are the same as those of the Settings module.
	Contract Vendor Name	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 60. This item is the same as the item of the Settings module.
	Contract Status	0 to 100 items can be added in addition to the default.	3 items	By default, **Active**, **Canceled**, and **Expired** are registered for Contract Status. These items are the same as those of the Settings module.
	Number of items for Export Columns	1 to 200	7 items	By default, **Contract #**, **Contract Name**, **Contract Type**, **Contract Start Date**, **Contract End Date**, **Contract Date**, and **Contract Status** are selected for Export Columns.
Other	Templates used for import and export	There is no upper limit.	--	The assumed maximum number of items that can be registered is 40 for a 32-bit OS, and 120 for a 64-bit OS.

Note: Even for items that have no upper limit, registering a huge amount of information might affect performance. For example, search performance might be degraded.

Device module

Function	Item	Limit value	Default	Description
Device Information	Device Information	Number of purchased licenses	0	--
	Installed software for one device	There is no upper limit.	--	The assumed maximum number of items that can be registered is 500.
	Number of accounts for one device that can be confirmed in Account Details on the Service Details tab	1 to 50	--	--

Function	Item	Limit value	Default	Description
Device Information	Number of services for one device that can be confirmed in Windows Security Details on the Service Details tab	1 to 30	--	--
Export Device Details	Number of records to be exported from the management window	There is no upper limit.	--	The assumed maximum number of items that can be registered is 10,000.
	Installed Software	There is no upper limit.	--	The assumed maximum number of items that can be registered is 10.
	Installed Updates	There is no upper limit.	--	The assumed maximum number of items that can be registered is 10.
Revision history	Number of entries that can be displayed in the device revision history list	600,000 entries	--	--
Software Inventory	Software	Number of software records that can be collected	0	--
	Number of items for Export Columns	1 to 9	8 items	By default, **Software Name**, **Version**, **Software Vendor**, **Installed Software Total**, **Registration Date/Time**, **Mandatory Software**, **Unauthorized Software**, and **Managed Software** are selected for Export Columns.

Distribution (ITDM-compatible) module

Function	Item	Limit value	Default	Description
Packages	Packages	0 to 10,000 items	0	--
	Number of archive files of ZIP files registered in packages	There is no upper limit.	--	The assumed maximum number of files that can be registered is 3,000.
Tasks	Tasks	0 to 10,000 items	0	--
	Target Computers	Number of managed computers	0	--

Events module

Function	Item	Limit value	Default	Description
Events	Number of events that can be displayed	Number of available product licenses x 250 + 10,000	0	--

Settings module

Function	Item	Limit value	Default	Description
User Management	Users	There is no upper limit.	1 item	The assumed maximum number of user accounts that can be registered is 50 for a 32-bit OS, and 150 for a 64-bit OS. By default, a built-in account is registered.
Agent	Agent Configurations	There is no upper limit.	1 item	By default, the default agent configuration is registered.
	Update Interval (Agentless Management)	24 hours	1 hour	--
Discovery	Discovered Nodes	There is no upper limit.	0 item	--
	Managed Nodes	Number of purchased licenses	0 item	--
	Ignored Nodes	There is no upper limit.	0 item	--
Network Access Control	Network Access Control Settings	There is no upper limit.	0 item	The assumed maximum number of records that can be registered is 10.
	Exclusive Communication Destination for Access-Denied Devices	There is no upper limit.	0 item	The assumed maximum number of records that can be registered is 110.
	Network Filter Settings	There is no upper limit.	0 item	The assumed maximum number of records that can be registered is 22,000 for a 32-bit OS, and 66,000 for a 64-bit OS. This value is obtained by doubling the total number of managed computers and unmanaged computers.
Assets	Custom Fields (Hardware Assets)	The number of fields that can be added varies depending on the selected data type as shown below. • Number: 0 to 20 fields A value in the range from -2147483647 to 2147483647 can be specified for each field.	0 item	The assumed maximum number of options that can be added for Enumeration fields is 50.

Function	Item	Limit value	Default	Description
Assets	Custom Fields (Hardware Assets)	- Date: 0 to 10 fields A date in the range from 1900/1/1 to 9000/12/31 can be specified for each field. - Enumeration: 0 to 20 fields There is no upper limit on the number of options for each field. - Text: 0 to 75 fields 0 to 256 characters can be specified for each field.	0 item	The assumed maximum number of options that can be added for Enumeration fields is 50.
	Custom Fields (Software License)	The number of fields that can be added varies depending on the selected data type as shown below. - Number: 0 to 10 fields A value in the range from -2147483647 to 2147483647 can be specified for each field. - Date: 0 to 10 fields A date in the range from 1900/1/1 to 9000/12/31 can be specified for each field. - Enumeration: 0 to 10 fields There is no upper limit on the number of options for each field. - Text: 0 to 10 fields 0 to 256 characters can be specified for each field.	0 item	The assumed maximum number of options that can be added for Enumeration fields is 50.
	Custom Fields (Contracts)	The number of fields that can be added varies depending on the selected data type as shown below. - Number: 0 to 10 fields A value in the range from -2147483647 to 2147483647 can be specified for each field. - Date: 0 to 10 fields A date in the range from 1900/1/1 to 9000/12/31 can be specified for each field. - Enumeration: 0 to 10 fields There is no upper limit on the number of options for each field. - Text: 0 to 10 fields 0 to 256 characters can be specified for each field.	0 item	The assumed maximum number of options that can be added for Enumeration fields is 50.
	Asset Status	0 to 100 items can be added in addition to the default.	4 items	By default, **Unconfirmed**, **In Stock**, **In Use**, and **Disposed** are registered for Asset Status.

Function	Item	Limit value	Default	Description
Assets	Asset Status	0 to 100 items can be added in addition to the default.	4 items	These items are the same as those of the Assets module.
	Device Type	0 to 100 items can be added in addition to the default.	11 items	By default, **PC**, **Server**, **Storage**, **Network Device**, **Printer**, **Smart Device**, **Peripheral Device**, **USB Device**, **Display**, **Other**, and **Unknown** are registered for Device Type. These items are the same as those of the Assets module.
	License Status	0 to 100 items can be added in addition to the default.	2 items	By default, **In Use** and **Expired** are registered for License Status. These items are the same as those of the Assets module.
	License Type	0 to 100 items can be added in addition to the default.	2 items	By default, **Install License** and **Other** are registered for License Type. These items are the same as those of the Assets module.
	Contract Status	0 to 100 items can be added in addition to the default.	3 items	By default, **Active**, **Canceled**, and **Expired** are registered for Contract Status. These items are the same as those of the Assets module.
	Contract Type	0 to 100 items can be added in addition to the default.	5 items	By default, **Lease**, **Rent**, **Maintenance**, and **Support**, **Fixed** are registered for Contract Type. These items are the same as those of the Assets module.
	Contract Vendor Name	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 60. This item is the same as the item of the Assets module.
	Number of items for Export Columns (Contact Vendor List)	1 to 6	6 items	--
Inventory	Software List	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 30.
General	Active Directory domain	There is no upper limit.	0 item	This item is the same as the item of the Home module (**Getting Started** button).
	MDM server information	There is no upper limit.	0 item	The assumed maximum number of items that can be registered is 10.

Note: Even for items that have no upper limit, registering a huge amount of information might affect performance. For example, search performance might be degraded.

Menu area

Function	Item	Limit value	Default	Description
Menu area	Total number of groups	There is no upper limit.	--	The assumed maximum number of groups that can be registered is as follows: For a 32-bit OS When user-defined groups are included: 800 groups When user-defined groups are not included: 500 groups For a 64-bit OS When user-defined groups are included: 1,500 groups When user-defined groups are not included: 1,200 groups
	User-Defined Groups	There is no upper limit.	--	The assumed maximum number of groups is 300.
	User-Defined Group Conditions	0 to 10	--	--
	Total number of devices assigned to user-defined groups	There is no upper limit.	--	The assumed maximum number of devices is 100,000.
• Security module • Assets module • Device module • Distribution (ITDM-compatible) module	Custom Group	There is no upper limit.	0 group	The assumed maximum number of groups that can be registered for each module is 50.
	Items that can be added for custom groups	There is no upper limit.	0 item	The assumed maximum number of items that can be added is 5,000.
• Security module • Assets module • Device module • Distribution (ITDM-compatible) module • Events module	Filter	There is no upper limit.	Depends on the module	The assumed maximum number of items that can be registered for each module is 50.
	Filter Conditions	1 to 10 items	5 items	--
Security module	Update Group	There is no upper limit.	0 group	The assumed maximum number of groups that can be registered is 200.
	Updates that can be added to Update Group	There is no upper limit.	0 item	The assumed maximum number of updates that can be registered is 3,000.

Note: Even for items that have no upper limit, registering a huge amount of information might affect performance. For example, search performance might be degraded.

Remote Installation Manager

Function	Item	Limit value	Default	Description
Packages	Packages	0 to 331,776	--	The following are the details of the upper limit of packages: The maximum number of cabinets 1,296 The maximum number of packages for a cabinet 256
Jobs	Jobs	There is no upper limit.	--	--
	Number of agents per job	There is no upper limit.	--	The assumed maximum number of agents is 3,000.

Note: Even for items that have no upper limit, registering a very large amount of information might affect performance. For example, search performance might be degraded.

A.8 Times at which functions are executed automatically

The time at which a function is executed automatically varies depending on the function as shown in the table below.

For details about the time at which a report is calculated, see 2.16.5 Calculation schedules for reports.

Function		Description	Execution time
Device management	Collecting information from agentless devices	Regularly collect information from agentless devices and update the information to the latest status.	Every hour[#1]
	Obtaining information from Active Directory	Search for computers managed by Active Directory, and then register them inJP1/IT Desktop Management 2. It is also possible to automatically install agents during the search. In addition, the configuration of departments is automatically registered in JP1/IT Desktop Management 2.	Every day at 23:00[#1]
	Collecting user information	If **End User** is specified as the input method for the department, location, user name, or other asset management item, the **Enter User Information** dialog box appears on the user's computer, and the system collects the information the user enters.	When input of user information is complete
	Collecting device revision history	When device information changes, the system compares the new device information against the old, and compiles the results as a revision history.	Every day at 0:00[#2]

Function		Description	Execution time
Security control	Evaluating the security status	Based on the device information collected from computers, determine the violation levels according to the security policy.	Every day at 0:00[#1]
	Regularly checking and updating support information	Connect to the service site according to the import schedule specified in the **Product Update** view of the Settings module, and automatically update information about Windows updates. When the latest information is obtained from the support service site, whether the latest Windows updates are applied to the managed computer can be determined based on the security policy.	Every day at a specified time (the time when the setup for JP1/IT Desktop Management 2 was completed, rounded up to the nearest hour)[#1]
	Updating **Scan Engine Version** and **Virus Definition File Version** settings for anti-virus products	Detect the latest versions of the scan engine and virus definition file for the anti-virus products specified for the security policy from the information collected from computers. Then update the **Scan Engine Version** and **Virus Definition File Version** security policy settings and evaluate the security status.	When information about the versions of the scan engine and virus definition file collected from computers is updated
Operation logs	Storing operation logs	Store the operation logs obtained from computers.	Every hour
	Periodically exporting operation logs	Periodically export the operation logs obtained from computers.	Every hour
	Monitoring free space for the operation log backup folder	Obtain information about free space for the operation log backup folder. If the amount of free space is insufficient, output an event. Use the event mail notification function to notify the administrator of insufficient capacity.	Every day at 6:00[#2]
	Deleting the operation log database and re-creating the index information	Delete the operation logs that exceeded the storage period from the operation log database, and re-create the index information.	Every day at 1:00[#2]
Events	Monitoring event occurrence	If an event of a predefined category and severity occurred, send a notification email to the administrator.	Every 30 minutes[#1]
Others	Obtaining information from an MDM system	Obtain smart device information managed by the MDM system according to the import schedule specified in the **MDM Linkage Settings** view of the Settings module. If information about a new smart device is obtained, the smart device is discovered as a	Every day at a specified time (the time when the setup for JP1/IT Desktop Management 2 was completed, rounded up to the nearest later hour)[#1]

Function		Description	Execution time
Others	Obtaining information from an MDM system	new device. If information about a managed smart device is obtained, the device information and hardware asset information are updated.	Every day at a specified time (the time when the setup for JP1/IT Desktop Management 2 was completed, rounded up to the nearest later hour)#1
	Regularly releasing used free pages in the database	Release used free pages that were generated when database data was deleted. This enables efficient use of the database capacity.	Every day at 5:00#2

#1: You can specify the execution time in the Settings module.

#2: You can specify the execution time in the configuration file.

A.9 Cases in which settings are applied after a restart

You sometimes need to restart a computer to apply settings for JP1/IT Desktop Management 2. A restart is required in the following cases:

- When a security policy is edited or assigned
- When security measures are manually performed

When a security policy is edited

If you edit any of the following items, restart the computer to which the edited security policy is assigned. The items inside the parentheses indicate the relevant security configuration items. After the computer is restarted, the edited security policy is applied to that computer.

- Auto enforce of Enable Automatic Windows Update (Windows Update)
- Auto enforce of Disable Administrative Share (OS Security)
- Auto enforce of Disable Anonymous Access (OS Security)
- Auto enforce of Enable Windows Firewall (OS Security)
  The following OSs do not require a restart: Windows Server 2003 and Windows XP
- Auto enforce of Disable DCOM (OS Security)
- Auto enforce of Disable Remote Desktop (OS Security)
- Suppression of Device Usage (Other Access Restrictions)#
- Enable or disable Acquisition of Operation Logs (including acquisition of Suspicious Operations to be Notified) (Operation Logs)#

# The settings of Suppression of Device Usage and Acquisition of Operation Logs are applied when a security policy is assigned. However, some settings of Suppression of Device Usage and Operation Logs might take effect after a restart.

When a security policy is assigned

Restart the computer to which the security policy is assigned. After the computer is restarted, the assigned security policy is applied to that computer.

The settings of Suppression of Device Usage and Acquisition of Operation Logs are applied when a security policy is assigned. However, some settings of Suppression of Device Usage and Operation Logs might take effect after a restart.

When security measures are manually performed

If you specify any of the following configuration items, restart the computer for which the items have been specified. The items inside the parentheses indicate the relevant security configuration items. After the computer is restarted, the security measures are executed on the computer.

- Enable Automatic Windows Update (Windows Update)
- Disable Administrative Share (OS Security)
- Disable Anonymous Access (OS Security)
- Enable Windows Firewall (OS Security)
  The following OSs do not require a restart: Windows Server 2003 and Windows XP
- Disable DCOM (OS Security)
- Disable Remote Desktop (OS Security)

A.10 Connectivity with lower versions

The following tables describe compatibility when products of different versions are connected.

Connectivity between JP1/IT Desktop Management 2 - Manager (or JP1/IT Desktop Management - Manager) and JP1/IT Desktop Management 2 - Agent (or JP1/IT Desktop Management - Agent)

JP1/IT Desktop Management 2 - Agent or JP1/IT Desktop Management - Agent	JP1/IT Desktop Management 2 - Manager or JP1/IT Desktop Management - Manager										
	09-50 Japanese edition	09-50 Multilanguage edition	09-51 Japanese edition	10-00 Japanese edition	10-01 Japanese edition	10-01 Multilanguage edition	10-02 Japanese edition	10-10 Japanese edition	10-10 Multilanguage edition	10-50 Japanese edition	10-50 Multilanguage edition
09-50 Japanese edition	Y	N	A	A	A	N	A	A	N	A	N
09-50 Multilanguage edition	N	Y	N	N	N	A	N	N	A	N	A
09-51 Japanese edition	N	N	Y	A	A	N	A	A	N	A	N
10-00 Japanese edition	N	N	N	Y	A	N	A	A	N	A	N
10-01 Japanese edition	N	N	N	N	Y	N	A	A	N	A	N
10-01 Multilanguage edition	N	N	N	N	N	Y	N	N	A	N	A
10-02 Japanese edition	N	N	N	N	N	N	Y	A	N	A	N
10-10 Japanese edition	N	N	N	N	N	N	N	Y	N	A	N
10-10 Multilanguage edition	N	N	N	N	N	N	N	N	Y	N	A
10-50 Japanese edition	N	N	N	N	N	N	N	N	N	Y	N
10-50 Multilanguage edition	N	N	N	N	N	N	N	N	N	N	Y

Legend: Y: Can be connected. A: Can be connected by agent functions only. N: Cannot be connected.

Connectivity between JP1/IT Desktop Management 2 - Network Monitor (or JP1/IT Desktop Management - Network Monitor) and JP1/IT Desktop Management 2 - Agent (or JP1/IT Desktop Management - Agent)

JP1/IT Desktop Management 2 - Network Monitor or JP1/IT Desktop Management - Network Monitor	JP1/IT Desktop Management 2 - Agent or JP1/IT Desktop Management - Agent										
	09-50 Japanese edition	09-50 Multilanguage edition	09-51 Japanese edition	10-00 Japanese edition	10-01 Japanese edition	10-01 Multilanguage edition	10-02 Japanese edition	10-10 Japanese edition	10-10 Multilanguage edition	10-50 Japanese edition	10-50 Multilanguage edition
09-50 Japanese edition	Y	N	A	A	A	N	A	A	N	A	N
09-50 Multilanguage edition	N	Y	N	N	N	A	N	N	A	N	A
09-51 Japanese edition	N	N	Y	A	A	N	A	A	N	A	N
10-00 Japanese edition	N	N	N	Y	A	N	A	A	N	A	N
10-01 Japanese edition	N	N	N	N	Y	N	A	A	N	A	N
10-01 Multilanguage edition	N	N	N	N	N	Y	N	N	A	N	A
10-02 Japanese edition	N	N	N	N	N	N	Y	A	N	N	N
10-10 Japanese edition	N	N	N	N	N	N	N	Y	N	A	N
10-10 Multilanguage edition	N	N	N	N	N	N	N	N	Y	N	A
10-50 Japanese edition	N	N	N	N	N	N	N	N	N	Y	N
10-50 Multilanguage edition	N	N	N	N	N	N	N	N	N	N	Y

Legend: Y: Can be connected. A: Can be connected by agent functions only. N: Cannot be connected.

Connectivity between Remote Control Agent and a controller

Remote Control Agent	Controller										
	09-50 Japanese edition	09-50 Multilanguage edition	09-51 Japanese edition	10-00 Japanese edition	10-01 Japanese edition	10-01 Multilanguage edition	10-02 Japanese edition	10-10 Japanese edition	10-10 Multilanguage edition	10-50 Japanese edition	10-50 Multilanguage edition
09-50 Japanese edition	Y	N	A	A	A	N	A	A	N	A	N
09-50 Multilanguage edition	N	Y	N	N	N	A	N	N	A	N	A
09-51 Japanese edition	N	N	Y	A	A	N	A	A	N	A	N
10-00 Japanese edition	N	N	N	Y	A	N	A	A	N	A	N
10-01 Japanese edition	N	N	N	N	Y	N	A	A	N	A	N
10-01 Multilanguage edition	N	N	N	N	N	Y	N	N	A	N	A
10-02 Japanese edition	N	N	N	N	N	N	Y	A	N	A	N
10-10 Japanese edition	N	N	N	N	N	N	N	Y	N	A	N

Remote Control Agent	Controller										
	09-50 Japanese edition	09-50 Multilanguage edition	09-51 Japanese edition	10-00 Japanese edition	10-01 Japanese edition	10-01 Multilanguage edition	10-02 Japanese edition	10-10 Japanese edition	10-10 Multilanguage edition	10-50 Japanese edition	10-50 Multilanguage edition
10-10 Multilanguage edition	N	N	N	N	N	N	N	N	Y	N	A
10-50 Japanese edition	N	N	N	N	N	N	N	N	N	Y	N
10-50 Multilanguage edition	N	N	N	N	N	N	N	N	N	N	Y

Legend: Y: Can be connected. A: Can be connected by agent functions only. N: Cannot be connected.

A.11 Version changes

Changes in 10-50

- The functionality of the site server configuration system was deleted. The relay system was added as a system required for distribution using Remote Installation Manager.
- By using the functionality of distribution using Remote Installation Manager, the user can now specify, in detail, the required conditions for the managed computers and their actions.
- Integrated management of hardware information (including network devices), software information, and contract information is now available in a database.
- Batch collection of files stored in the managed computers is now available.
- The user can now suppress the use of the following devices:
    - Bluetooth devices
    - Imaging devices
    - Windows Portable Devices

  The user was able to suppress the use of the devices below as removable disks in Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista. The user can now suppress the use of each type of the following devices:

    - USB devices
    - IEEE1394 devices
    - Internal SD cards
- The user can now select whether to obtain a list of files stored in a USB device that are allowed to be used.
- The user can now specify whether to display on users' computers the message indicating that the use of a device has been suppressed.
- By using the **Getting Started** Wizard, the user can now manage devices by installing agents on them.
- The functionality of the multi-server configuration system was deleted. One management server can now manage up to 30,000 devices.
- The user can now set the conditions for collecting operation logs regarding the following operations:
    - File operations

    - Startup and stop of programs
    - Window operations
- The user can now collect operation logs for device connection permission.
- The user can now set the interval of sending notifications about prohibited-operation suppression events and operation logs to the higher system, and the maximum period the user's computer can retain such events and logs.
- The user can now set the number of consecutive login failures allowed before the account is locked, and the number of days until the password expires.
- Settings during installation, setup, and agent setup were changed due to the change in the product structure.
- Windows 8.1 and Windows Server 2012 R2 were added to the supported OSs for the following products:
    - JP1/IT Desktop Management 2 - Manager
    - JP1/IT Desktop Management 2 - Agent
    - JP1/IT Desktop Management 2 - Network Monitor
    - JP1/IT Desktop Management 2 - RC Manager
- Windows 8 and Windows 7 are now excluded from the supported OSs for the following product:
    - JP1/IT Desktop Management 2 - Manager
- Windows 2000 is now excluded from the supported OSs for the following product:
    - JP1/IT Desktop Management 2 - Agent
- JP1/IT Desktop Management 09-50 or later, and JP1/IT Desktop Management 2 10-50 were added to the versions that can use Remote Control Agent.
- A description that the AMT version required to use AMT functions is version 9.5 or earlier was added.
- The following products were added to the supported anti-virus products:
    - Kaspersky Endpoint Security 10 for Windows
    - Sophos Endpoint Security and Control for Windows
- Among the supported anti-virus products, the supported versions of the following products were changed:
    - Norton AntiVirus
    - Symantec Endpoint Protection
    - McAfee SaaS Endpoint Protection
    - ウイルスバスター クラウド
    - ウイルスバスター ビジネスセキュリティ
    - Forefront Client Security
    - Kaspersky Endpoint Security 10 for Windows
    - ESET NOD32 Antivirus
    - F-Secure Client Security
- The supported Internet Explorer versions were changed.
- The supported MobileIron versions were changed.
- Microsoft Cluster Service was deleted from the list of supported cluster software products.
- A part of port numbers was changed.
- Services and processes were added and changed.

- Memory requirements, disk space requirements, and required CPUs were changed.
- Collection of print operation logs and suppression of print operations are now unavailable for network shared printers.
- SLL was deleted from the security-protected connection methods used for communication with the SMTP server.
- The function of enabling SSL communication was deleted from the Active Directory settings.
- A description that a fixed IP address must be used for the global IP address of the management server was added.
- A description about the following was added: A software name is judged by partial match, and a version is judged by Starts-with match during determination of the prohibited software and mandatory software.
- A description about the following was added: Only software that exactly matches the specified software name and version is uninstalled from the **Tasks** view.
- A description about the following was added: If the distributed package has the same name as an existing file in the distribution destination, the access permissions for the existing file is inherited to the distributed package.
- A description that the assessment levels in **Category Assessment Status** and **Assessment and # of Target Trend** are possibly different was added.
- The descriptions of the View and Exclusive connection modes in Agent Configuration for remote control sessions were replaced, and the explanation of determining the connection mode was changed.
- A description that OneDrive cannot be used for file transfer in remote control sessions was added.
- A description about connectivity with lower versions was added.
- Host description was added to the device information that can be collected.
- The structure of folders created under JP1/IT Desktop Management 2 - Manager was changed due to a change in the product structure.

Changes in 10-10

- By linking with JP1/NETM/NM - Manager, the user can now use JP1/IT Desktop Management to control the network connections monitored by an appliance product on which JP1/NETM/NM is running.
- In the Security module and Device module, the user can now create a group that can be used to automatically assign managed computers according to the specified conditions.
- The differences in operation windows when administration scopes are assigned were corrected.
- The following description was added: To conduct an intensive search for devices in the network by specifying a discovery period, specify 50,000 or less IP addresses in the discovery range.
- The explanation of the total free space in the computer information was changed as follows:
    - A description that the type of logical drive is Local Disk was added to the explanation about the hard disk.
    - A description that, if the total amount of free space on the local disk exceeds 9,223,372,036,854,775,807 bytes, 9,223,372,036,854,775,807 (bytes) is displayed, was added.
- The user can now select whether to display on the user's computer the balloon tip on the JP1/IT Desktop Management icon in Taskbar, and a window for entering user information.
- Among the device information that can be obtained from the MDM system, the explanation about the system information was changed. The explanation for when an underscore (_) is used in the host name for MDM server linkage was deleted.
- A workaround for the problem that ten IP addresses leased by the DHCP server are reserved by the Remote Access function of RRAS (Routing and Remote Access Service), was added.
- The user can now specify whether to enable all automatic updates on the network filter list or to enable automatic updates only for add operations.

- Among the supported anti-virus products, the supported versions of the following products were changed:
    - ウイルスバスター コーポレートエディション
    - ウイルスバスター コーポレートエディション アドバンス
    - ウイルスバスター コーポレートエディション サーバ版
    - ウイルスバスター コーポレートエディション サーバ版 アドバンス
    - ESET Endpoint Antivirus
    - ESET File Security for Microsoft Windows Server
    - OfficeScan Corporate Edition

  Also, a note on when the anti-virus product is ServerProtect for Windows NT/NetWare was added.
- The minimum values that can be entered for the judgment values in User-Defined Security Settings were added.
- A description about the following was added: If version information for the executable file of the target software program is corrupted or contradicted, the program might not be blocked. This might occur even if the **Formal file name** or **Original file name** settings in Windows Explorer matches the **File name** setting for the program.
- Firefox was deleted from the Web browsers that can be used to collect operation logs for Web access, upload of files, and download of files.
- An explanation about the required conditions for the managed files was added.
- A description about the following was added: If the processing is forcibly terminated after operation logs are sent from a computer running an agent to the management server, operation logs might be duplicately collected until the operation logs on that computer are deleted.
- A description that operation logs for uploading files might not be collected in Internet Explorer 10 was added.
- A description that the access permissions for the distribution-destination folder are inherited to the distributed package was added. Also, a description that the user needs to operate on the distribution-target computer to change the access permissions for the distributed package was added.
- The description about reducing the load caused by distribution was corrected.
- Notes on distribution were added.
- Android was added to the required OSs for smart devices that are managed with linkage with the MDM system.
- The description about the versions of the JP1 Smart Device Management service in a MDM linkage configuration system was changed.
- When the free space of individual data folders on the site server is insufficient, the following actions might be now taken: Events are output according to the free space size, or a part of the JP1/IT Desktop Management functions is automatically stopped.
- The guideline of the disk capacity required for the operation log database was changed.
- The guideline of the recommended disk capacity was changed.
- The explanation about port setting was corrected. An explanation about the network between JP1/IT Desktop Management - Remote Site Server and an agentless computer was added.
- The values that can be specified for the following items in the Settings module were corrected:
    - Items under **Protection settings for registering USB devices** of **Agent Configuration Items** that can be opened from the **Agent Configurations** view under **Agent**
    - Items in the **AMT** view under **Inventory**
    - Items in the **Active Directory** view under **General**
    - Items in the **MDM Linkage Settings** view under **General**

- The memory usage on the following servers was changed:
    - Management server in a single-server configuration system
    - Database server in a multi-server configuration system

Changes in 10-01

- The offline management function can now be used to manage computers that are not connected to the management server via a network.
- Information about JP1/IT Desktop Management can now be updated by acquiring support service information including anti-virus product information.
- During asset management, the license types and product IDs of some purchased software products, as well as software types, can now be managed.
- A description stating the following was added: Suspicious file reproduction operations and suspicious printing operations are handled differently.
- Differences in the Home module and Assets module when administration scopes are assigned were corrected.
- Software can now be added to the managed-software list by using the **Software Inventory** view of the Device module.
- The description of the case in which a site server is deployed within the network search range was improved.
- A description stating the following was added: To discover networked devices in an environment with site servers deployed, the management server and the site server must be mutually accessible by their IP addresses.
- A cautionary note about when a discovery range includes a loop-back address or broadcast address was added.
- Windows 8 and Windows Server 2012 were added as applicable OSs for JP1/IT Desktop Management - Agent.
- The explanation of the legend of the table indicating the system information that can be acquired from Active Directory was improved.
- A description stating the following was added: **SNMP: NG(No credential)** might appear if not enough information was collected to identify a device.
- The Host Name entry was added in the computer information that can be collected as system information.
- A description stating that the Workstation service of the OS of a managed computer must be running to collect the following information was added.
    - Automatic Windows Update in Windows Update Details
    - Windows Service Details
    - OS Security Details
- The description of **Registered Date/Time** shown on the **Installed Computers** tab was corrected.
- The conditions that must be met to control the power status of a computer were corrected.
- The time when the computer is restarted can now be set in the **Add Agent Configuration** dialog box and the **Edit Agent Configuration** dialog box. Accordingly, the descriptions of the **Shutdown Computer** and **Computer Restart settings** dialog boxes that appear on a computer with the agent installed were changed.
- Whether device information can be collected from any MDM system was added. The explanation of the legend was improved.
- A description stating the following was added: When you use the remote control feature, if there is no mouse connected to a computer with the agent installed, the mouse pointer will always be shaped as an arrow regardless of context.
- A description of how to specify the settings to control network connections so that newly discovered devices are automatically permitted to connect to the network was added.

- The settings you need to enter in the network control list for devices used in particular ways were added.
- A description stating that the computers for which network monitor is enabled are not judged for Windows firewall was added.
- The following products were added as supported anti-virus products (Japanese versions):
    - Norton AntiVirus 2012 (32-bit, 64-bit)
    - Norton AntiVirus (32-bit, 64-bit)
    - ウイルスバスター 2012 クラウド (32-bit, 64-bit)
    - ウイルスバスター クラウド (32-bit, 64-bit)
    - ウイルスバスター コーポレートエディション 10.6 (32-bit, 64-bit)
    - ウイルスバスター ビジネスセキュリティ 7.0 (32-bit, 64-bit)
    - Kaspersky Endpoint Security 8 for Windows 8.1 (32-bit, 64bit)
    - Kaspersky Endpoint Security 8 for Windows (32-bit, 64-bit)
    - ESET NOD32 Antivirus 5.0 (32-bit, 64-bit)
    - ESET NOD32 Antivirus 5.2 (32-bit, 64-bit)
    - Sophos Endpoint Protection - Enterprise 10 (32-bit, 64-bit)
    - Sophos Endpoint Protection - Advanced 10 (32-bit, 64-bit)
    - Sophos Endpoint Protection - Basic 10 (32-bit, 64-bit)
    - F-Secure Client Security 9.11 (32-bit, 64-bit)
    - F-Secure Client Security 9.20 (32-bit, 64-bit)
    - F-Secure Client Security 9.31 (32-bit, 64-bit)
    - F-Secure Client Security 9.32 (32-bit, 64-bit)

  The following products were removed from the supported anti-virus products (Japanese versions).
    - ウイルスバスター 2010 (32-bit, 64-bit)
    - F-Secure Client Security 8.01 (32-bit, 64-bit)
- A note that applies when a security policy (for which Block Printing or Acquisition of Operations Logs is set) is assigned to an agent-installed computer, and actions to be taken were added.
- A note that applies when both JP1/IT Desktop Management and another program restrict startup of the same software program was added.
- A note that applies when **Restrict reading/writing** is enabled for USB devices in a security policy was added.
- A note on computers running a 64-bit edition of an OS and with VMWare Server installed was added.
- Windows Internet Explorer 10 and Firefox 5 were added as Web browsers for which operation logs can be acquired.
- The description of **Original File Created Date/Time** acquired in an operation log was corrected.
- The note on the `recreatelogdb` command was corrected.
- It is now stated that ReFS is also applicable to the notes on acquiring source information of incoming files when files are moved or copied to a drive that uses a file system other than NTFS.
- The description of how devices and hardware assets are identified was corrected.
- Information about unconfirmed software can now be displayed in the **Software Inventory** view of the Device module.

- A description stating the following was added: Computers with the network monitor enabled cannot be configured in a cluster configuration.
- The description of a server on which the `ioutils exportoplog` command can be executed was corrected.
- A note for users operating a computer was added.
- Windows Internet Explorer 10 was added as a software product required for a computer on which the agent will be installed.
- The site server prerequisites were corrected.
- The prerequisites for a computer on which the network monitor is enabled were corrected.
- The prerequisites for linking with JP1/IM were added.
- The maximum disk space requirements are now separately described for the management server in a single-server configuration system, for the management server and database server in a multi-server configuration system, and for a site server.
- The list of services was changed as described below.
  - The JP1/IT Desktop Management - Manager services and the site server services were described separately.
  - Descriptions of the network monitor services and agent services were added.
  - An entry showing whether the service starts automatically was added.

    An entry showing whether the process is resident was added to the list of processes.
- The port numbers used for JP1/IT Desktop Management - Manager were described separately for a single-server configuration and for a multi-server configuration.
- Descriptions of the values set for the setup parameters and agent setting parameters when JP1/IT Desktop Management is upgraded from a version earlier than 09-50 were added.
- In accordance with the addition of the following event numbers, the range of values that can be specified for events not subject to notification was changed to *0 to 1123*.

  1117, 1118, 1123
- The default value of the start time of the acquisition schedule that can be specified in the MDM linkage settings was changed to *(Blank)*.
- Memory requirements for each system component of the product were changed.
- Disk space requirements for each system component of the product were changed.
- Prerequisite CPUs for each system component of the product were changed.
- The list of limit values was updated.
- The description of automatically obtaining information from an MDM system and the time at which information is collected were corrected.
- A description of the Windows menu names used in this manual was added.
- A maximum of 50,000 devices can now be managed by using a multi-server configuration system.
- The information that will be displayed and operations that can be performed can now be limited according to the task allocation set for the user account.
- Suppression of only writes is now possible for floppy drives and removable disks.
- JP1 event can now be reported by linkage with JP1/IM.
- A description was added stating that the root OU settings in the information about connections to Active Directory domains are not case sensitive.

- A description of the LDAP attribute name used for obtaining information such as Department, Country, and State from Active Directory was added.
- A description stating the following was added: If security countermeasures are automatically enforced, you cannot change the settings of the managed computers back to the state before the countermeasures were taken even if you use the JP1/IT Desktop Management functions.
- The following notes on network monitoring were added:
  - Notes on the Routing and Remote Access service
  - A wired LAN connection is recommended for computers for which the network monitor is enabled.
  - A mission-critical server, such as a file server, should not be configured as the network monitoring computer with network monitor enabled.
  - A note on using a DHCP server to monitor the network in which IP addresses are dynamically allocated
- A description about when a network control list is updated was added.
- A description stating the following was added: Maintenance of a network control list is performed automatically when device information is updated or deleted.
- A description stating the following was added: The devices disconnected from the network by the network monitor can only communicate with computers with the network monitor enabled in the network segment or computers registered for **Exclusive Communication Destination for Access-Denied Devices**.
- Descriptions of monitoring targets for the network monitor feature, including the networks, OSs on monitored computers, and protocols, were added.
- A description stating the following was added: If a device discovered by the monitor feature is deleted, the device will not be discovered again unless it is disconnected and then reconnected to the network.
- A description stating the following was added: A list populated with a MAC address and associated with a device can no longer be deleted from the network control list.
- A description stating the following was added: Site servers are automatically registered for **Exclusive Communication Destination for Access-Denied Devices**.
- A description stating the following was added: If a network monitor agent is installed, the service is automatically enabled and the firewall settings are automatically disabled.
- A description stating the following was added: Serial numbers that can be used as mapping keys during imports are serial numbers specified in BIOS information.
- A description stating the following was added: Installation and uninstallation of software by using the distribution function are performed with local system account permissions.
- A description stating the following was added: If a connection between a computer and a management server fails, operation logs are temporarily saved in the computer.
- A description stating the following was added: When you delete devices from the network control list, information for the devices with **Permit** specified for network connection is also deleted from the network control list. However, information for the devices with **Not Permit** specified remains in the list.
- A description stating the following was added: Servers on which Citrix XenApp or Windows terminal service is installed cannot be managed even if you install an agent.
- The description of the devices for which Windows administrative shares or SNMP authentication cannot be used was changed.
- A description stating the following was added: The Workstation service of the OS must be running on a computer on which an agent will be installed.
- A note was added on performance degradation in printer servers and network in an environment in which a network shared printer has been registered on a computer on which an agent will be installed.

- The following descriptions about agentless management were added:
  - Notes on using agentless management
  - When device information is collected
  - When executable programs for acquiring device information are sent
  - Settings necessary for managing agentless computers
- The settings required to acquire device information from agentless devices when Windows Administrative Share is enabled in Windows 7, Windows Vista, and Windows Server 2008 were changed.
- A description stating the following was added: If you delete a hardware asset for which **Asset Status** is **Unconfirmed**, the device is deleted from the Inventory Information view of the Device module.
- A description stating the following was added: A virtual environment configured by combining VMware vSphere and VMware View is not supported.
- A description of how to set the user permissions required for remote control using Windows authentication was added.
- A description stating the following was added: Devices manually registered in the network control list can also be deleted from the network control list.
- A description stating the following was added: Devices that must always be connected to the network must be registered in the network control list as the devices permitted for network connection.
- The following were added as the events that cause the network connection to change automatically:
  - Device information is updated or deleted
  - Network-connected device information is changed.
- The descriptions of information used for judgement of unauthorized software and unauthorized Windows service was corrected.
- Descriptions of user accounts not subject to security judgement were added.
- The description of Other Access Restrictions in the items that can be set for security policies was corrected.
- Supplementary notes on external media for which operation can be suppressed for each OS were added.
- Prerequisites for acquiring the following types of operation logs were changed:
  - Start and termination of programs
  - File and folder operations
  - Web access
- A description stating the following was added: Operation logs for file deletion might not be acquired depending on the method of deleting the file.
- Descriptions of the operation log information that is acquired when the user performs an undo operation (using the keyboard or **Undo** menu item) were added.
- A description of the Content-type of MIME header of email that is not handled as an attached file was added to the notes on operation logs acquired by sending and receiving emails.
- A description of the case in which files are moved or copied to a drive formatted by using other than NTFS, such as a FAT Drive, was added to the notes on acquiring source information of incoming files.
- The CSV file coding format for importing the following hardware asset information was changed:
  - Memory
  - Storage capacity
  - Free storage capacity

    - Display size
- The recommended disk space was corrected. The recommended disk space values when only operation logs related to suspicious operations are collected on the site server were added.
- A description stating the following was added: To distribute packages to many devices, distribute them in several batches or use site servers.
- The `ioutils exportdevice` command can now be used to export device information.
- The `ioutils exportdevicedetail` command can now be used to export detailed device information.
- The balloon tip message that appears when you apply a security policy that requires restarting of the computer was changed.
- Network connection environments for each system component were added to the network prerequisites.
- The condition required to use an RFB connection for starting a remote control session was changed. In addition, a caution stating that operation is not always guaranteed for remote control using the RFB connection was added.
- Descriptions of the system environment for using a site server configuration and the number of devices that can be managed by a single site server were added.
- `mgr\definition` was added as a folder that is created under the installation folder.
- The explanations of automatic execution of the following functions and when they are executed were corrected:
    - Collecting user information
    - Regularly checking and updating support information
    - Updating **Scan Engine Version** and **Virus Definition File Version** settings for anti-virus products
- The descriptions in the list of processes were corrected.
- Smart devices can now be managed by linkage with an MDM service.
- The total number of installed devices (number of used licenses) is now displayed in managed software information.
- The information that will be displayed and operations that can be performed can now be limited according to the task allocation set for the user account.
- A description stating the following was added: Agentless devices cannot be managed in a NAT environment.
- A description stating the following was added: You cannot use the network monitor feature to detect devices in network segments that are not directly accessible from the management server.
- A description stating the following was added: You can monitor multiple network segments from one computer on which the network monitor is enabled and the agent is installed if the computer has access to several networks through a number of network cards.
- Windows Server 2008 R2 Datacenter was added in the prerequisites for a management server, computers on which an agent will be installed, and site servers.
- A description of the confirmation method when software is added to a managed computer was added.
- A description of how departments and locations are defined was added. The name of a department and location can now be changed from the menu area.
- A description stating the following was added: By configuring event notification by email, you can have the administrator notified by email when a network connection is blocked or permitted.
- A description stating the following was added: If access to removable disks is suppressed, the use of USB-connected removable disks is not permitted even if they are registered as hardware assets.
- A description stating the following was added: You can use automatic update distribution based on security policies and the Windows automatic update function (Windows Update and Microsoft Update).

- If multiple instances of a managed software product are installed on one computer, they are now counted as one license used.
- A description stating the following was added: If hyphens (-) are displayed in the information area, they are replaced by null strings when exported.
- A description of the types of software that can be uninstalled by using the distribution function was added.
- A command can now be used to delete operation logs on a site server.
- Windows 7 was added in perquisites for computers for which the network monitor is enabled.
- The description of network prerequisites was improved.
- A description stating the following was added: The site servers specified to store operation logs must be placed in the same network segment as the management server in a NAT environment.
- The guidelines for the required disk space for backing up operation logs for one year were changed.
- The guidelines for the recommended disk space for all data (including operation logs) managed by JP1/IT Desktop Management 2 were changed.
- Port number 31000 was added to the list of port numbers for site servers.
- Descriptions of the rules for setting a user account password were added.
- A description stating the following was added: If a domain user is authenticated by a Windows administrative share, the user ID must be in *user-ID*@*FQDN* (*FQDN*: fully qualified domain name) or in *domain-name*\user-ID format.
- A description stating the following was added: For custom installation, at least 20 GB of disk space is required on the database storage folder drive to acquire operation logs.

A.12 Miscellaneous information for this manual

(1) Related manuals

- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Getting Started (3021-3-367(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Configuration Guide (3021-3-369(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide (3021-3-370(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Distribution Function Administration Guide (3021-3-373(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Automatic Installation Tool Administration Guide (3021-3-374(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Description (3021-3-375(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Planning and Configuration Guide (3021-3-376(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Administration (3021-3-377(E))
- Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Messages (3021-3-378(E))

(2) Related publications

- Job Management Partner 1/IT Desktop Management 2 Online Help

(3) Abbreviations for product names

Windows menu names used in this manual assume the operating systems shown below.

For management servers, computers for which the network monitor is enabled, and computers on which the controller is installed:

Windows Server 2008

For computers on which an agent is installed:

Windows XP

The **Start** menu is not displayed in Windows 8.1, Windows 8, and Windows Server 2012. Open the **Start** window in the bottom left corner of the desktop, and then select the menu.

This manual uses the following abbreviations for product names.

Abbreviation		Full name or meaning
AMT		Intel(R) Active Management Technology
Firefox		Firefox(R)
Linux		Linux(R)
NetWare		NetWare(R)
Pentium		Intel Pentium(R)
VMWare		VMWare(R)
Asset Console		Job Management Partner 1/IT Desktop Management 2 - Asset Console
JP1/AJS		Job Management Partner 1/Automatic Job Management System 2
		Job Management Partner 1/Automatic Job Management System 3
JP1/Base		Job Management Partner 1/Base
JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
JP1/NETM/NM		JP1/NETM/Network Monitor
Hibun	JP1/Hibun IC	JP1/秘文 Advanced Edition Information Cypher
	JP1/Hibun IF	JP1/秘文 Advanced Edition Information Fortress
	JP1/Hibun IF Mail Option	JP1/秘文 Advanced Edition Information Fortress Mail Option
	JP1/Hibun IS	JP1/秘文 Advanced Edition Information Share
	Hibun IC	秘文 Advanced Edition Information Cypher
	Hibun IF	秘文 Advanced Edition Information Fortress
	Hibun IF Mail Option	秘文 Advanced Edition Information Fortress Mail Option
	Hibun IS	秘文 Advanced Edition Information Share

This manual uses the following abbreviations for function names.

Abbreviations	Full name
Programs and Features	Add/Remove Programs
	Add/Remove Programs
	Programs and Features

This manual uses the following abbreviations for Microsoft product names.

Abbreviations			Full name or meaning
Active Directory			Microsoft(R) Active Directory
Internet Explorer	Windows Internet Explorer		Windows(R) Internet Explorer(R)
Microsoft.NET			Microsoft(R).NET
Microsoft Cluster Service			Microsoft(R) Cluster Service
Microsoft Excel			Microsoft(R) Excel(R)
Microsoft Office Excel			Microsoft(R) Office Excel(R)
Microsoft Forefront			Microsoft(R) Forefront(TM)
Microsoft Lync			Microsoft(R) Lync
Microsoft Office			Microsoft(R) Office
Microsoft Office Access			Microsoft(R) Office Access(R)
Microsoft Office InfoPath			Microsoft(R) Office InfoPath(R)
Microsoft Office OneNote			Microsoft(R) Office OneNote
Microsoft Office Outlook			Microsoft(R) Office Outlook(R)
Microsoft Outlook			
Microsoft Office PowerPoint			Microsoft(R) Office PowerPoint(R)
Microsoft Office Project			Microsoft(R) Office Project
Microsoft Office Publisher			Microsoft(R) Office Publisher
Microsoft Office Visio			Microsoft(R) Office Visio(R)
Microsoft OneNote			Microsoft(R) OneNote
Microsoft Outlook Express			Microsoft(R) Outlook(R) Express
Microsoft Project			Microsoft(R) Project
Microsoft Publisher			Microsoft(R) Publisher
Microsoft Visio			Microsoft(R) Visio(R)
Microsoft InfoPath			Microsoft(R) InfoPath(R)
MS-DOS			Microsoft(R) MS-DOS(R)
Windows	Windows 2000	Windows 2000 Advanced Server	Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Windows 2000 Professional	Microsoft(R) Windows(R) 2000 Professional Operating System
		Windows 2000 Server	Microsoft(R) Windows(R) 2000 Server Operating System

Abbreviations			Full name or meaning
Windows	Windows 7	Windows 7 Enterprise	Microsoft(R) Windows(R) 7 Enterprise
		Windows 7 Home Basic	Microsoft(R) Windows(R) 7 Home Basic
		Windows 7 Home Premium	Microsoft(R) Windows(R) 7 Home Premium
		Windows 7 Professional	Microsoft(R) Windows(R) 7 Professional
		Windows 7 Starter	Microsoft(R) Windows(R) 7 Starter
		Windows 7 Ultimate	Microsoft(R) Windows(R) 7 Ultimate
	Windows 8	Windows 8	Windows(R) 8
		Windows 8 Enterprise	Windows(R) 8 Enterprise
		Windows 8 Pro	Windows(R) 8 Pro
	Windows 8.1	Windows 8.1	Windows(R) 8.1
		Windows 8.1 Enterprise	Windows(R) 8.1 Enterprise
		Windows 8.1 Pro	Windows(R) 8.1 Pro
	Windows Server 2003	Windows Server 2003 (x86)	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
			Microsoft(R) Windows Server(R) 2003, Standard Edition
			Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
		Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
			Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows Server 2008	Windows Server 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 Enterprise without Hyper-V(R)
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Windows Server 2008 Foundation	Microsoft(R) Windows Server(R) 2008 R2 Foundation
		Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 Standard
			Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(R)
			Microsoft(R) Windows Server(R) 2008 R2 Standard

Abbreviations			Full name or meaning
Windows	Windows Server 2012	Windows Server 2012 Datacenter	Microsoft(R) Windows Server(R) 2012 Datacenter
		Windows Server 2012 Standard	Microsoft(R) Windows Server(R) 2012 Standard
		Microsoft Windows Server 2012 R2 Datacenter	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Windows Server 2012 R2 Standard	Microsoft(R) Windows Server(R) 2012 R2 Standard
	Windows Vista	Windows Vista Business	Microsoft(R) Windows Vista(R) Business
		Windows Vista Enterprise	Microsoft(R) Windows Vista(R) Enterprise
		Windows Vista Home Basic	Microsoft(R) Windows Vista(R) Home Basic
		Windows Vista Home Premium	Microsoft(R) Windows Vista(R) Home Premium
		Windows Vista Ultimate	Microsoft(R) Windows Vista(R) Ultimate
	Windows XP	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
		Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System
Windows 95			Microsoft(R) Windows(R) 95 Operating System
Windows 98			Microsoft(R) Windows(R) 98 Operating System
Windows Live Mail			Windows Live(TM) Mail
Windows Me			Microsoft(R) Windows(R) Millennium Edition Operating System
Windows Media Player			Windows Media(R) Player
Windows NT 4.0			Microsoft(R) Windows NT(R) Server Enterprise Edition Version 4.0
			Microsoft(R) Windows NT(R) Server Network Operating System Version4.0
			Microsoft(R) Windows NT(R) Workstation Operating System Version4.0
Windows NT 3.51			Microsoft(R) Windows NT(R) Server Network Operating System Version3.51
			Microsoft(R) Windows NT(R) Workstation Operating System Version3.51
Windows Mail			Windows(R) Mail

(4) Acronyms

Acronym	Full name or meaning
ARP	Address Resolution Protocol
AVI	Audio Video Interleave
BIOS	Basic Input / Output System

Acronym	Full name or meaning
BMP	Bit Map
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory
CF	CompactFlash
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Database
DBMS	Database Management System
DCOM	Distributed Component Object Model
DHCP	Dynamic Host Configuration Protocol
DVD	Digital Versatile Disc
FC	Fibre Channel
FD	Floppy Disk
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
ICCID	Integrated Circuit Card ID
ICMP	Internet Control Message Protocol
ID	IDentification
IDE	Integrated Drive Electronics
IEEE	Institute of Electrical and Electronic Engineers
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
ISMS	Information Security Management System
IT	Information Technology
KVM	Keyboard Video Mouse
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
NAPT	Network Address Port Translation
NAS	Network Attached Storage
NAT	Network Address Translation
NTFS	NT File System

Acronym	Full name or meaning
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PDCA	Plan Do Check Action
PGP	Pretty Good Privacy
RAM	Random Access Memory
RFB	Remote Framebuffer
SD	Secure Digital
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSD	Solid State Drive
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Account Control
UDID	Unique Device IDentifier
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time, Coordinated
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRAM	Video Random Access Memory
WAN	Wide Area Network
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

(5) Fonts and symbols used in this manual

Fonts and symbols used in explanations

Text formatting	Description
Character string	Italic characters indicate a variable. Example: A date is specified in *YYYYMMDD* format.

Text formatting	Description
Bold - Bold	Indicates selecting menu items in succession. Example: Select **File** - **New**. This example means that you select **New** from the **File** menu.
key + **key**	Indicates pressing keys on the keyboard at the same time. Example: **Ctrl** + **Alt** + **Delete** means pressing the **Ctrl**, **Alt**, and **Delete** keys at the same time.
/	Slashes between multiple items represent the word "or". Example: `A/B` means `A` or `B`.

Conventions in syntax explanations

Symbols	Convention
`String`	Indicates a variable.
[ ]	Square brackets indicate that the enclosed item or items are optional. Example: [A] means that you can specify A or nothing.
{ }	Curly brackets indicate that one of the enclosed items must be selected. Items are delimited by vertical bars (|). Example: {A | B | C} means you must specify A, B, or C.
|	A vertical bar separates multiple items, and has the meaning of OR. Example: A | B | C means A, B, or C.

(6) About Help

JP1/IT Desktop Management 2 provides the following online help information.

Product operation help

This help provides product operation examples and explains how to use functions and do troubleshooting. You can view the help by selecting **Help** and then **JP1/IT Desktop Management 2 Help** in the JP1/IT Desktop Management 2 operation window.

Window explanation help

This help explains about the currently displayed operation window. You can view the help by clicking the **Help** button in the operation window.

(7) Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

1 KB (kilobyte) is 1,024 bytes. 1 MB (megabyte) is 1,024^2 bytes. 1 GB (gigabyte) is 1,024^3 bytes. 1 TB (terabyte) is 1,024^4 bytes. 1 PB (petabyte) is 1,024^5 bytes.

B. Glossary

This section explains the terminology used in JP1/IT Desktop Management 2.

A

Active Directory server

A server with Active Directory installed. An Active Directory server connects to Job Management Partner 1/IT Desktop Management 2 in systems that manage devices by linking with Active Directory.

added management item

A custom management item added to the asset information managed by JP1/IT Desktop Management 2. By creating added management items, administrators can manage information tailored to their needs.

Administration scope

A user account parameter that defines the scope of the administrator's responsibility within the organization.

administrator computer

The computer a JP1/IT Desktop Management 2 administrator uses to log in to JP1/IT Desktop Management 2.

agent

A program installed on computers managed by JP1/IT Desktop Management 2. The agent reports information to JP1/IT Desktop Management 2 - Manager, and controls the computer based on instructions received from JP1/IT Desktop Management 2 - Manager. The program name is JP1/IT Desktop Management 2 - Agent.

agent configurations

The settings used to set up the agent on a managed computer. Agent configurations are kept on the management server. You can remotely change how an agent is configured by creating agent configurations from an operation window and assigning them to the agent.

agentless

A managed device without JP1/IT Desktop Management 2 - Agent installed.

Asset management using Asset Console

A feature that manages assets by using Asset Console, which is a JP1/IT Desktop Management 2 component. Asset management using an operation window is called as such.

B

blacklist method

A method of controlling network access by specifying devices that are not allowed to connect to the network. Devices not specified in the list are allowed to connect to the network.

C

chat server

A connection destination for computers that will be taking part in a chat session.

connection list

A feature that lets you manage connection-destination computers for the remote control function independently, without using the JP1/IT Desktop Management 2 operation module.

contract company information

A class of asset information managed by JP1/IT Desktop Management 2. Contract company information consists of contact information for companies from which an organization has licensed software or entered into an agreement regarding a device (hardware asset).

contract company list

A list used to manage contract company information.

contract information

A class of asset information managed by JP1/IT Desktop Management 2. Contract information consists of information about contracts related to devices (hardware assets) and licensed software.

controller

A program that remotely controls a managed computer.

custom group

A group created by an administrator for a specific purpose. You can use custom groups to group the information managed by JP1/IT Desktop Management 2 in meaningful ways.

D

database manager

A tool used to back up and restore the database, and reorganize the database area.

default agent configuration

A group of agent settings provided by JP1/IT Desktop Management 2. These settings include the connection-target management server, installation parameters, and other settings needed to set up the agent.

default policy

A security policy provided by JP1/IT Desktop Management 2. This policy contains the basic settings required to maintain a secure environment.

The default policy is assigned to managed computers by default. It is also assigned if you remove a security policy from a managed computer to which no other security policies are assigned.

device information

Information that JP1/IT Desktop Management 2 collects from managed devices. Device information is required for managing computers, and includes the hardware usage and installed software types on the managed computers. You can view device information in the **Device Inventory** view of the Device module.

diagnosis

The process of evaluating a system by assessing its security status. You can view the results of a diagnosis in a report.

Distribution using Remote Installation Manager

A feature of distribution using Remote Install Manager (which is a JP1/IT Desktop Management 2 component). You can also use a command for distribution. This is one of the two distribution features provided by JP1/IT Desktop Management 2, and the other is ITDM-compatible distribution.

E

external media

Writable media such as USB memory and external hard drives. You can use external media to install offline management agents and to collect device information from computers that are being managed offline.

H

hardware asset information

A class of asset information managed by JP1/IT Desktop Management 2. Information about the devices (hardware assets) held by an organization is registered as hardware asset information.

I

information area

An area that appears in the right side of the operation window. The information displayed in this area depends on the menu item selected in the menu area on the left side of the window.

information collection tool

A tool that collects device information from computers being managed offline. The information collection tool consists of the `getinv.vbs` command and files containing the information needed to collect device information.

installation set

A program that helps users install and set up JP1/IT Desktop Management 2 - Agent in one operation. An installation set is created on a management server, and provides an installer that handles the installation and setup of the agent.

installed software

The software installed on a managed computer. JP1/IT Desktop Management 2 automatically collects information about installed software as device information.

ITDM-compatible distribution

A feature of distribution using the Distribution (ITDM-compatible) operation window, which is one of the two distribution features provided by JP1/IT Desktop Management 2. The other distribution feature is one that uses Remote Installation Manager.

J

JCR file

A file used by JP1/IT Desktop Management 2 to store video information. Video recorded during a remote control session is saved as a JCR file with the extension `JCR`. You can play back JCR files in the remote control player.

Job Management Partner 1/IT Desktop Management 2

A system that manages IT assets from device management, security management, and asset management perspectives.

Job Management Partner 1/IT Desktop Management 2 - Agent

A program installed on computers managed by Job Management Partner 1/IT Desktop Management 2.

Job Management Partner 1/IT Desktop Management 2 - Asset Console

A program installed on the asset management server.

Job Management Partner 1/IT Desktop Management 2 - Manager

A program that provides the server functionality of Job Management Partner 1/IT Desktop Management 2.

Job Management Partner 1/IT Desktop Management 2 - Network Monitor

A program installed on a computer that monitors the network.

JP1/NETM/Network Monitor

A program that monitors the network and controls the network connections of devices. JP1/NETM/NM is installed on a network control appliance.

JP1/NETM/Network Monitor - Manager

A program that centrally manages JP1/NETM/NM. JP1/NETM/NM - Manager is installed on the management server in systems that link with JP1/NETM/NM - Manager.

judgment

The process of assessing the device information collected from each computer by JP1/IT Desktop Management 2 against a security policy, and assigning a security level (violation level) for each item in the security policy and for the computer in general.

judgment-excluded user settings file

A file that specifies OS user accounts to exclude from security status judgment.

L

license key file

A file provided to purchasers of JP1/IT Desktop Management 2 licenses. A license key file is used to activate a license.

M

managed-software information

A class of asset information managed by JP1/IT Desktop Management 2. JP1/IT Desktop Manager uses managed-software information to keep track of software licenses. You can display the number of software licenses for each piece of managed software, and see how many of those licenses are in use. You can also manage several versions of the same software as one set of managed-software information.

management server

A computer on which JP1/IT Desktop Management 2 - Manager is installed. This can be also called a *distribution management system* or *manager* in a description regarding distribution using Remote Installation Manager.

mandatory software

Software that must be installed on every computer in an organization. Mandatory software is one aspect of a security policy.

MDM product

A product that manages smart devices. An MDM product is installed on an MDM server, and links with Job Management Partner 1/IT Desktop Management 2 to manage smart devices.

MDM server

A server with an MDM solution installed. An MDM server connects with Job Management Partner 1/IT Desktop Management 2 when you manage smart devices by linking with an MDM product.

MDM system

A generic name for the MDM products that manage smart devices.

menu area

An area that appears in the left side of the operation window. The menu displayed in this area depends on the selected module. Select a menu item to display the corresponding information in the information area on the right side of the operation window.

N

network control appliance

An appliance product with JP1/NETM/NM installed. By linking with JP1/NETM/NM - Manager, you can use JP1/IT Desktop Management 2 to control the network connections in network segments that are monitored by a network control appliance.

network control list

Settings that define whether individual devices are allowed to connect to the network. You can also permit a device to access the network for a set period of time.

network monitor

A feature that automatically detects when a device without permission (a device that is not registered as a management target or exclusion target) is connected to the network, and controls the network connection.

network monitor agent

A program installed on a computer that monitors the network. The network monitor agent is installed automatically when you select a computer that is managed online in the operation module and enable the network monitor. The program name is Job Management Partner 1/IT Desktop Management 2 - Network Monitor.

network monitor settings

Settings that define how network monitor controls the network connections of devices that establish new connections to network segments with the network monitor feature enabled.

O

offline management

A method of using external media to manage computers that the management server cannot access over the network. In contrast to *online management*.

offline management agent

An agent that is configured to not connect to the management server in the agent configurations. Install an offline management agent on computers that you want to manage offline. In contrast to an *online management agent*.

offline management framework

A framework used to manage computers that the management server cannot access over the network. This includes standalone computers and computers connected to an isolated network at a remote site.

online management

A way to manage computers that are connected to the management server by a network. In contrast to *offline management*.

online management agent

An agent that is configured to communicate with the higher systems in the agent configurations. Install an online management agent on computers that you want to manage online. In contrast to *offline management agent*.

operation log

Log information about operations performed on managed computers. You can collect operation logs from computers that are managed online.

P

package (for ITDM-compatible distribution)

A set of software programs or files to be distributed to other computers, which is registered in JP1/IT Desktop Management 2 from the Distribution (ITDM-compatible) window. You can also use this window to distribute a package.

prohibited software

Software whose use is prohibited within an organization. Prohibited software is one aspect of a security policy.

R

recommended security policy

A security policy provided by JP1/IT Desktop Management 2. The settings in this policy are designed to create a robust security environment.

Relay system

A server on which JP1/IT Desktop Management 2 - Agent is installed as a relay system. Using a relay system can reduce the load caused by remote installation and remote collection on the management server and the network. The program name is JP1/IT Desktop Management 2 - Agent.

Remote collection

A feature of batch collection of files stored in the managed computers by using Remote Installation Manager.

remote control agent

A component of the agent program. All remote control functions become available when a standard connection is used between the remote control agent and the controller.

remote control feature

A feature that allows a user to connect to a remote computer and control it using keyboard and mouse operations.

remote control player

A video player that plays back video recorded in a remote control session. The remote control player lets you pause and skip the video as needed.

Remote installation

A feature of batch distribution of software programs and files from the management server to users' computers via the network.

Remote Installation Manager

A component of JP1/IT Desktop Management 2. Install this component if you want to perform distribution using Remote Installation Manager.

removable disk

A recordable disk that can be removed from a disk drive.

report

A window that presents information compiled from the JP1/IT Desktop Management 2 database for a certain purpose. You can then print the information displayed on the screen.

request server

A feature that processes connection requests for the remote control function.

revision history

Information that serves as a record of changes made to the device information of a managed computer. You can view revision history from the operations module, or output it to a CSV file for archival purposes.

revision history archive

Revision history entries output as a CSV file for archival purposes.

RFB

A communication protocol used to access remote computers over a network. RFB is primarily used in Virtual Network Computing (VNC), and supports communication between computers running different operating systems. JP1/IT Desktop Management 2 uses RFB to remotely control agentless computers and computers running OSs other than Windows.

S

search

The process of discovering devices connected to the network in a specified network range, and devices registered with Active Directory.

security policy

A set of rules that define the criteria for determining danger levels, and actions to perform when certain conditions are met. You can define security policies on the management server and assign them to managed computers.

In a security policy, you can set criteria for determining the danger level of a computer, and define actions that take place automatically under certain conditions. You can also configure the system to warn the user when a computer reaches a particular danger level.

smart device

A small, portable terminal device such as a smartphone, tablet PC, or PDA.

software license information

A class of asset information managed by JP1/IT Desktop Management 2. Software license information is used to manage software licenses for individual purchases (at the asset level).

support information file

A file used to register information about the latest program updates information in JP1/IT Desktop Management 2.

support service site

A Web site to provide support services. JP1/IT Desktop Management 2 can acquire the latest updates for the OS and Internet Explorer by connecting to the support service site over the Internet.

suspicious file transfer

A suspicious operation detected when the following actions are deemed suspicious in a security policy:

Send/Receive E-mail with Attachments

Use Web/FTP Server

Copy/Move the File to External Device

suspicious print operation

A suspicious operation detected when **Large Number of Printing Jobs** is selected as a target of suspicious activity monitoring in a security policy.

system administrator permission

A permission you can assign when you create a user account in JP1/IT Desktop Management 2. A user with this permission has full access to the management features of JP1/IT Desktop Management 2, with the exception of user account management.

T

task

An single act of installing software distributed from the management server, distributing files, or uninstalling software. Each software or file distribution task involves the distribution of a specific package.

task allocation

A user account parameter that defines the tasks for which an administrator is responsible. By setting up user accounts with the appropriate combination of task allocations and permissions, you can limit the operations an administrator can perform to those appropriate to his or her role.

U

update group

A group of update programs to be applied or removed together. By specifying an update group in a security policy, you can apply or remove the update programs in that group to or from all computers that are subject to the security policy.

user management permission

A permission you can assign when you create a user account in JP1/IT Desktop Management 2. A user with this permission is able to add and delete user accounts in JP1/IT Desktop Management 2.

V

view permission

A permission assigned when you create a user account in JP1/IT Desktop Management 2. A user with this permission is able to view modules other than the Settings module, but cannot add new information or change existing settings.

violation level

A rating that indicates the security risk posed by a computer. A computer's violation level is determined by assessing it against a security policy. There are six violation levels: Critical, Important, Warning, Safe, Unknown, and Out of Target.

VNC

Software used to remotely control another computer over a network.

W

whitelist method

A method of controlling network access by specifying devices that are allowed to connect to the network. Devices not specified in the list are blocked from connecting to the network.

Windows Update

A program that applies updates to Windows, Internet Explorer, and other products provided by Microsoft.

Index