HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/IT Desktop Management Administration Guide

3021-3-339-10(E)

Notices

■ Relevant program products

P-2642-73AL Job Management Partner 1/IT Desktop Management - Manager 10-10

The above product includes the following:

• P-2642-74AL Job Management Partner 1/IT Desktop Management - Manager (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-2642-75AL Job Management Partner 1/IT Desktop Management - Remote Site Server (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-2642-76AL Job Management Partner 1/IT Desktop Management - Network Monitor (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 (x86))

• P-2642-77AL Job Management Partner 1/IT Desktop Management - Agent (for Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Vista, Windows Server 2003, Windows XP, Windows 2000)

■ Trademarks

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

ActiveX 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.

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

Firefox is a registered trademark of the Mozilla Foundation.

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.

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

Mac and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

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

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

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

MobileIron is a registered trademark of MobileIron in the United States.

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

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

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

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

Symantec, Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

VMware is a registered trademark or a trademark of VMware, Inc. in the United States and/or other jurisdictions.

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/).

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

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

Feb. 2014: 3021-3-339-10(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-339-10(E)) and product changes related to this manual.

Changes	Location
Information was added to explain that no more than 50,000 IP addresses can be set for the search range when you specify a period to perform an intensive search for the devices on a network.	1.1.1(2), 6.4
You can now add any policies that are related to computer security settings to the security policies and judge security status by using any conditions.	1.8.2(3), 9.3.7
You can now collect the revision history of device information.	1.9.9, 15.6.7, 18.7, 18.9, A.11(1)
You can now manage license usage for each managed software product from the **Software License Status** view.	1.10.1(6), 1.10.2(2), 1.10.2(5), 1.10.2(6), 1.10.4(1), 1.10.4(2), 1.12.3
A policy related to the computer's security settings can now be added to the security policies to allow security evaluation based on user-specified conditions.	1.14, 1.14.1, 1.14.2, 1.14.4
For the groups displayed in the menu area, you can now batch-delete departments and locations that have already been deleted from definitions.	1.14.3, 6.28, 6.29, 6.30, 6.31, 15.5.6
In the Security module and Device module, you can now create groups that automatically sort managed computers according to any condition.	5.5, 9.1
You can now select whether to display the balloon hints of the Job Management Partner 1/IT Desktop Management icon in the task tray and the entry window for user information on user computers.	6.11, 6.14, 12.6
In the Settings module, you (the system administrator) can now specify when users can start entering user information.	6.14
For the Network Filter List, you can now specify whether to enable automatic updates for all items or only for additional items.	8.7.4, A.11(1)
By linking with Job Management Partner 1/NETM/Network Monitor - Manager, you can now, from Job Management Partner 1/IT Desktop Management, control network connections that are monitored by the appliance products on which Job Management Partner 1/NETM/Network Monitor is installed.	8.9, A.11(1)
You can now limit software licenses and the display range of contracts according to the jurisdiction range specified for user accounts.	11.2.5
An explanation about changing the MDM system server certificate after importing the server certificate to the management server was added. Also, the Internet Explorer version was deleted from the procedure for specifying settings to link with an MDM system.	15.9.4
All descriptions of command execution restrictions were moved to 17.1 *Executing Commands*. Also, a description about executing a command other than `getinv.vbs` when OS user account control (UAD) is enabled was added.	17.
The procedure for executing commands on a computer on which an agent is already installed was added.	17.1
Items to be noted during command execution were added.	17.1, 17.34
You can now import or export definitions of asset management items in CSV format.	17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 17.10, 17.11, 17.12, 17.13, 17.14, 17.15, 17.16, 17.20, 17.21, 17.22,

Changes	Location
You can now import or export definitions of asset management items in CSV format.	17.23, 17.24, 17.25, 17.26, 17.27, 17.33, 17.34, 18.6, A.7
The return value (1) was added to the description of the `ioutils importfield` command.	17.7
A note regarding the specification of the -filter option for the `ioutils exportoplog` command was added.	17.16
A description was added of the export format of the CSV file when you export operation logs by using the `ioutils exportoplog` command.	17.16, A.6
A description of the characters that can be used in folder names specified by the following commands was added: • `exportdb` • `importdb` • `reorgdb` • `getlogs` • `getinstlogs`	17.23, 17.24, 17.25, 17.28, 17.29
The /i option was added to the `resetnid.vbs` command to display the following two dialog boxes on the user's computer: the dialog box for selecting whether to execute the command, and the dialog box for displaying the execution results.	17.31
The following event was added as an event that requires troubleshooting: 1059	18.9
The following messages were added: KDEX1597-E, KDEX1598-E, KDEX3319-I, KDEX3320-E, KDEX3321-I, KDEX3322-E, KDEX4126-W, KDEX4387-E, KDEX4388-E, KDEX4389-E, KDEX4390-E, KDEX4391-E, KDEX4392-E, KDEX4393-E, KDEX4394-E, KDEX4395-E, KDEX4396-E, KDEX4397-E, KDEX4398-W, KDEX4399-I, KDEX4400-E, KDEX4401-E, KDEX4402-E, KDEX4403-E, KDEX5305-I, KDEX5306-E, KDEX5460-I, KDEX5461-I, KDEX5462-E, KDEX5463-E, KDEX5464-I, KDEX5465-I, KDEX5466-E, KDEX5467-E, KDEX5468-E, KDEX5469-E, KDEX5470-E, and KDEX5471-E The following messages were changed: KDEX1534-W, KDEX1557-W, KDEX1576-W, KDEX1583-W, KDEX4010-E, KDEX4387-E, KDEX4388-E, KDEX4389-E, KDEX4390-E, KDEX4391-E, KDEX4392-E, KDEX4394-E, KDEX4395-E, KDEX4396-E, KDEX4397-E, and KDEX4398-W The following messages were deleted: KDEX1543-E, KDEX4065-E, and KDEX6321-E	19.2
The following events were added: 1127, 1128, 1129, 1130, 1131, 1134, 1135, 1136, and 1137 The following event was changed: 19 The following events were deleted: 50, 51, and 52	19.3
The JP1 event attribute was added to the following events: 1132, 1133, 1135, 1136, and 1137 The JP1 event attribute of the following events was changed: 1079, 1082, and 1118	19.3.1

Changes	Location
The description about port settings was modified. In addition, a description about the network between Job Management Partner 1/IT Desktop Management - Remote Site Server and agentless computers was added.	A.1
A description was added of the registration date and time and management-start date and time that appear in the device list.	A.10

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

Preface

This manual explains and gives examples of how to use Job Management Partner 1/IT Desktop Management - Manager (hereafter abbreviated as *JP1/IT Desktop Management*).

Note that details about using the GUI are explained in online Help.

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

■ Intended readers

This manual is intended for:

- Administrators who manage security and assets in an organization using JP1/IT Desktop Management.
- Readers who want to know how to use and operate JP1/IT Desktop Management.

■ Organization of this manual

This manual is organized into the following chapters:

1. Managing Computers by Using JP1/IT Desktop Management
   This chapter explains how to operate and utilize JP1/IT Desktop Management.
2. Registering a product license
   This chapter explains how to register product licenses.
3. Logging in to the Operation Window
   This chapter explains how to log in to the operation window in order to use JP1/IT Desktop Management.
4. Managing User Accounts
   This chapter explains how to manage user accounts.
5. Window Operations
   This chapter describes the common operations that can be performed in the operation windows of JP1/IT Desktop Management.
6. Device Management
   This chapter explains how to collect information from the devices and how to grasp the current status of the organization.
7. Remotely Controlling Devices
   This chapter explains how to remotely control devices within an organization.
8. Managing Network Connections of Devices
   This chapter explains how to connect or block the network of a device within the organization.
9. Managing the Security Status
   This chapter explains the concept of security management and the security status within the organization.

10. Operation Log Management

    This chapter explains how to grasp and track user operations.

11. Asset Management

    This chapter explains how to manage hardware assets, software licenses, and contracts.

12. Software and File Distribution

    This chapter explains how to perform software installation and uninstallation, and file distribution.

13. Event Reference

    This chapter explains how to reference events that are output by JP1/IT Desktop Management.

14. Report Reference

    This chapter explains how to check the statuses of security management and asset management within the organization by displaying reports.

15. Customizing Settings

    This chapter describes the items that can be customized in the Settings module and during setup.

16. Database Management

    This chapter explains how to manage a database by using the database manager.

17. Commands

    This chapter describes the JP1/IT Desktop Management commands.

18. Troubleshooting

    This chapter describes the actions to be taken when a problem occurs in JP1/IT Desktop Management.

19. Messages

    This chapter lists the JP1/IT Desktop Management messages and events.

For reference information when reading this manual, please see the Job Management Partner 1/IT Desktop Management Overview and System Design Guide.

Contents

1 Managing Computers by Using JP1/IT Desktop Management

This section describes how to manage computers by using JP1/IT Desktop Management.

1.1 Installing agents

Install agents on computers to be managed by JP1/IT Desktop Management.

When you install an agent on a computer, that computer automatically becomes a management target and device information about the computer will be collected. Using agents, you can do the following to manage your computers:

Keep track of security status.

By assigning a security policy, you can determine the security status of computers. Using a security policy, you can automatically correct any detected security problem.

Manage assets.

When computers become the management targets, their hardware asset information is automatically registered. Information collected from devices is automatically reflected in the asset information. This information, combined with other information that is not collected from the devices, such as asset management numbers and user information, allows you to keep the hardware assets of the entire organization up-to-date. You can also keep track of the usage status of software licenses.

Distribute software and files.

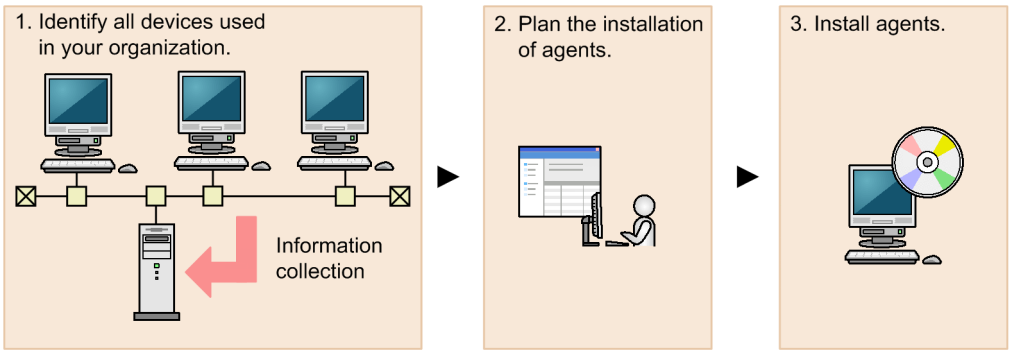
After installing agents on computers, you can use the management server to distribute and install software on, to distribute files to, or to uninstall software from the computers. This allows you to efficiently maintain software used in your organization.

If you are using JP1/IT Desktop Management to manage devices used in your organization, we recommend that you install agents on all the computers in your organization.

Tip

A device that is not a computer can be managed without installing an agent on the device.

The following figure shows you how to install agents on computers:



1. Identify all devices used in your organization.

To determine the computers on which to install agents, you need to have the latest information about all the devices currently used in your organization.

If such information is not available (for example, the management ledger is not kept up-to-date or not available), use JP1/IT Desktop Management to search for devices used in your organization.

You can skip the above step if you have the latest information about the devices used in your organization (for example, you manage all the computers by using Active Directory, or the management ledger is kept up-to-date).

2. Plan the installation of agents.

Determine which computers in your organization need to have agents installed, and how to install the agents.

Using JP1/IT Desktop Management, you can install the agents in two ways: install them using the installer provided with the agents, or distribute them for automatic installation.

3. Install agents.

   Install agents according to your installation plan.

You can perform the following management tasks for agentless computers: acquire detailed computer information, apply security policies to them, determine their security status, and create security diagnostic reports.

However, you cannot perform some functions for agentless computers, such as using a security policy to automatically correct problems or to send message notifications, and distributing software or files.

Related Topics:

- 1.1.1 Identifying all devices used in your organization
- (4) Planning the installation of agents
- 1.1.2 Manually installing agents on computers
- 1.1.3 Automatically installing agents on computers
- 1.1.4 General procedure for checking the agent installation status

1.1.1 Identifying all devices used in your organization

To determine the computers on which to install agents, you need to have the latest information about all the devices currently used in your organization.

If such information is not available (for example, the management ledger is not kept up-to-date or not available), use JP1/IT Desktop Management to search for devices used in your organization. This search allows you to collect information about all the devices used in your organization. After identifying all the devices used in your organization, plan the installation of agents. You can also have agents automatically deployed to every device discovered during the search.

If you have a management ledger or other information about the devices currently used in your organization, you do not need to perform the above search. Plan the installation of agents.

Related Topics:

- (4) Planning the installation of agents

(1) Searching for devices registered in Active Directory

This approach is one way of searching for devices used in your organization. Using the **Getting Started** wizard, you can search for devices registered in Active Directory.

The **Getting Started** wizard allows you to set the domain information and search schedule for the Active Directory you want to search. When the wizard is complete, the search begins according to the set schedule.

To search for devices registered in Active Directory:

1. In the top of the view, select the **Go** menu, and then **Getting Started Wizard**.
2. In the **What is this Wizard?** view, check the settings for managing devices, and then click the **Next** button.
3. Select **Discover Nodes**, and then click the **Next** button.

4. Select **Discovery from Active Directory**, and then click the **Next** button.
5. Set the domain information of the Active Directory you want to access, and then click the **Next** button.
   To make sure that you can access the set Active Directory, click the **Test** button.
6. Set the search schedule, and then click the **Next** button.
7. Set whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them, and then click the **Next** button.
8. If you want to inform yourself (administrator) of completion of the search by email, specify the notification destination and the mail server information, and then click the **Next** button.
9. In the **Confirm Content and Finish Settings** view, check the settings, and then click the **Complete** button.
10. In the displayed **Discovery Settings Configured** view, click the **Close** button.

The search is performed according to the set search schedule.

To view the search results, in the Settings module, select **Discovery**, **Last Discovery Log**, and then **Active Directory** to display the Active Directory view.

Tip

The settings specified in the wizard are applied to the Active Directory view. To display the Active Directory view, in the Settings module, select **Discovery**, **Configurations**, and then **Active Directory**. You can also start a search by specifying search conditions in this view.

Related Topics:

- 15.2.2 Specifying search conditions (searching Active Directory)
- 15.2.4 Checking the device discovery status

(2) Searching for devices connected to the network

This approach is one way of searching for devices used in your organization. Using the **Getting Started** wizard, you can search for devices connected to the network.

The **Getting Started** wizard allows you to set the range of IP addresses to be searched and the authentication information to be used during the search. When the wizard is complete, the search begins according to the set schedule.

To search for devices connected to the network:

1. In the top of the view, select the **Go** menu, and then **Getting Started Wizard**.
2. In the **What is this Wizard?** view, check the method used to specify the settings for managing devices, and then click the **Next** button.
3. Select **Discover Nodes**, and then click the **Next** button.
4. Select **Discovery from IP Address Range**, and then click the **Next** button.
5. Set the range of IP addresses to be searched, and then click the **Next** button.

By default, **Management Server** is set as the IP address range. **Management Server** is a network segment that contains a management server.

> **Important note**
>
> If you want to specify a period of time to intensively search, specify settings so that the number of IP addresses that are contained in the IP address range is 50,000 or lower. If the number of IP addresses exceeds 50,000, the network search might stop.

6. Set the authentication information to be used during the search, and then click the **Next** button.
7. Set the authentication information to be used for each IP address range, and then click the **Next** button.

> **Important note**
>
> If an IP address range includes devices that are configured to lock the account after a specific number of failed logon attempts, assign specific authentication information for each IP address range. If you select **Any**, all authentication information items are used in an attempt to access devices, which can lead to some users unexpectedly getting locked out of their accounts.

> **Important note**
>
> If you select **Any**, each authentication information item is used in an attempt to access devices. The high network access frequency imposes a heavy load on the network. Select this option only after carefully considering the possible network load.

8. Set the search schedule, and then click the **Next** button.

> **Important note**
>
> If you select the **Intensive Discovery** check box, the search is repeated one after another during the specified period of time. During this time, the network is placed under heavy load. Select this option only after carefully considering the possible network load.

9. Set whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them, and then click the **Next** button.
10. If you want to inform yourself (administrator) of completion of the search by email, specify the notification destination and the mail server information, and then click the **Next** button.
11. In the **Confirm Content and Finish Settings** view, check the settings, and then click the **Complete** button.
12. In the displayed **Discovery Settings Configured** view, click the **Close** button.

The search is performed according to the set search schedule.

To view the search results, in the Settings module, select **Discovery**, **Last Discovery Log**, and then **IP Address Range** to display the IP Address Range view.

Tip

The settings specified in the wizard are applied to the IP Address Range view. To display the IP Address Range view, in the Settings module, select **Discovery**, **Configurations**, and then **IP Address Range**. You can also start a search by specifying search conditions in this view.

Related Topics:

- 15.2.1 Specifying search conditions (discovery from IP address)
- 15.2.4 Checking the device discovery status

(3) 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.

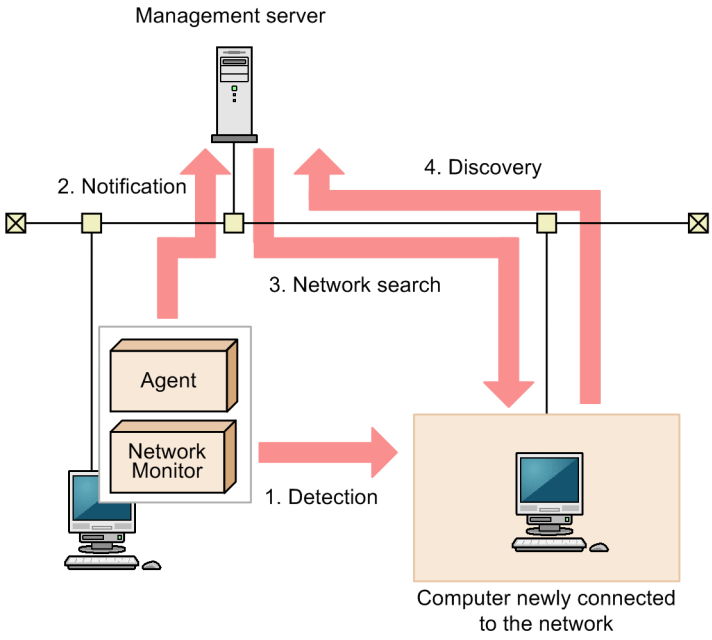
Important note

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:



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
- 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.

(4) Planning the installation of agents

After identifying all the devices used in your organization, determine which computers in your organization need to have agents installed, and how to install the agents.

Computers on which to install agents

Of the computers used in your organization, select the ones to which you want to apply security control and distribute software by using JP1/IT Desktop Management, and then install agents on them.

Computers with agents installed automatically become the management target of JP1/IT Desktop Management. A JP1/IT Desktop Management license is used for each computer that becomes a management target. Therefore, we recommend that you consider the number of available licenses when determining the computers on which to install agents.

Tip

If you want to apply security control to the management server, install an agent on the security server in the same way as you install an agent on a user's computer.

How to install agents

You can install agents on computers either manually or automatically.

You might prefer one approach over another in terms of installation conditions that are important to you. Check each approach and use the one that is appropriate for your environment.

Manually installing agents on computers

First, create an installation set. Then, using the installation set, install agents on computers. You can manually install agents on computers in one of the following seven ways:

- Upload an agent to a Web server.
- Upload an agent to a file server.
- Distribute the agent installation media (CD-R or USB memory) to users.
- Distribute agents to users as a file attached to an email.
- Install an agent on the computer by using a logon script.
- Install an agent on the computer by using the disk copy feature.
- Install an agent on the computer from the provided medium.

Automatically installing agents on computers

From the management server, automatically deploy agents to the individual computers. You can automatically install agents on computers in one of the following two ways:

- Automatically deploy agents to every computer discovered during the search.
- Deploy agents to selected groups of computers on which agents have not yet been installed.

Related Topics:

- 1.1.2 Manually installing agents on computers
- 1.1.3 Automatically installing agents on computers

1.1.2 Manually installing agents on computers

To manually install agents on computers, first create an agent installation set. Then, using the installation set, install agents on computers.

For details about how to create an installation set, see 6.2 Creating an installation set.

There are several approaches to installing agents on computers by using the installation set. You might prefer one approach over the others in terms of installation conditions that are important to you. Check each approach and use the one that is appropriate for your environment.

If you want to allow users to perform the installation task:

Set up the environment so that users can activate the installation set. In this way, users can install an agent on their computers without having to perform the setup task. Using one of the following approaches, you can allow users to perform the installation task:

- (3) Uploading an agent to a Web server
- (4) Uploading an agent to a file server
- (5) Distributing the agent installation media (CD-R or USB memory) to users
- (6) Distributing agents to users as a file attached to an email

If you do not want to allow users to perform the installation task:

Store the installation set on a file server. Then, register a logon script in a domain controller so that when a user logs on to Windows, an agent is automatically installed on the user's computer. Using the following approach, you can have an agent installed on a user's computer without having the user perform the installation task:

- (7) Installing an agent on the computer by using a logon script

If you want to install agents on computers before distributing the computers to users:

Before distributing computers to users, install an agent on a model computer by using an installation set. Then, copy the entire contents of a hard drive of the model computer to a hard drive of each computer to be distributed, by using a tool or software specially designed for this purpose. Using the following approach, you can install agents on computers before distributing the computers to users:

- (8) Installing an agent on the computer by using the disk copy feature

You can also allow users to manually install an agent on their computers from the provided medium. This approach requires a setup task.

(1) Creating an installation set

To manage computers in your organization by installing agents on the computers, you need to create an installation set. You can upload the created installation set to a Web portal so that users can download it to their computers. You can also record the installation set on CDs or DVDs and distribute them to users. In this way, the users can install agents on their computers by simply running the installation set on their computers.

Create an installation set as described below.

To create an installation set:

1. In the top of the view, select the **Go** menu, and then **Getting Started Wizard**.
2. In the displayed dialog box, click the **Next** button.
3. Select **Create Agent Installer**, and then click the **Next** button.

4. Select an agent configuration you want to apply to each computer, and then click the **Create** button.

   A dialog box for downloading an installation set appears. The default file name displayed in the dialog box is `ITDMAgt.exe`.

   An agent configuration defines the actions of each agent. You can add a new agent configuration in the Agent Configurations view. To display the Agent Configurations view, in the Settings module, select **Agent** and then **Agent Configurations**.

   To change the installation folder or to specify an account with Administrator privileges to allow general users to install agents on their computers, select the following check boxes and enter necessary information:

   Change Installation Folder

   Allows you to change the folder to which to install an agent.

   To change the installation folder, select this check box, and then enter the new installation destination for an agent under **Installation Folder**.

   Set the account to install Agent.

   Allows you to select whether to specify an account with Administrator privileges to allow users to install agents on their computers. This setting is enabled only for the task of installing agents on the computers running the following OSs: Windows 2000, Windows XP, and Windows Server 2003.

   The users need to have Administrator privileges on their computers in order to install agents on the computers.

   If you select this check box, users who do not have Administrator privileges can install agents by using the specified account. The use of the Administrator privileges is restricted to the task of installing an agent. This setting is therefore useful when you want to allow users with restricted privileges to install agents on their computers.

Downloading of the installation set begins.

Tip

You can also create an installation set in the Agent Configurations view. To display the Agent Configurations view, in the Settings module, select **Agent** and then **Agent Configurations**. Click the **Create Agent Installer** button for the agent configuration you want to apply to computers. In the displayed dialog box, enter the necessary information, and then click the **OK** button. Downloading of the installation set begins.

Related Topics:

- 15.3.2 Adding agent configurations
- (2) Installing agents on computers

(2) Installing agents on computers

After creating an installation set, use it to install agents on computers. The following are examples of how to use the installation set:

Upload an agent to a Web server.

Store the installation set on a Web server and take measures to make sure that users can download it from any sites within your organization. The computer users access the Web server from any sites within your organization, download the installation set, and then install an agent on their computers.

Upload an agent to a file server.

Store the installation set on a file server and take measures to make sure that users can access the file server and download the installation set. The computer users access the file server, download the installation set, and then install an agent on their computers.

Distribute the agent installation media to users.

Store the installation set on media (CD-R or USB memory) and distribute the media to the computer users. The computer users install an agent on their computers from the provided medium.

Distribute agents to users as a file attached to an email.

Attach the installation set to an email and send it to the computer users. The computer users run the file attached to the received email to install an agent on their computers.

Install an agent on the computer by using a logon script.

Create an installation set, prepare a batch file for the logon script that runs the installation set, and then store the batch file on a domain controller. When the computer users log on to the OS, an agent is automatically installed on their computers.

Install an agent on the computer by using the disk copy feature.

Install an agent on a model computer. Create a backup of the entire contents of a hard drive of the model computer, and then restore the backup data to the computers on which you want to install agents.

Related Topics:

- (3) Uploading an agent to a Web server
- (4) Uploading an agent to a file server
- (5) Distributing the agent installation media (CD-R or USB memory) to users
- (6) Distributing agents to users as a file attached to an email
- (7) Installing an agent on the computer by using a logon script
- (8) Installing an agent on the computer by using the disk copy feature

(3) Uploading an agent to a Web server

Create and store the installation set on a Web server located within your organization. Then, take measures to make sure that users can download the installation set from any sites within your organization, and inform users that the installation set has been uploaded.

The users then access the applicable page to install an agent on their computers.

Tip

An alternative to this approach would be to provide a URL that enables the users to directly navigate to the file stored on the Web server and download it to their computers.

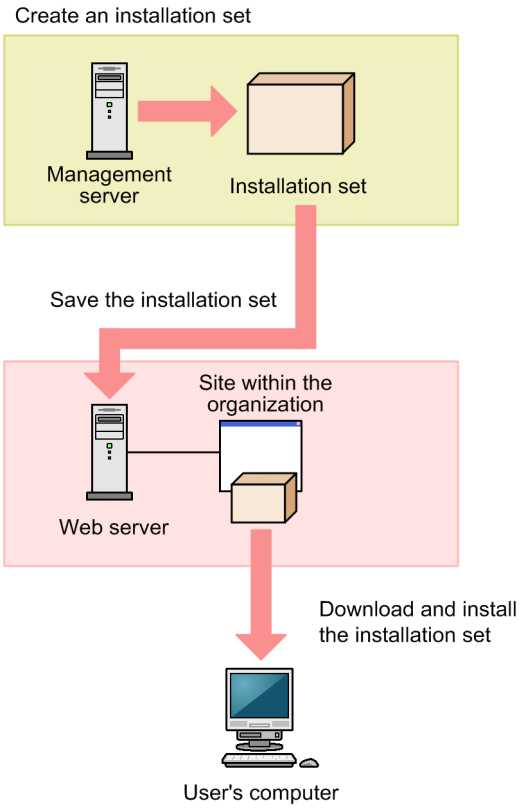
Advantage:

Informing all applicable users of the URL of the applicable site is a quick way of having agents installed on a large number of computers. In addition, because a Web system is used in this approach, the server side remains secure even without access control.

Disadvantage:

This approach requires an environment that allows you to build a Web server and enables users to access the Web server.

The following figure shows an overview of how an agent is installed from the Web server:



Related Topics:

- 6.2 Creating an installation set
- 1.1.4 General procedure for checking the agent installation status

(4) Uploading an agent to a file server

Store the installation set on the file server (file sharing server). Users then access the file server to install an agent on their computers.

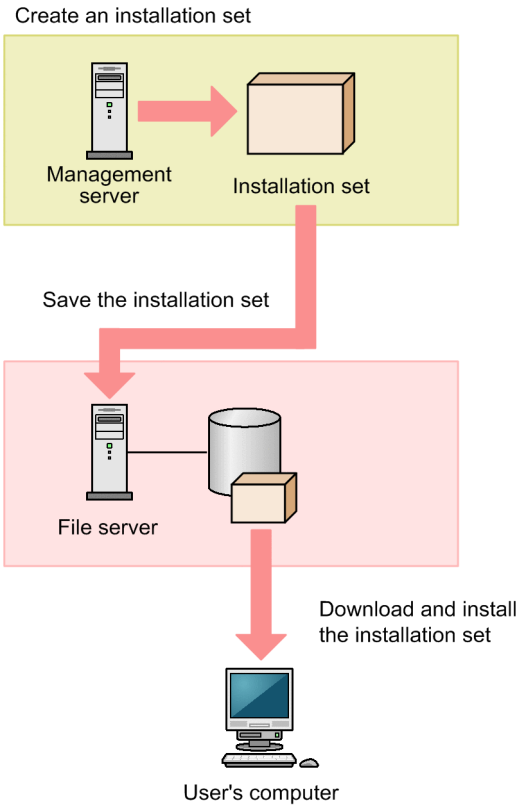
Advantage:

Informing all applicable users of the location where the installation set is stored is a quick way of having agents installed on a large number of computers.

Disadvantage:

This approach requires an environment that allows for file sharing. In addition, because users are accessing a file sharing server, the server side must have access control capabilities to prevent users from accessing files for which they do not have permissions.

The following figure shows an overview of how an agent is installed from the file server:



Related Topics:

- 6.2 Creating an installation set
- 1.1.4 General procedure for checking the agent installation status

(5) Distributing the agent installation media (CD-R or USB memory) to users

Record the installation set data to a medium (CD-R or USB memory), and then distribute it to each user. Users then use the distributed medium to install an agent on their computers.

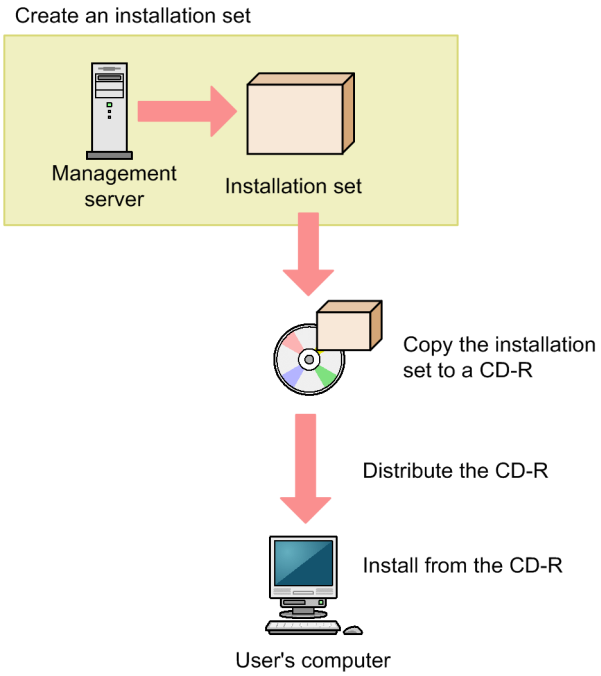
Advantage:

This approach does not require you to create a security control page on a Web site, or to create an environment that allows for shared folder. This approach is useful when there are relatively small number of computers on which to install agents. In addition, even when the network speed is slow, users can install an agent without affecting network performance. This approach also makes an agent program available to each user who has the privileges to configure user computers.

Disadvantage:

This approach is time-consuming because it requires you to copy data to a required number of media and then distribute them to users.

The following figure shows an overview of how an agent is installed from a distributed CD-R medium:



Tip

If you create `Autorun.inf` and then record it to a CD-R medium along with the installation set, installation starts automatically when a user inserts the medium into the user's computer. The following example shows how to create `Autorun.inf`, where `ITDMAgt.exe` is the name of the file storing the installation set:

```
[Autorun]
```

```
open=ITDMAgt.exe
```

Related Topics:

- 6.2 Creating an installation set
- 1.1.4 General procedure for checking the agent installation status

(6) Distributing agents to users as a file attached to an email

Attach the installation set to emails, and then send them to users. Users then double-click the attached file to install an agent on their computers.

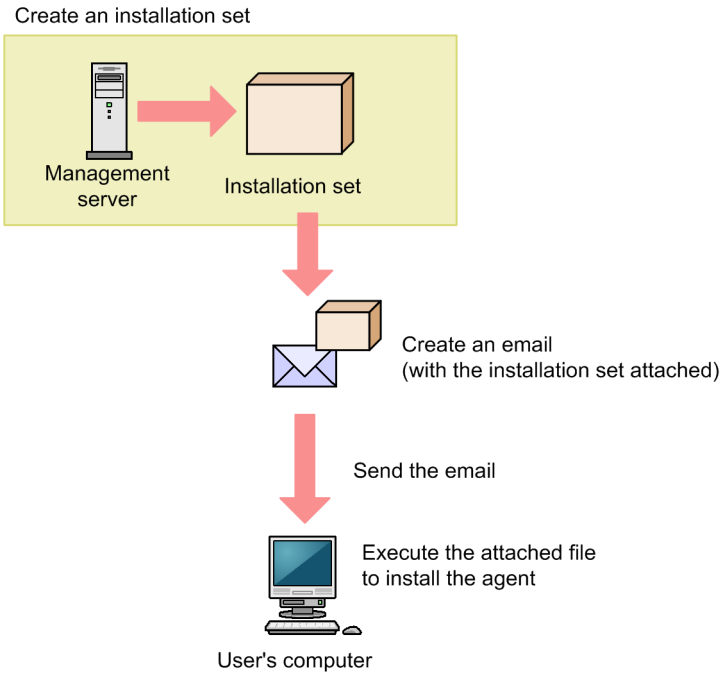
Advantage:

Sending emails to all applicable users is a quick way of having agents installed on a large number of computers.

Disadvantage:

The size of an installation set is approximately 30 MB. Sending an email with the installation set attached to a large number of destinations can increase the burden on the mail server. In addition, if there is a limit on the size of files that can be attached to an email, email transmission might fail.

The following figure shows an overview of how an agent is installed from the file attached to an email:



Related Topics:

- 6.2 Creating an installation set
- 1.1.4 General procedure for checking the agent installation status

(7) Installing an agent on the computer by using a logon script

Store the installation set on a file server. Then, create a batch file for the logon script that runs the installation set, and store it on the Active Directory server. When users log on to Windows, an agent is automatically installed on their computers. If an agent is already installed on a computer, the agent is not reinstalled.

The following example shows how to create a batch file for the logon script:

```
if %PROCESSOR_ARCHITECTURE%==AMD64 (
if not exist "%ProgramFiles(x86)%\Hitachi\jp1itdma\bin\jdnglogon.exe" (
start /w \\server-name\shared-folder-name\ITDMAgt.exe
)
) else (
if not exist "%ProgramFiles%\Hitachi\jp1itdma\bin\jdnglogon.exe" (
start /w \\server-name\shared-folder-name\ITDMAgt.exe
)
)
```

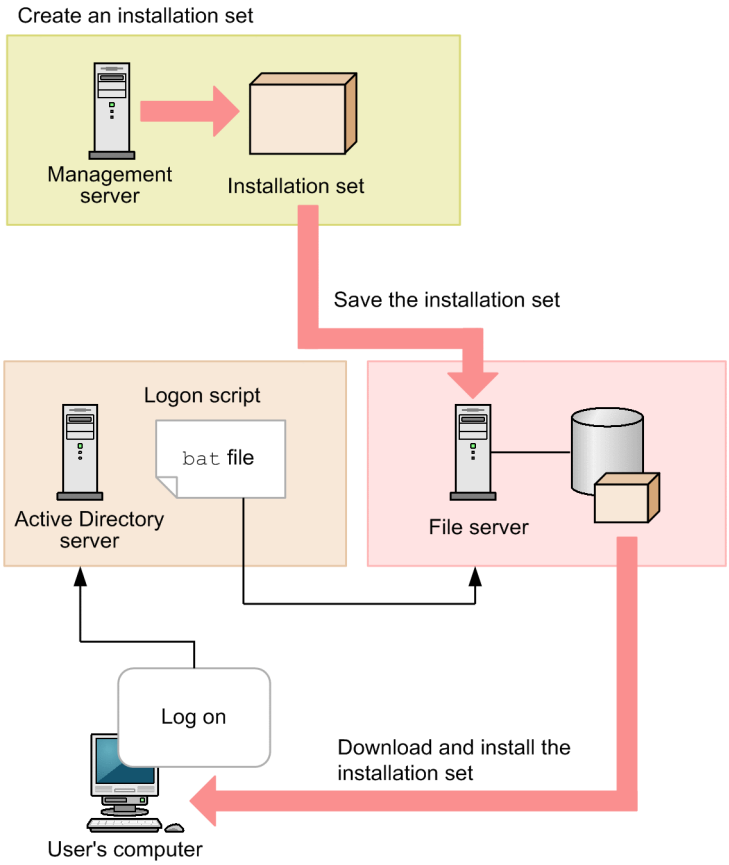
Advantage:

By using the logon script, you can have agents automatically installed on computers without having users perform the installation task. This eliminates the risk of errors caused by operational mistakes made by users.

Disadvantage:

This approach requires a file server and the environment that allows users to access the file server. In addition, the users' computers must be controlled by a domain controller, and there must be an environment that allows the logon script to run.

The following figure shows an overview of how an agent is automatically installed by the logon script:



Related Topics:

- 6.2 Creating an installation set
- 1.1.4 General procedure for checking the agent installation status

(8) Installing an agent on the computer by using the disk copy feature

Before distributing computers to users, install an agent on a model computer by using an installation set. After the installation is complete, execute the `resetnid.vbs` command on the model computer to reset the unique ID (host identifier) assigned to the model computer. Then, copy the entire contents of a hard drive of the model computer to a hard drive of each computer to be distributed, by using a tool or software specially designed for this purpose. After completing this task, distribute the computers to users.

Important note

Before using the disk copy feature, make sure that you execute the `resetnid.vbs` command on the model computer (source computer). If you do not execute this command, the target computers become indistinguishable from the source computer.

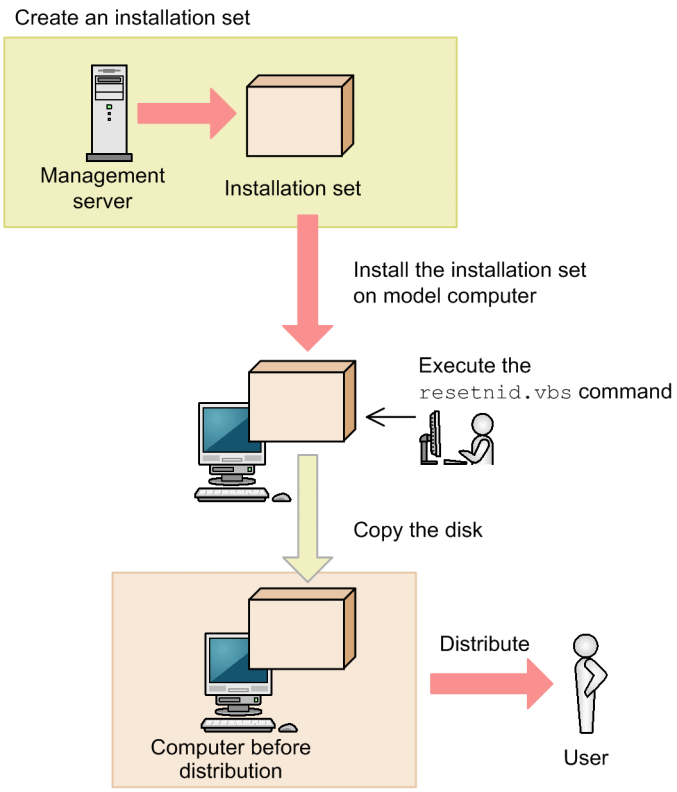
Advantage:

Because computers are distributed with agents installed and set up, users do not have to perform the installation task. This eliminates the risk of errors caused by operational mistakes made by users.

Disadvantage:

You can use this approach only for computers that are not distributed to users yet. When computers are already distributed to users, you cannot use this approach to install agents on them.

The following figure shows an overview of how an agent is installed through the disk copy feature:



Related Topics:

- 6.2 Creating an installation set
- 1.1.4 General procedure for checking the agent installation status
- 17.31 resetnid.vbs (resetting the host ID)

1.1.3 Automatically installing agents on computers

You can automatically deploy agents to the individual computers from the management server. You can use one of the following two approaches to deploy agents to computers:

Automatically deploy agents to every computer discovered during the search.

You can automatically deploy agents to computers discovered during the search if these computers run the Windows OS. With this approach, you can have an agent deployed to every computer discovered during the search. Therefore, select this approach when you want to automatically deploy agents to all the computers in your organization.

Deploy agents to selected groups of computers on which agents have not yet been installed.

With this approach, you can deploy agents to selected groups of computers to be managed and computers discovered during the search. This approach gives you the option to select the computers to which you want to deploy agents. Therefore, select this approach when you do not want to install agents on some of the computers in your organization.

(1) Automatically deploying an agent to every computer discovered during the search (Active Directory search)

This is one way of automatically deploying agents to computers discovered during the search. You can use this approach to deploy an agent to every computer discovered during the Active Directory search.

Tip

During agent deployment, approximately 30 MB of data is transmitted to each computer.

To automatically deploy an agent to every computer discovered during the search (Active Directory search):

1. In the Settings module, select **Discovery**, **Configurations**, and then **Active Directory** to display the Active Directory view.
2. Under **Discovery Option:**, click the **Edit** button.
3. In the displayed dialog box, select the **Auto-Install Agent** check box.
4. Click the **OK** button to close the dialog box.
5. Click the **Start Discovery** button.

The search begins and an agent is deployed to every discovered computer. To view the agent deployment status, in the Settings module, select **Agent** and then **Agent Deployment** to display the Agent Deployment view.

Tip

To start the Active Directory search from the **Getting Started** wizard, display the **Specify Discovery Option** view, and then select the **Auto-Install Agent** check box.

(2) Automatically deploying an agent to every computer discovered during the search (network search)

This is one way of automatically deploying agents to computers discovered during the search. You can use this approach to deploy an agent to every computer discovered during the network search.

Tip

During agent deployment, approximately 30 MB of data is transmitted to each computer.

To automatically deploy an agent to every computer discovered during the search (network search):

1. In the Settings module, select **Discovery**, **Configurations**, and then **IP Address Range** to display the IP Address Range view.
2. Under **Discovery Option:**, click the **Edit** button.
3. In the displayed dialog box, select the **Auto-Install Agent** check box.
4. Click the **OK** button to close the dialog box.
5. Click the **Start Discovery** button.
6. In the displayed dialog box, click the **OK** button.

The search begins and an agent is deployed to every discovered computer. To view the agent deployment status, in the Settings module, select **Agent** and then **Agent Deployment** to display the Agent Deployment view.

Tip

To start the network search from the **Getting Started** wizard, display the **Specify Discovery Option** view, and then select the **Auto-Install Agent** check box.

(3) Automatically deploying an agent to every computer discovered during the search (monitoring device's network connection)

This is one way of automatically deploying agents to computers discovered during the search. You can use this approach to deploy an agent to every computer discovered during the search performed by the network monitoring function.

Tip

During agent deployment, approximately 30 MB of data is transmitted to each computer.

To automatically deploy an agent to every computer discovered during the search (monitoring device's network connection)

If network access from a newly connected device is detected during network access monitoring, the network is automatically searched for the detected device. To have an agent automatically deployed to the device discovered during the search, you need to specify the following two settings:

- Permit network access from newly connected devices.
- Enable the setting that automatically deploys an agent to every computer discovered during the network search.

To permit network access from newly connected devices:

1. In the Settings module, select **Network Access Control**, and then **Assign Network Access Control Settings** to display the Assign Network Access Control Settings view.
2. Select the path to the network segment to which you want to automatically deploy agents.
3. Click the **Change Assigned Settings** button.
4. In the displayed dialog box, select the network monitor setting for which **Allow Network Access** is set for **Discovered Nodes Option:**.

   Note that **Allow Network Access** is set for **(Standard)** that is provided by default.
5. Click the **OK** button.

When a newly connected device accessing the target network segment is detected, the device is automatically granted access to the network. The network is then searched for the detected device.

To enable the setting that automatically deploys an agent to every computer discovered during the network search:

1. In the Settings module, select **Discovery**, **Configurations**, and then **IP Address Range** to display the IP Address Range view.
2. Under **Discovery Option:**, click the **Edit** button.
3. In the displayed dialog box, select the **Auto-Install Agent** check box.
4. Click the **OK** button.

The network is searched for the detected device. If the device is discovered, an agent is automatically deployed to the device.

(4) Checking the device discovery status

In JP1/IT Desktop Management, after discovering devices in an organization, you can check the discovery history or the status of the discovered devices in the **Discovery** view of the Settings module. In this way, you can determine the current status of an organization's devices.

There are the following two types of device discovery history. Check the discovery history appropriate for the discovery method you used.

- Active Directory discovery history
- IP discovery history

There are the following three device management statuses. If necessary, either include or exclude a discovered device as a managed device.

Discovered

A discovered device is managed and displayed in the **Discovered Nodes** view that opens when you select **Discovery** in the Settings module. You can manage discovered devices or exclude them from the management target.

Managed

Specify this management status for the devices you want to manage in JP1/IT Desktop Management. The devices are displayed in the **Managed Nodes** view that opens when you select **Discovery** in the Settings module. You can also exclude these devices from management. Note that specifying this status for a device you want to manage consumes a product license.

Ignored

Specify this management status for devices that do not need to be managed in JP1/IT Desktop Management. These devices are displayed in the **Ignored Nodes** view that opens when you select **Discovery** in the Settings module. You can also change the status to *Managed* or delete these devices. When *Ignored* has been set for a device, the device is not displayed in the **Discovered Nodes** view even if you run a discovery again.

Related Topics:

- 15.2.5 Checking the latest discovery status
- 15.2.6 Checking the discovered devices
- 15.2.7 Checking the managed devices
- 15.2.8 Checking the excluded devices

(5) Checking the latest discovery status

You can check the latest discovery execution status and results in a list.

To check the latest discovery status:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Last Discovery Log**.
3. In the information area, select **Active Directory** or **IP Address Range**.

The **Active Directory** view or the **IP Address Range** view appears. The discovery log is updated according to the progress of search.

> **Tip**
>
> You can also stop or start a search from the **Active Directory** view or the **IP Address Range** view. If a discovery error occurs frequently, we recommend that you stop the search and correct the search condition settings. After correcting the settings, perform a search again.

(6) Checking the discovered devices

You can check the devices discovered during the Active Directory or network search in a list. In addition, you can change the status of the discovered devices to **Managed** (management targets) or **Ignored** (exclusion targets), or remove them from the list.

To check the discovered devices:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Discovered Nodes**.

The **Discovered Nodes** view appears. In this view, you can check the number of discovered devices, number of devices that can be managed, and the number of managed devices.

To change the status of a device to **Managed**, select a device in the information area, and then click the **Manage** button. To change the status of the device to **Ignored**, click the **Ignore** button. To remove the device from the list, from **Action**, select **Remove**. You can also select multiple devices at a time and change their status to **Managed** or **Ignored**, or remove them from the list.

Note that devices with the **Ignored** status are not displayed in the **Discovered Nodes** view. If you want to manage these devices again, access the **Ignored Nodes** view, and then change their status to **Managed**. If you want to manage the devices that you have previously removed, perform a search again.

Related Topics:

- 15.2.7 Checking the managed devices
- 15.2.8 Checking the excluded devices

(7) Checking the managed devices

You can check the devices managed by JP1/IT Desktop Management in a list. In addition, you can change the status of the managed devices to **Ignored** (exclusion targets), or remove them from the list.

To check the managed devices:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Managed Nodes**.

The **Managed Nodes** view appears. In this view, you can check the number of managed devices and the remaining number of devices that can be managed.

To change the status of a device to **Ignored**, select a device in the information area, and then click the **Ignore** button. To remove the device from the list, from **Action**, select **Remove**. You can also select multiple devices at a time and change their status to **Ignored** or remove them from the list.

Note that devices with the **Ignored** status are not displayed in the **Managed Nodes** view. If you want to manage these devices again, access the **Ignored Nodes** view, and then change their status to **Managed**.

Tip

If you remove a device from the list and then perform a search again, the removed device is displayed in the **Discovered Nodes** view. To display the **Discovered Nodes** view, in the Settings module, select **Discovery** and then **Discovered Nodes**.

Related Topics:

- 15.2.8 Checking the excluded devices

(8) Checking the excluded devices

You can check the devices that are excluded from being managed by JP1/IT Desktop Management in a list. In addition, you can change the status of the excluded devices to **Managed** (management targets).

To check the excluded devices:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Ignored Nodes**.

The **Ignored Nodes** view appears. In this view, you can check the number of excluded devices and the remaining number of devices that can be managed.

To change the status of a device to **Managed**, select a device in the information area, and then click the **Manage** button. To remove the device from the list, from **Action**, select **Remove**. You can also select multiple devices at a time and change their status to **Managed** or remove them from the list.

Tip

If you remove a device from the list and then perform a search again, the removed device is displayed in the Discovered Nodes view. To display the Discovered Nodes view, in the Settings module, select **Discovery** and then **Discovered Nodes**.

Related Topics:

- 15.2.7 Checking the managed devices

(9) Deploying agents to selected groups of computers on which agents have not yet been installed

You can deploy agents to selected groups of computers to be managed.

Tip

During agent deployment, approximately 30 MB of data is transmitted to each computer.

To deploy agents to selected groups of computers:

1. In the Settings module, select **Agent** and then **Agent Deployment** to display the **Agent Deployment** view.
2. Select the computers to which you want to deploy agents.
3. Click the **Deploy Agent** button.
4. In the displayed dialog box, select an agent configuration you want to apply to computers.
5. Click the **OK** button.

Agents are deployed to selected computers. To view the agent deployment status, in the Settings module, select **Agent** and then **Agent Deployment** to display the **Agent Deployment** view.

Tip

An agent is installed to the folder specified in the default agent configuration. If you have changed the installation folder, you need to specify the drive and the write-enabled folder. Note that the specified agent configuration is applied to computers after the installation is complete.

1.1.4 General procedure for checking the agent installation status

To check whether agents have been installed on computers within your organization, use the **Device Inventory** view of the Device module.

In the **Device Inventory** view, you can view a list of managed devices. Icons displayed in the **Management Type** column of the list show you whether an agent has been installed on each computer to be managed.

One of the following icons is displayed in the **Management Type** column before and after agent installation:

-  : An agent has been installed on this computer.
-  : An agent has not been installed on this computer. The computer, however, is managed as an agentless computer.
-  : An agent has not been installed on this computer.

To check whether agents have been installed on all computers, compare the computers listed in the management ledger against the computers displayed in the **Device Inventory** view of the Device module.

Tip

If you do not have a management ledger, use the search function to discover the devices used in your organization. You can create a management ledger by including the discovered devices as management targets.

1. View only the computers on which agents have been installed.

   Using the filtering function, display the computers for which **Agent Management** is set as **Management Type**.

2. Export device information.

   From **Action**, select either **Export Device List** or **Export Device Details**. In the displayed dialog box, select the information items you want to export, and then click the **OK** button. Select the information items that you can use to make a comparison against the items listed in the management ledger.

3. Check the agent installation status.

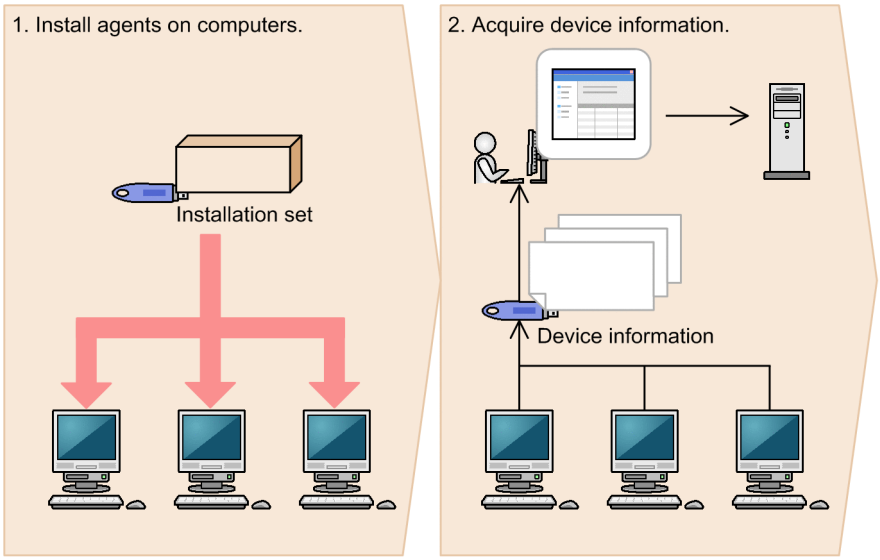
   Compare the computers listed in the management ledger against the exported list of computers. Computers that are listed in the management ledger but not listed in the exported list are the ones on which agents have not yet been installed.

If you find any computers on which agents have not yet be installed, inform the applicable users to install an agent on their computers as soon as possible. If you have configured automatic agent deployment, agent deployment might have failed. In this case, check the deployment status in the **Agent Deployment** view of the Settings module, and then deploy agents to computers again, or manually install agents on computers on which agent deployment has previously failed.

1.2 Managing devices offline

Using the offline management function provided by JP1/IT Desktop Management, you can manage computers not connected to the management server in the same way as you manage online computers.

To manage devices offline:



1. Install agents on computers.

   To manage computers offline by using JP1/IT Desktop Management, create an agent configuration for offline management, and then create an installation set. Using an external storage medium, install agents on computers.

2. Acquire device information.

   To acquire device information, collect device information from a computer on which an agent has been installed, and then send the collected device information to the management server. You can acquire device information in one of the following two ways:

   - Acquire device information by using an external storage medium.

     This approach is useful when you want to acquire device information from a stand-alone computer or when there are relatively few number of computers to be managed offline.

   - Acquire device information by using a logon script.

     This approach is useful when you want to acquire device information from computers connected to a local network or when there are relatively large number of computers to be managed offline.

By preparing two external storage media, one for installing an agent on a computer and the other for acquiring device information, you can perform the installation task, and then immediately proceed to acquire device information.

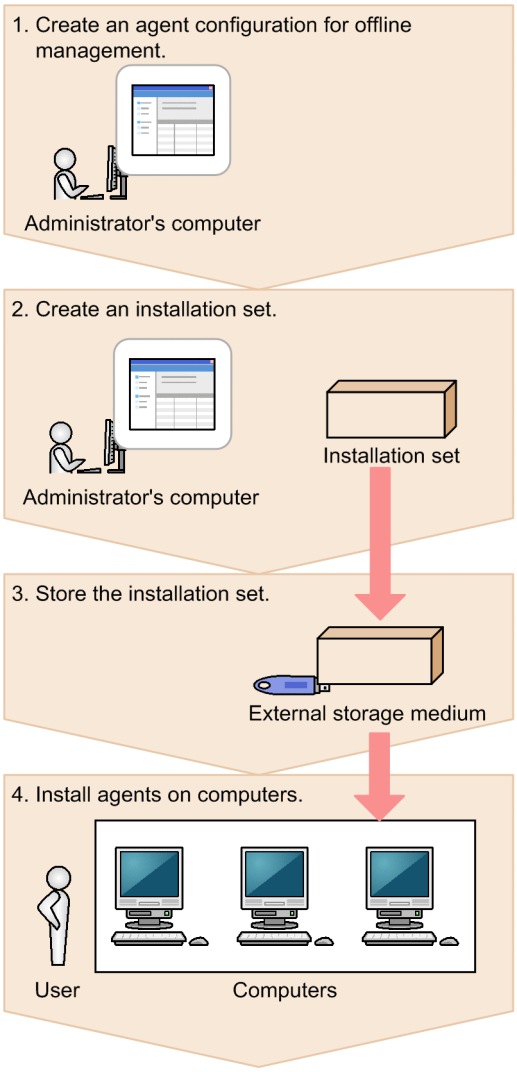
Related Topics:

- 1.2.1 General procedure for installing agents on computers to be managed offline
- 1.2.2 General procedure for acquiring device information from computers managed offline by using an external storage medium
- 1.2.3 General procedure for acquiring device information from computers managed offline by using a logon script

1.2.1 General procedure for installing agents on computers to be managed offline

To manage computers offline by using JP1/IT Desktop Management, first create an agent configuration for offline management, and then create an installation set. Using an external storage medium, install agents on computers.

The following figure shows you (system administrator) how to install agents on computers to be managed offline:



1. Create an agent configuration for offline management.

   Create an agent configuration in which the **Connect to the management server** check box is cleared by using **Agent Configurations** in the Settings module.

2. Create an installation set.

   Create an installation set with an agent configuration for offline management, and then download the created installation set on your computer.

3. Store the installation set on an external storage medium.

   Store the installation set on an external storage medium, and then provide the external storage medium to a user.

4. Install agents on computers.

The user inserts the external storage medium into a computer to be managed offline, and then runs the installation set to install an agent on the computer. Using the same external storage medium, the user repeats this step to install agents on all computers to be managed offline.

Agents are installed on all computers. When the agent installation task is complete, acquire device information from the computers to be managed offline to include them as the management targets of JP1/IT Desktop Management.

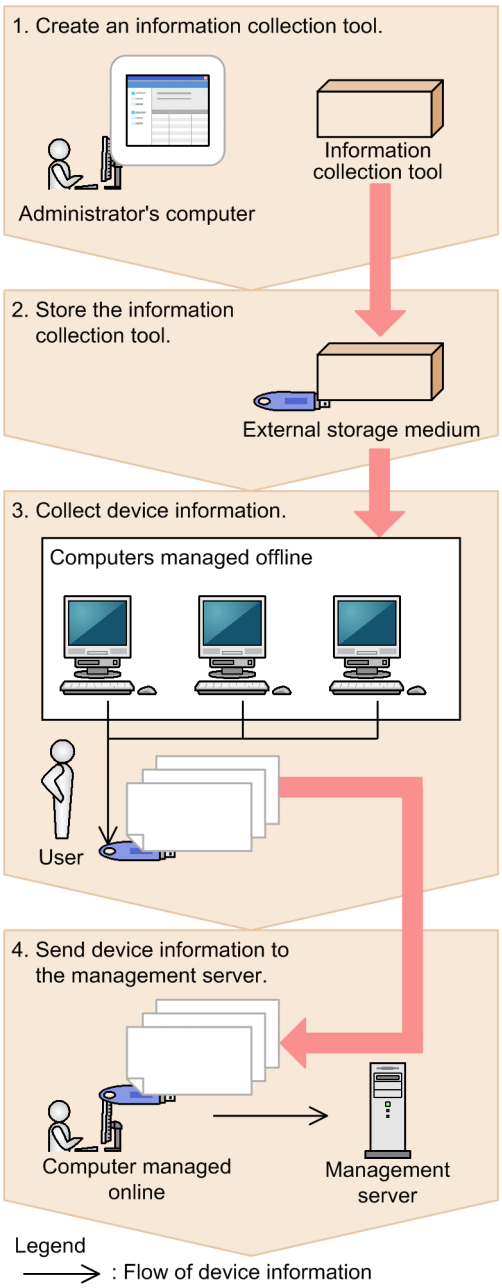
Tip

If you are installing an agent on a computer that is to be frequently switched between offline management and online management, we recommend that you prepare an agent configuration specifically designed for this purpose. If you simply apply the agent configuration for offline management to these computers, you have to change the agent configuration every time you switch between offline management and online management.

1.2.2 General procedure for acquiring device information from computers managed offline by using an external storage medium

Use an external storage medium to acquire device information from computers managed offline.

The following figure shows you (system administrator) how to acquire device information from computers managed offline:



1. Create an information collection tool.

   Access the **Device List** view, and then from **Action**, select **Create the Information Collection Tool** to create an information collection tool. The information collection tool is compressed in ZIP format.

2. Store the information collection tool.

   Decompress the information collection tool, store it on an external storage medium, and then provide the external storage medium to a user.

3. Collect device information.

   The user inserts the external storage medium into a computer that is managed offline, and then collects device information from the computer. Using the same external storage medium, the user performs this step on all computers from which the user wants to collect device information.

   When device information is collected from all computers, the user returns the external storage medium to you.

4. Send device information to the management server.

Connect the external storage medium to a computer that is managed online, and then send the collected device information to the management server.

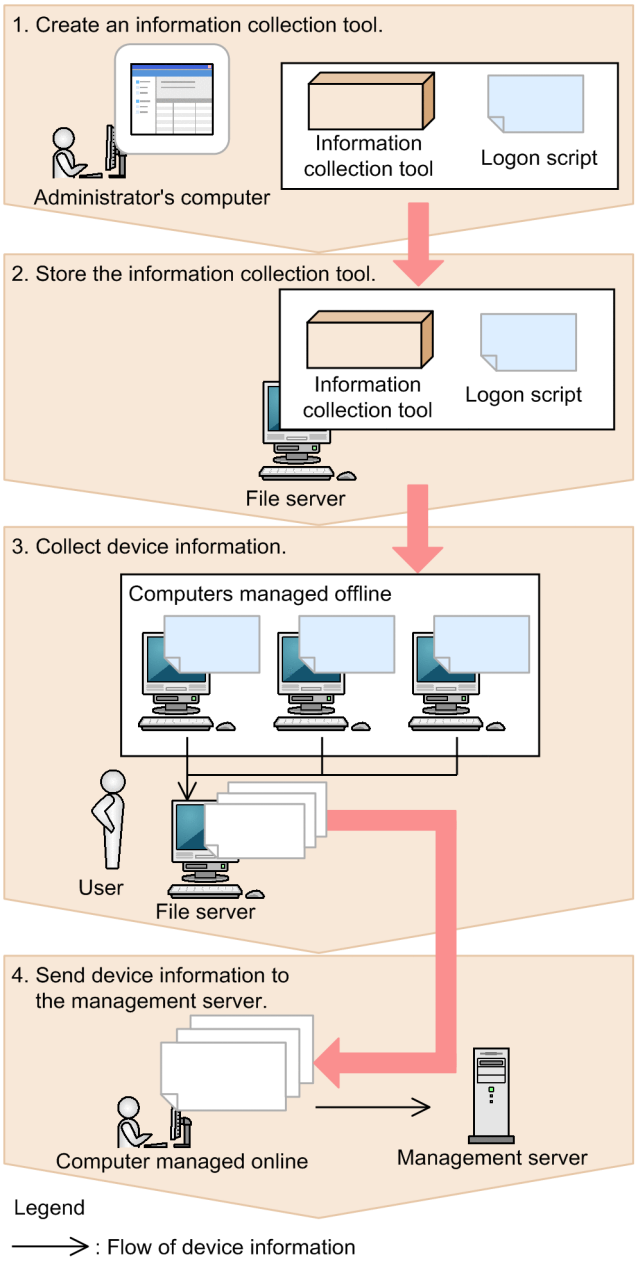
Device information of computers managed offline is acquired.

1.2.3 General procedure for acquiring device information from computers managed offline by using a logon script

You can also use a logon script to acquire device information from computers managed offline.

The figure below shows you (system administrator) how to acquire device information from computers managed offline.

Each computer managed offline must be able to access a shared folder on a file server so that you can acquire device information from computers managed offline by using a logon script.



1. Create an information collection tool.

   Access the **Device List** view, and then from **Action**, select **Create the Information Collection Tool** to create an information collection tool. The information collection tool is compressed in ZIP format.

   Then provide the information collection tool and the logon script to a user.

2. Store the information collection tool.

   The user decompresses the information collection tool, stores it in a shared folder on a file server, and then distributes the logon script to each computer managed offline.

3. Collect device information.

   When the user logs on to a Windows-based computer that is managed offline, device information is collected automatically.

   When device information is collected from every computer managed offline, the user provides the collected device information to you.

4. Send device information to the management server.

   Using a computer that is managed online, send the device information collected from computers managed offline to the management server.

Device information of computers managed offline is acquired.

Tip

Create a logon script to be distributed to computers managed offline as follows:

1. Assign a shared folder on a file server to a network drive.
2. Copy the information collection tool from the shared folder.
3. Execute the `getinv.vbs` command.
4. Copy the collected device information to the shared folder.
5. Disconnect the network drive.

1.3 General procedure for dividing tasks among administrators

With an increase in the number of employees distributed across multiple locations, it becomes increasingly more difficult for a single system administrator to manage devices and hardware assets of the entire company.

To facilitate management of the entire company under this circumstance, you (system administrator) have to divide system management tasks among several administrators by designating an administrator (or administrators) in charge of each task or business department. By specifying the permissions, task allocation, and administration scope for the user account of each administrator, you can limit the scope of information to be managed by each administrator.

You are responsible for monitoring the management status of devices and hardware assets across the entire company and giving instructions to each administrator as necessary. In this way, division of tasks among administrators helps reduce your workload and facilitates efficient management of devices and hardware assets across the entire company.

To divide tasks among administrators:

1. Determine the responsibilities of each administrator.

   Based on the structure and rules of your organization, determine the responsibilities of each administrator.

2. Register a user account to be used by each administrator.

   Register a user account for each administrator according to their responsibilities.

3. Facilitate collaboration among administrators in executing their tasks.

   Administrators perform their management tasks by accessing views in which information about their responsibilities is displayed.

   You (system administrator) perform management tasks by accessing views in which management information about the entire company is displayed.

1.3.1 General procedure for determining the settings to be specified for each user account

If there are a large number of employees distributed across multiple locations in the organization, a single system administrator might not be able to manage all the devices and hardware assets of the entire company. You (system administrator) can solve this problem by dividing system management tasks among several administrators. In addition, by specifying the permissions, task allocation, and administration scope for the user account of each administrator, you can limit the scope of information to be managed by each administrator.

To determine the permissions, task allocation, and administration scope to be specified for each user account:

1. Determine the responsibilities of each administrator.

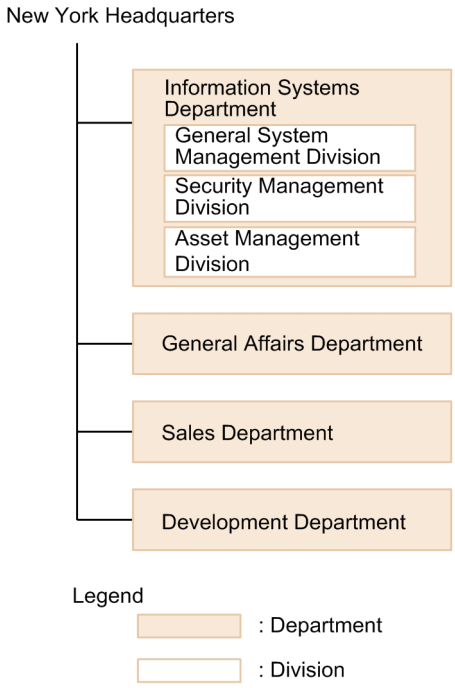
   Determine the system management tasks to be assigned to each administrator. For example, there are various system management tasks that include creating and assigning a security policy to computers, managing devices, managing software licenses, distributing software to computers, and managing user accounts. Assign these tasks to each administrator. For example, decide that Administrator B from the Security Division is responsible for creating a security policy and then assigning it to computers.

2. Determine the settings to be specified for each user account.

   Determine the settings to be specified for each user account based on the responsibilities of each administrator. You can restrict the scope of operations to be performed by each administrator by using a combination of permissions, task allocation, and administration scope specified for each user account.

Example of how to set each user account

The description below assumes an organization with the following structure:



The following table describes how to set a user account of each administrator based on their responsibilities:

Administrator's name	Division under Information Systems Department to which an administrator belongs	Responsibilities	Settings specified for each user account		
			Permissions	Task allocation	Administration scope
Administrator A	General System Management Division	• Oversee system management tasks. • Manage user accounts.	• System Administrator • User Management	All tasks	All departments
Administrator B	Security Management Division	• Create a security policy and assign it to computers. • Execute a security countermeasure. • Distribute an update program. • Distribute software.	• System Administrator	• Security management • Asset management • Device management • Distribution management	All departments
Administrator C	Asset Management Division	• Purchase, replace, or dispose of hardware assets. • Purchase, transfer, or discard software licenses. • Register asset and contract information. • Monitor the remaining number of software licenses and take necessary measures.	• System Administrator	• Asset management • Device management	Information Systems Department

Administrator's name	Division under Information Systems Department to which an administrator belongs	Responsibilities	Settings specified for each user account		
			Permissions	Task allocation	Administration scope
Administrator D	Asset Management Division	• Purchase, replace, or dispose of hardware assets. • Purchase, transfer, or discard software licenses. • Register asset and contract information. • Monitor the remaining number of software licenses and take necessary measures.	• System Administrator	• Asset management • Device management	General Affairs Department
Administrator E		• Purchase, replace, or dispose of hardware assets. • Purchase, transfer, or discard software licenses. • Register asset and contract information. • Monitor the remaining number of software licenses and take necessary measures.	• System Administrator	• Asset management • Device management	Sales Department
Administrator F		• Purchase, replace, or dispose of hardware assets. • Purchase, transfer, or discard software licenses. • Monitor the remaining number of software licenses and take necessary measures.	• System Administrator	• Asset management • Device management	Development Department
Administrator G		• Register asset and contract information.	• System Administrator	• Asset management	

In the above example, Administrator A is responsible for the overall system management tasks, including overseeing system management tasks and managing user accounts. No restriction is therefore applied to the permissions, task allocation, and administration scope specified for Administrator A's user account. Administrator G, on the other hand, is only responsible for managing the assets of Development Department. Restrictions are therefore applied to Administrator G's user account settings so that Administrator G only has the *System Administrator* permission in *Development Department*. In addition, because Development Department is large, tasks are divided between Administrator G and Administrator F, and Administrator G is only responsible for registering asset and contract information. Task allocation for Administrator G is therefore restricted to *asset management* that is required to register asset and contract information.

1.3.2 General procedure for registering multiple user accounts

With JP1/IT Desktop Management, you (system administrator) can register multiple user accounts, each of which is specified according to the responsibilities of each administrator and the department to which that administrator belongs. If there are a large number of employees distributed across multiple locations, a single system administrator might not be able to manage all the devices and hardware assets of the entire company. You can solve this problem by registering multiple user accounts to facilitate division of system management tasks among multiple administrators. In addition, because you can restrict the scope of operations performed by administrators according to the responsibilities of each administrator and the department to which that administrator belongs, you can facilitate management tasks that comply with good internal control practice.

To register multiple user accounts:

1. Collect information required to register user accounts.

   Ask administrators to provide information necessary to register user accounts (administrator's name, task description, department to which that administrator belongs, email address, and so on).

2. Register user accounts in JP1/IT Desktop Management.

   Access the Settings module, select **User Management**, and then **Account Management** to display the Account Management view in which you can register user accounts. Specify the permissions, task allocation, and administration scope for each user account according to the responsibilities of each administrator and the department to which that administrator belongs.

3. Notify administrators that their user accounts have been registered.

   Send an email to administrators notifying them of the user ID and password required to log in to JP1/IT Desktop Management.

An administrator logging in to an operation view by using the provided user account can only manage the scope of information specified in that administrator's user account.

Related Topics:

- 4.1 Adding a user account

1.3.3 General procedure for allowing multiple administrators to collaborate in performing tasks

You (system administrator) can limit the scope of information displayed on an operation view by specifying task allocation and administration scope for a user account. In this way, you can make sure that each administrator manages only the information that is relevant to either their responsibilities or the department to which they belong.

For example, if your workload increases during stocktaking, you can reduce this workload by dividing the stocktaking tasks among asset management administrators assigned each department.

To divide the hardware asset stocktaking tasks among administrators assigned to each department:

1. You ask the asset management administrator of each department to perform stocktaking of hardware assets.

   Send an email to the asset management administrator of each department asking them to perform stocktaking, instructing them how to do it, and giving them a due date of completion of stocktaking.

2. The asset management administrator of each department performs stocktaking of hardware assets that belong to the asset management administrator's own department.

   The asset management administrator of each department logs in to JP1/IT Desktop Management. When the asset management administrator displays the **Hardware Asset** view of the Assets module, that asset management

administrator can view a list of hardware assets that are within the administration scope specified for the user account. The asset management administrator exports the displayed list to a CSV file, and then prints the list.

The asset management administrator uses the printed list to conduct a physical count, enters the stocktaking results in the exported CSV file, and then imports the CSV file to JP1/IT Desktop Management. The stocktaking date and time are updated for the hardware assets of the applicable department.

3. You check the last modified date and time.

   A day after the due date of completion of stocktaking, confirm that stocktaking tasks have been completed in the entire company. To do so, you need to check the last modified date and time column of the list displayed in the **Hardware Asset** view of the Assets module.

   If you find any departments for which the stocktaking date and time have not been updated, contact the asset management administrators of the corresponding departments by email.

The stocktaking tasks of the entire company are completed.

1.4 Managing smart devices

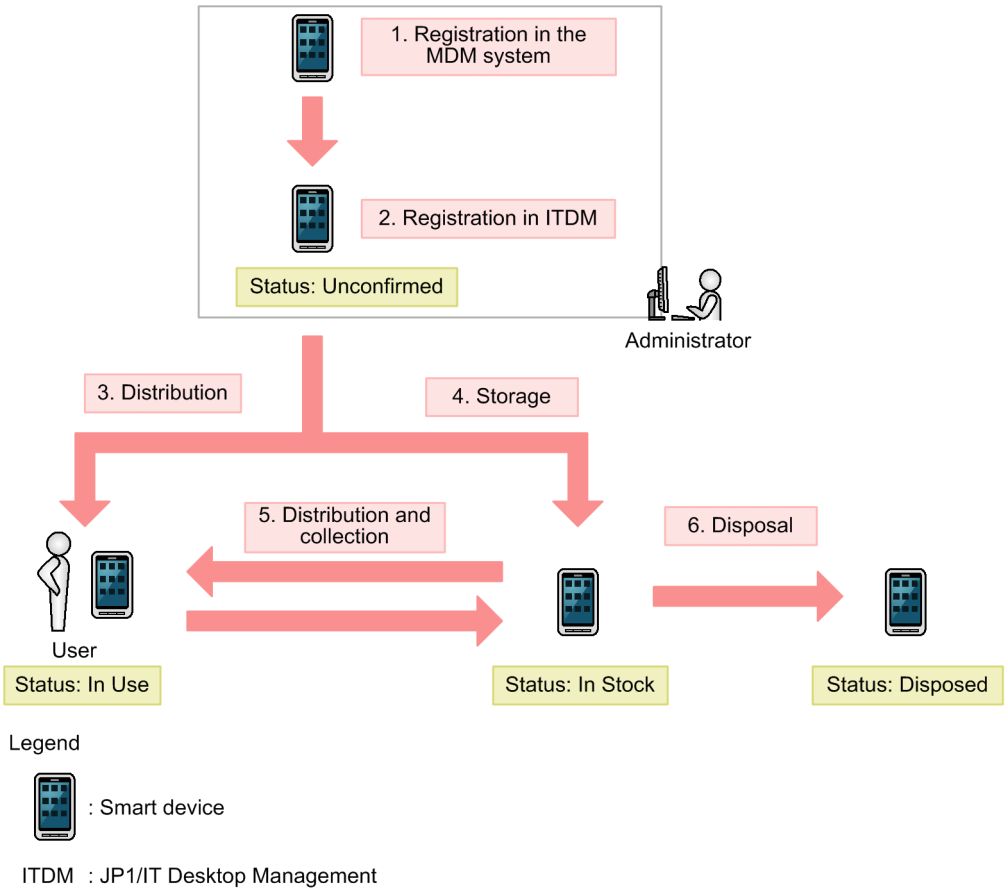
As smart devices become increasingly popular, many more companies are incorporating smart devices into their business operations. Although incorporation of smart devices into business operations is expected to improve business efficiency, such incorporation raises the risk of information leakage. To prevent information leakage or theft and loss of smart devices, you must manage smart devices in the same way as you manage other in-house assets.

By using the MDM linkage function provided by JP1/IT Desktop Management, you can efficiently manage smart devices as follows:

- Using JP1/IT Desktop Management, you can manage all smart devices in the same way as you manage computers, servers, printers, network devices, and USB devices used in your organization.
- When you include smart devices as the management targets of JP1/IT Desktop Management, you can manage the device information, asset information, and security of the smart devices.
- Using JP1/IT Desktop Management, you can lock and initialize smart devices, as well as reset their passcodes.

You can manage smart devices by using the Device module, the Assets module, and the Settings module. To manage smart devices, specify the settings to acquire smart device information from an MDM system, and then include the smart devices as the management targets of JP1/IT Desktop Management.

The following figure shows you how to manage smart devices:



After registering smart devices in an MDM system, include them as the management targets of JP1/IT Desktop Management, and then distribute them to users. Keep unused smart devices in stock and store them in a proper location. As necessary, collect the smart devices that are currently in use for replacement, or lend in-stock smart devices to new users. Discard and dispose of any unwanted smart devices.

This section explains how to use JP1/IT Desktop Management to perform the following tasks:

Start the management of smart devices.

Before starting to use the purchased smart devices, include them as the management targets of JP1/IT Desktop Management, and then distribute them to users.

Replace smart devices.

If you need to replace the smart devices used in your organization due to relocation of employees or renewal of smart devices, use JP1/IT Desktop Management to identify the smart devices to be replaced. Then, distribute new smart devices to, and collect the old ones from, the users.

Change the user of a smart device.

If a smart device is to be transferred to a new user due to relocation of the previous user, change the user of a smart device.

Implement measures to secure smart devices when they become lost.

You can configure smart devices to be locked or initialized for security protection when they become lost.

Take measures to deal with a situation in which a user forgets the passcode of that user's smart device.

Reset the passcode of the smart device. If the smart device is initialized after consecutive failed passcode attempts, register the smart device in an MDM system again, and then include it as the management target of JP1/IT Desktop Management.

Discard smart devices.

If smart devices collected for replacement or repair are too old or damaged to be reused, discard them.

1.4.1 General procedure for starting the management of smart devices

Before starting to use the purchased smart devices, include them as the management targets of JP1/IT Desktop Management, and then distribute them to users.

To start the management of smart devices:

1. Install an MDM system.

   To start the management of smart devices by using JP1/IT Desktop Management, install an MDM system, and then register the smart devices in the MDM system.

2. Include smart devices as management targets.

   By including smart devices as the management targets of JP1/IT Desktop Management, you can manage smart devices in the same way as you manage other devices and assets in your organization.

   To include smart devices as management targets, specify the MDM linkage settings, and then acquire smart device information from the MDM system.

3. Distribute smart devices to users.

   After including smart devices as the management targets of JP1/IT Desktop Management, determine users to which you distribute the smart devices by applications of smart device usage. First create a list of smart devices and the corresponding users, and then distribute the smart device to each user according to the list.

Start managing smart devices by using JP1/IT Desktop Management in the same way as you manage other devices and hardware assets.

(1) General procedure for installing an MDM system

To start the management of smart devices by using JP1/IT Desktop Management, install an MDM system, and then register the smart devices in the MDM system.

1. Purchase an MDM product.

   After purchasing smart devices, purchase an MDM product.

2. Build an MDM server.

   Install the purchased MDM product on a server within your organization.

3. Register smart devices in the MDM product.

   Install an agent program for the MDM product on each smart device, and then register the smart devices in the MDM product. In addition, apply the MDM product policy to the smart devices.

   Tip

   Using JP1/IT Desktop Management, you can manage the smart devices registered in an MDM product. Make sure that you register all the smart devices to be managed in the MDM product.

The installation of an MDM product is complete.

(2) General procedure for including smart devices as management targets

By including smart devices as the management targets of JP1/IT Desktop Management, you can manage smart devices in the same way as you manage other devices and assets in your organization.

To include smart devices as management targets, specify the MDM linkage settings, and then acquire smart device information from the MDM system.

1. In JP1/IT Desktop Management, specify the MDM linkage settings.

   If you are using the MDM linkage function for the first time, access the **MDM Linkage Settings** view of the Settings module, and then specify the setting to acquire smart device information from the MDM system. If the MDM linkage settings are already specified, skip this step.

2. Include smart devices as the management targets of JP1/IT Desktop Management.

   In the **MDM Linkage Settings** view of the Settings module, from **Action** select **Collect Device Info. from MDM Systems**. Device information is acquired from the MDM system, and the discovered smart devices are automatically included as the management targets of JP1/IT Desktop Management.

   If **Not Defined** is displayed under **Discovery Option:** in the **MDM Linkage Settings** view of the Settings module, access the **Discovered Nodes** view of the Settings module to manually include the discovered devices as management targets.

3. Confirm that the smart devices have been included as management targets.

   Confirm that the smart devices included as management targets are displayed in the **Device List** view of the Device module. By using filtering conditions such as **Device Type** (**Smart Device**) and **Registered Date/Time**, you can find the smart devices of interest more quickly.

4. Edit hardware asset information.

   In the hardware asset information for smart devices, **Unconfirmed** is displayed under **Asset Status**. In addition, only the information collected from the MDM system is registered as the hardware asset information. You need to therefore manually register information items that are not automatically collected, such as **User Name**, **Department**, **Asset #**, and **Asset Status**.

If necessary, register information items related to purchase contracts and communication contracts, and then associate them with hardware asset information.

The preparations for managing smart devices by using JP1/IT Desktop Management are complete. After registering necessary information, distribute smart devices to users. If there are any smart devices to be held in stock, store them in the specified location.

Related Topics:

- 1.9.2 Maintaining hardware asset information

(3) General procedure for distributing smart devices to users

By applications of smart device usage, determine users to which you distribute the smart devices managed by JP1/IT Desktop Management. First create a list of smart devices and the corresponding users, and then distribute the smart device to each user according to the list.

1. Accept an application for using a smart device submitted by each user.

   Ask users submitting an application for using a smart device to provide user information that is necessary to manage smart devices. Collect the following information from users:

   - Department
   - Location to which to distribute the device
   - User name
   - Email address
   - Phone number

2. Identify the available smart devices.

   In the **Hardware Asset** view of the Assets module, identify smart devices whose **Asset Status** is **In Stock**. Use the filtering function to facilitate this processing.

3. Change user information.

   In the **Hardware Asset** view of the Assets module, click the **Change Status** button to change the user information of smart devices. In addition, change the status of the smart devices under **Asset Status** to **In Use**.

4. Create a list of smart devices to be distributed.

   Before distributing smart devices to users, create a list of smart devices to be distributed. Export the hardware asset information of smart devices to be distributed to a CSV file. Make sure that you export all the hardware asset information items that you need to distribute smart devices to users. For example, export **Asset #** that identifies each smart device to be distributed, **Department** and **Location** that identify the locations to which to distribute smart devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently distribute smart devices to users. To sort the hardware asset information items, click an item name in the operation view.

5. Distribute smart devices to users.

   Using an exported list of smart devices, distribute smart devices to appropriate users. If you are asking delivery companies to deliver smart devices to users, give them the list and ask them to use the list when they deliver the smart devices. By having users put their signatures on the list when they receive a smart device, you can confirm later that the smart devices have been delivered to all destinations.

After distributing smart devices to users, start managing them by using JP1/IT Desktop Management. When new tasks arise, update the hardware asset information as necessary to keep it up to date.

Related Topics:

- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information
- 11.1.6 Changing the asset status

1.4.2 General procedure for replacing smart devices

If you need to replace the smart devices used in your organization due to relocation of employees or renewal of smart devices, use JP1/IT Desktop Management to identify the smart devices to be replaced. Then, distribute new smart devices to, and collect the old ones from, the users.

To replace smart devices:

1. Plan the replacement of smart devices.

   Use JP1/IT Desktop Management to identify the smart devices that need to be replaced. After determining the smart devices to be collected for replacement, prepare replacement smart devices.

2. Distribute new smart devices to users.

   Using JP1/IT Desktop Management, output information about the locations to which to distribute new smart devices. Use the output information to distribute a new smart device to each applicable user.

   After distributing new smart devices to users, instruct users to transfer the data stored in an old smart device to a new one.

3. Collect old smart devices from users.

   When users have transferred the data stored in an old smart device to a new one, ask users to return the old smart devices.

   Using JP1/IT Desktop Management, output information about the locations from which to collect old smart devices. Use the output information to collect an old smart device from each applicable user.

The replacement of smart devices is complete.

(1) General procedure for planning the replacement of smart devices

If you need to replace the devices used in your organization due to relocation of employees or renewal of devices, identify the devices that need to be replaced, determine the devices to be replaced, and then prepare replacement devices. In addition, notify the users in advance about the replacement.

1. Determine the devices to be replaced.

   In the **Hardware Asset** view of the Assets module, identify if there are any devices that need to be replaced. For example, if there is a policy to replace any devices that have been used for three years or more, use the filtering function to identify devices whose **Registered Date/Time** is over three years ago.

   Tip

   By saving frequently used filtering conditions, you can save the effort of specifying the filtering condition every time you have to identify devices that need to be replaced. To apply the saved filtering condition to a list, select a filtering condition in the menu area.

If you find devices that need to be replaced, access the **Hardware Asset** view of the Assets module, set **Planned Asset Status** to **In Stock**, and then enter the date of collection under **Planned Date**. In this way, you can identify devices that are due to be collected.

2. Prepare replacement devices.

   Prepare replacement devices to be distributed to users.

   - To distribute in-stock devices to users:

     In the **Hardware Asset** view of the Assets module, identify devices whose **Asset Status** is **In Stock**. To limit the information to be displayed in the view, use the filtering function. Check the specifications of the identified devices. If you do not find any problems in the specifications, set **Planned Asset Status** to **In Use** and enter the date of distribution under **Planned Date**. In this way, you can identify devices that are due to be distributed.

   - To distribute newly purchased devices to users:

     After purchasing new devices, include them as the management targets of JP1/IT Desktop Management, and then register both the hardware asset information and contract information for each device. Set **Planned Asset Status** to **In Use** and enter the date of distribution under **Planned Date**. In this way, you can identify devices that are due to be distributed.

3. Notify each user about the replacement.

   To facilitate the replacement processing, inform applicable users about the reason why their devices need to be replaced and the date on which the devices are to be replaced.

Preparation for replacement of devices is complete.

Related Topics:

- 11.1.7 Changing the planned asset status
- 1.9.3 General procedure for purchasing devices

(2) General procedure for distributing new smart devices to users

After preparing for replacement, create a list of new smart devices to be distributed to users. Using the created list, distribute the new smart devices to users. After distributing the new smart devices to users, update the hardware asset information.

1. Create a list of smart devices to be distributed.

   Before distributing smart devices to users, create a list of smart devices to be distributed. Export the hardware asset information of smart devices to be distributed to a CSV file. Make sure that you export all the hardware asset information items that you need to distribute smart devices to users. For example, export **Asset #** that identifies each smart device to be distributed, **Department** and **Location** that identify the locations to which to distribute smart devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently distribute smart devices to users. To sort the hardware asset information items, click an item name in the operation view.

2. Distribute smart devices to users.

   Using an exported list of smart devices, distribute smart devices to appropriate users. If you are asking delivery companies to deliver smart devices to users, give them the list and ask them to use the list when they deliver the smart devices. By having users put their signatures on the list when they receive a smart device, you can confirm later that the smart devices have been delivered to all destinations.

3. Update the hardware asset information.

After distributing the new smart devices to users, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change the **Asset Status** of each distributed smart device from **In Stock** to **In Use**. In addition, update **Department**, **Location**, and user information.

After distributing new smart devices to users, instruct users to transfer the data stored in an old smart device to a new one.

Related Topics:

- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information
- 11.1.6 Changing the asset status

(3) General procedure for collecting the smart devices that are no longer in use

If you want to put the smart devices that are no longer in use back in stock, collect them when the planned date of collection arrives. Before collecting the smart devices from users, create a list of smart devices to be collected. Using the created list, collect the smart devices from users. After collecting the smart devices from users, update the hardware asset information.

Tip

In **Hardware Asset Status (Planned)** on the Summary Reports, you can check the number of smart devices that are due to be collected from users (smart devices whose **Planned Asset Status** is **In Stock**). You can also send a summary report by email.

Tip

To facilitate the collection processing, we recommend that you notify the users of smart devices to be collected in advance about the reason for collecting the device and the planned date of collection.

1. Create a list of smart devices to be collected.

Before collecting smart devices from users, create a list of smart devices to be collected. Export the hardware asset information whose **Planned Asset Status** is **In Stock** to a CSV file. Make sure that you export all the hardware asset information items that you need to collect the smart devices from users. For example, export **Asset #** that identifies each smart device to be collected, **Department** and **Location** that identify the locations from which to collect smart devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

Tip

When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently collect smart devices from users. To sort the hardware asset information items, click an item name in the operation view.

2. Collect the smart devices from users.

Use the exported list to collect the smart devices from users. If you are asking delivery companies to collect smart devices from users, give them the list and ask them to use the list when they collect the smart devices from users.

After collecting all the smart devices from users, check the collected smart devices against the information in the exported list to confirm that all the devices have been collected from users.

3. Update the hardware asset information.

After collecting smart devices from users, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change the **Asset Status** of each collected smart device from **In Use** to **In Stock**. In addition, specify the location where the collected smart devices are stored in **Location**, and change **Department** and user information for the collected smart devices so that a system administrator is now in charge of these smart devices.

The collected smart devices are managed as in-stock devices.

Related Topics:

- 15.7.2 Setting recipients of summary reports
- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information
- 11.1.6 Changing the asset status

1.4.3 General procedure for changing the user of a smart device

If a smart device is to be transferred to a new user due to relocation of the previous user to another department, change the user of the smart device.

To change the user of the smart device, first initialize the smart device, and then re-register it in the MDM system.

To change the user of the smart device:

1. Collect the smart device from the user.

Collect the smart device from the user who is no longer using it.

2. Prepare for redistribution of the smart device to a new user.

Initialize the collected smart device, and then re-register it in the MDM system.

3. Distribute the smart device to a new user.

Distribute the smart device to a new user who has submitted an application for using a smart device.

The user of the smart device has been changed.

(1) General procedure for collecting the smart devices that are no longer in use

If you want to put the smart devices that are no longer in use back in stock, collect them when the planned date of collection arrives. Before collecting the smart devices from users, create a list of smart devices to be collected. Using the created list, collect the smart devices from users. After collecting the smart devices from users, update the hardware asset information.

Tip

In **Hardware Asset Status (Planned)** on the Summary Reports, you can check the number of smart devices that are due to be collected from users (smart devices whose **Planned Asset Status** is **In Stock**). You can also send a summary report by email.

Tip

To facilitate the collection processing, we recommend that you notify the users of smart devices to be collected in advance about the reason for collecting the device and the planned date of collection.

1. Create a list of smart devices to be collected.

   Before collecting smart devices from users, create a list of smart devices to be collected. Export the hardware asset information whose **Planned Asset Status** is **In Stock** to a CSV file. Make sure that you export all the hardware asset information items that you need to collect the smart devices from users. For example, export **Asset #** that identifies each smart device to be collected, **Department** and **Location** that identify the locations from which to collect smart devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently collect smart devices from users. To sort the hardware asset information items, click an item name in the operation view.

2. Collect the smart devices from users.

   Use the exported list to collect the smart devices from users. If you are asking delivery companies to collect smart devices from users, give them the list and ask them to use the list when they collect the smart devices from users.

   After collecting all the smart devices from users, check the collected smart devices against the information in the exported list to confirm that all the devices have been collected from users.

3. Update the hardware asset information.

   After collecting smart devices from users, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change the **Asset Status** of each collected smart device from **In Use** to **In Stock**. In addition, specify the location where the collected smart devices are stored in **Location**, and change **Department** and user information for the collected smart devices so that a system administrator is now in charge of these smart devices.

The collected smart devices are managed as in-stock devices.

Related Topics:

- 15.7.2 Setting recipients of summary reports
- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information
- 11.1.6 Changing the asset status

(2) General procedure for preparing for redistribution of the collected smart devices to new users

To lend the collected smart devices to new users, initialize the smart devices, and then re-register them in the MDM system.

1. Identify the collected smart devices.

   Based on the asset management numbers assigned to the collected smart devices, identify the collected smart devices in the **Hardware Asset** view of the Assets module. Use the filtering function to facilitate this processing.

2. Initialize the smart devices.

   In the **Hardware Asset** view, click the **Go to Device List** button to display the Device module. Then, from **Action**, select **Initialize Smart Device**.

   To retain the smart device information in JP1/IT Desktop Management, clear the **Delete initialized smart device information** check box in the displayed dialog box, and then initialize the smart devices.

   > **Tip**
   >
   > When the smart device is initialized, the agent program for the MDM system is also removed from the smart device.

3. Delete the smart device information from the MDM system.

   In the **MDM Linkage Settings** view of the Settings module, click the host name of the MDM server of the MDM system that is linked with JP1/IT Desktop Management, and then log in to the MDM system. In the MDM system, delete the applicable smart device information.

4. Re-register the initialized smart devices in the MDM system.

   Re-register the initialized smart devices in the MDM system. Install an agent program for the MDM system on each smart device, and then apply the MDM system policy to the smart devices.

   > **Tip**
   >
   > After you re-register the smart devices in the MDM system, the MDM system collects the smart device information. At this time, the device information is updated.

Preparations for redistribution of the collected smart devices to new users are complete.

Related Topics:

- 6.27 Resetting a smart device

(3) General procedure for distributing smart devices to users

By applications of smart device usage, determine users to which you distribute the smart devices managed by JP1/IT Desktop Management. First create a list of smart devices and the corresponding users, and then distribute the smart device to each user according to the list.

1. Accept an application for using a smart device submitted by each user.

   Ask users submitting an application for using a smart device to provide user information that is necessary to manage smart devices. Collect the following information from users:

   - Department
   - Location to which to distribute the device
   - User name
   - Email address
   - Phone number

2. Identify the available smart devices.

   In the **Hardware Asset** view of the Assets module, identify smart devices whose **Asset Status** is **In Stock**. Use the filtering function to facilitate this processing.

3. Change user information.

   In the **Hardware Asset** view of the Assets module, click the **Change Status** button to change the user information of smart devices. In addition, change the status of the smart devices under **Asset Status** to **In Use**.

4. Create a list of smart devices to be distributed.

   Before distributing smart devices to users, create a list of smart devices to be distributed. Export the hardware asset information of smart devices to be distributed to a CSV file. Make sure that you export all the hardware asset information items that you need to distribute smart devices to users. For example, export **Asset #** that identifies each smart device to be distributed, **Department** and **Location** that identify the locations to which to distribute smart devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently distribute smart devices to users. To sort the hardware asset information items, click an item name in the operation view.

5. Distribute smart devices to users.

   Using an exported list of smart devices, distribute smart devices to appropriate users. If you are asking delivery companies to deliver smart devices to users, give them the list and ask them to use the list when they deliver the smart devices. By having users put their signatures on the list when they receive a smart device, you can confirm later that the smart devices have been delivered to all destinations.

After distributing smart devices to users, start managing them by using JP1/IT Desktop Management. When new tasks arise, update the hardware asset information as necessary to keep it up to date.

Related Topics:

- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information
- 11.1.6 Changing the asset status

1.4.4 Implementing measures to secure smart devices when they become lost

When a smart device used in your organization becomes lost, it can lead to leakage of confidential information that is stored in the smart device, including customer data, sales data, and development data. An immediate action must therefore be taken when a smart device becomes lost.

You can use one of the following two types of measures to secure a smart device when it becomes lost:

Initialize a lost smart device.

If a smart device becomes lost and cannot be found within a specified period of time, initialize the smart device to prevent information leakage.

Lock a lost smart device.

If the specified interval of inactivity before the smart device becomes locked is too long (this specification is provided by the MDM system policy), lock the smart device to protect it from unauthorized access.

(1) General procedure for initializing a lost smart device

If a smart device becomes lost, initialize it to prevent information leakage.

To initialize a lost smart device:

1. Receive notification from a user that a smart device has become lost.

   Receive notification from a user that a smart device has become lost. To identify the smart device, ask the user for the user name and contract phone number.

2. Wait for the smart device to be found.

   Follow the security rules of your organization, and wait for the smart device to be found. If the smart device cannot be found within a specified period of time, decide to initialize the smart device to prevent information leakage.

3. Identify the smart device.

   Based on the information you have collected from the user, identify the lost smart device by using the **Device List** view of the Device module. Use the filtering function to facilitate this processing.

4. Initialize the identified smart device.

   In the **Device List** view of the Device module, from **Action**, select **Initialize Smart Device** to initialize the lost smart device.

   Tip

   When the smart device is initialized, the agent program for the MDM system is also removed from the smart device.

5. Delete the smart device information from the MDM system.

   In the **MDM Linkage Settings** view of the Settings module, click the host name of the MDM server of the MDM system that is linked with JP1/IT Desktop Management, and then log in to the MDM system. In the MDM system, delete the information of the lost smart device.

6. Edit the asset information of the smart device.

   In the Hardware **Asset view** of the Assets module, select the lost smart device, and then click the **Change Status** button. In the displayed dialog box, change **Asset Status** from **In Use** to **Disposed**.

   Also, enter comments in the **Notes** tab, describing the remarks such as reason or date and time of loss.

The initialization of the lost smart device is complete.

If necessary, cancel the communication contract of the lost smart device, and update the contract information accordingly.

Tip

Any problems that can potentially lead to information leakage must be disclosed to all employees, and make sure that all employees are fully aware of good security practices.

Related Topics:

- 6.27 Resetting a smart device

(2) General procedure for locking a lost smart device

The specified interval of inactivity before the smart device becomes locked can be too long (this specification is provided by the MDM system policy). In this case, lock a lost smart device from JP1/IT Desktop Management to prevent information leakage from the lost smart device.

To lock a lost smart device:

1. Receive notification from a user that a smart device has become lost.

   Receive notification from a user that a smart device has become lost. To identify the smart device, ask the user for the user name and contract phone number.

2. Identify the smart device.

   Based on the information you have collected from the user, identify the lost smart device by using the **Device List** view of the Device module. Use the filtering function to facilitate this processing.

3. Lock the identified smart device.

   In the **Device List** view of the Device module, from **Action**, select **Lock Smart Device**. In the displayed dialog box, click the **OK** button.

The lost smart device is locked.

If necessary, cancel the communication contract of the lost smart device, and update the contract information accordingly.

Tip

If the lost smart device is found, check for signs of unauthorized access to the smart device. If the smart device is not found within a specified period of time, we recommend that you initialize the smart device to prevent information leakage.

Related Topics:

- 6.25 Locking a smart device

1.4.5 Taking measures to deal with a situation in which a user forgets the passcode of the smart device

There are two types of measures you (administrator) can take to deal with a situation in which a user forgets the passcode of the smart device. Select the measure appropriate to the circumstance.

Reset the passcode of the smart device.

If a user forgets the passcode of the smart device, reset the passcode, and then instruct the user to set a new passcode for the smart device.

Re-register the initialized smart device.

If a user repeatedly enters an incorrect passcode in the smart device, the smart device might be initialized according to the MDM system policy. In order for the user to be able to use the initialized smart device, you need to re-register the smart device in the MDM system and JP1/IT Desktop Management.

(1) General procedure for resetting the passcode of a smart device

If a user forgets the passcode of the smart device, you (administrator) reset the passcode, and then instruct the user to set a new passcode for the smart device.

To reset the passcode of a smart device:

1. Receive notification from a user that the user has forgotten the passcode of the smart device.

   Receive notification from a user that the user has forgotten the passcode of the smart device. To identify the smart device, ask the user for the asset management number. In addition, ask for the contact information so that you can contact the user later.

2. Identify the smart device.

   Based on the asset management number, identify the smart device by using the **Hardware Asset** view of the Assets module. Use the filtering function to facilitate this processing.

3. Check the asset information of the identified smart device.

   Based on the user name and contact information registered in the asset information, confirm that the user who has forgotten the passcode is identical to the registered user of the smart device. Then, inform the user that the passcode of the smart device will be reset.

4. Reset the passcode of the identified smart device.

   In the **Device List** view of the Device module, from **Action**, select **Reset Smart Device Passcode** to reset the passcode of the smart device.

   Tip

   You can reset the passcode of one smart device at a time. If you want to reset the passcodes of multiple smart devices, perform the reset procedure for each one of these devices.

The passcode of the smart device has been reset.

Inform the user that the passcode of the smart device has been reset, and then instruct the user to set a new passcode.

Related Topics:

- 6.26 Resetting a smart device passcode

(2) General procedure for re-registering the initialized smart device

If a user repeatedly enters an incorrect passcode in the smart device, the smart device might be initialized according to the MDM system policy. In order for the user to be able to use the initialized smart device, you (administrator) need to re-register the smart device in the MDM product and JP1/IT Desktop Management.

To re-register the initialized smart device:

1. Receive notification from a user that the smart device has been initialized.

   Receive notification from a user that the smart device has been initialized. To identify the smart device, ask the user for the asset management number. In addition, collect the initialized smart device from the user so that you can re-register the said smart device in the MDM system and install an agent program for the MDM product on the said smart device.

2. Identify the smart device.

   Based on the asset management number, identify the smart device by using the **Hardware Asset** view of the Assets module. Use the filtering function to facilitate this processing.

3. If necessary, delete the initialized smart device information from the MDM system.

   In the **MDM Linkage Settings** view of the Settings module, click **Host name of MDM server** of the MDM system that is linked with JP1/IT Desktop Management, and then log in to the MDM system. If the initialized smart device information still remains in the MDM system, delete that information.

4. Re-register the initialized smart device in the MDM system.

   Re-register the initialized smart device in the MDM system. Install an agent program for the MDM product on the smart device, and then apply the MDM system policy to the smart device.

   Tip

   After you re-register the smart device in the MDM system, the MDM system collects the smart device information. At this time, the device information is updated.

5. Return the smart device to its user.

   Return the re-registered smart device to its user.

The re-registration of the initialized smart device is complete.

Related Topics:

- (3) General procedure for collecting the smart devices that are no longer in use

1.4.6 General procedure for discarding smart devices

If smart devices collected for replacement or repair are too old or damaged to be reused, discard them.

To discard smart devices:

1. Determine the devices to be discarded.

   If the collected smart devices are no longer to be used, set them as the devices to be discarded. To prevent information leakage, initialize the smart devices to be discarded.

2. Dispose of the devices.

   When the planned date of disposal arrives, dispose of the applicable devices.

The disposal of faulty smart devices is complete.

(1) General procedure for determining the devices to be discarded

If devices collected for replacement or repair are too old or damaged to be reused, set them as the devices to be discarded. If the collected devices are still usable, keep them in stock.

1. Identify the devices that are no longer to be used.

   Check the collected devices for any devices that are no longer to be used.

   For example, if there is a policy to discard any devices that have been used for five years or more, check how long the collected devices have been used. To do this, access the **Hardware Asset** view of the Assets module, and then check **Registered Date/Time** or **Contract Date** of the collected devices. To limit the information to be displayed in the view, use the filtering function.

   If neither **Registered Date/Time** nor **Contract Date** is displayed in the view, right-click an item name in the list, and then select **Select Columns**. In the displayed dialog box, select the **Registered Date/Time** or **Contract Date** check box, and then click the **OK** button. **Registered Date/Time** or **Contract Date** is then displayed in the view. If no contract information is registered for hardware assets, **-** is displayed under **Contract Date**.

2. Set as the devices to be discarded.

   If there are devices that are no longer to be used, set **Planned Asset Status** to **Disposed**, and then enter the planned date of disposal under **Planned Date**. In this way, you can identify devices that are due to be discarded.

3. Clear all data stored in the hard disk.

   To prevent information leakage, erase all data stored in the hard disks of the devices to be discarded by using a tool specifically designed for this purpose.

   If you are discarding the smart devices, initialize them. To initialize the smart devices, click the **Go to Device List** button in the **Hardware Asset** view to display the Device module, and then from **Action**, select **Initialize Smart Device**.

   If you are keeping the smart devices in stock, make a disk copy of them so that they can be put to use without delay when necessary.

The devices to be discarded are ready for disposal at any time.

Related Topics:

- 11.1.7 Changing the planned asset status
- 1.11 General procedure for managing asset contract information

(2) General procedure for disposing of devices

When the planned date of disposal arrives, dispose of all devices that are no longer to be used. Before disposing of the devices, create a list of devices to be disposed of. Using the created list, dispose of the devices. After disposing of the devices, update the hardware asset information.

1. Create a list of devices to be disposed of.

   Before disposing of the devices, create a list of the devices to be disposed of. Export the hardware asset information whose **Planned Asset Status** is **Disposed** to a CSV file. Make sure that you export all the hardware asset information items that you need to dispose of the devices. For example, export an item such as **Asset #**, which identifies each device to be disposed of.

2. Dispose of the devices.

   Use the exported list to dispose of the devices. If you are asking a waste disposal contractor to dispose of the devices, give the contractor the list and ask the contractor to use the list to dispose of the devices.

3. Update the hardware asset information.

   After disposing of the devices, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change **Asset Status** of each device that has been disposed of from **In Stock** to **Disposed**.

   Tip

   If you change **Asset Status** of hardware assets to **Disposed**, the corresponding device information is deleted.

   Tip

   If you change **Asset Status** of hardware assets to **Disposed** when the network monitor is enabled, the corresponding device information is removed from the network control list. If, however, agents are installed on the corresponding devices and these devices are connected to the network, the devices are automatically included as management targets and re-registered in the network control list.

The disposal of devices is complete. The hardware asset information of the devices that have been disposed of is retained, with their **Asset Status** set to **Disposed**.

Cancel the contracts relevant to the discarded devices as necessary.

Related Topics:

- 11.5 Exporting asset information
- 11.1.6 Changing the asset status

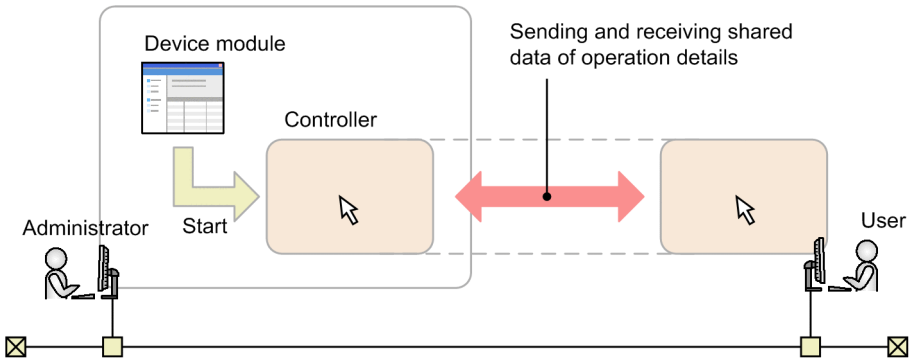
1.5 Remote controlling devices

Administrators are responsible for handling failures that occur in users' computers and taking care of inquiries from users in the entire organization. Assisting every one of users by visiting them at their desks to investigate and resolve the problems is an extremely time-consuming task. In addition, if the servers of the organization are located in a distant place, administrators would have to travel to the server room carrying necessary data with them every time they need to work with the servers.

By using the remote control function, administrators can efficiently cope with failures of devices and operate servers located at a remote site. The remote control function allows administrators to:

- Remote control computers and servers located at a remote site.
- Send and receive data by using the file transfer function without the need for special software or settings.
- Record operations performed on devices or simultaneously chat with multiple connected devices.

An administrator can remote control devices by starting a controller on the computer from the Device module. After the administrator starts a controller on the computer once, the administrator can start the controller on the same computer without logging in to JP1/IT Desktop Management. The following figure shows how an administrator can remote control a device:



From the Device module, an administrator selects the computer to which the administrator wants to connect, and then establishes a connection to that computer. When the connection is established, remote control is started. During the remote control, the administrator and the user can share views. In addition, the administrator can use convenient functions, such as the file transfer function and the recording function.

This section explains how administrators use JP1/IT Desktop Management to perform the following tasks:

Connect to computers and take care of inquiries.

If a failure occurs in a user's computer and an administrator receives a request to fix the problem, the administrator remote controls the user's computer from the administrator's computer to investigate the cause and resolve the problem.

Operate a server located at a remote site.

An administrator remote controls and operates a server located at a remote site (different floor or location).

Give instructions to a user located at a remote site.

Using the remote control function, an administrator gives instructions to a user located at a remote site while monitoring the operations performed by the user.

Related Topics:

- 1.5.1 General procedure for remote controlling computers to respond to inquiries

- 1.5.2 General procedure for operating a server located at a remote site
- 1.5.3 General procedure for giving instructions to users located at a remote site

1.5.1 General procedure for remote controlling computers to respond to inquiries

If you (administrator) receive an inquiry from a user about a problem, such as a failure on the user's computer, you can remote controls the user's computer from your computer to investigate the cause and resolve the problem.

To remote control a computer and take care of an inquiry:

1. Identify the computer to which to connect to.

   When you receive a request from a user to fix a problem, ask the user to provide information necessary to identify the computer, including the user's name and asset management number. Using the provided information, identify the computer to be remote controlled.

2. Connect to the computer.

   Notify the user that you are connecting to the user's computer, and then establish a connection to the computer. When the user permits connection from your computer, you can remote control the user's computer from your computer.

3. Investigate and resolve the problem in the user's computer.

   Remotely operate on the user's computer to investigate a log on the user's computer, and then identify and resolve the problem. When the problem is resolved, end the remote control session.

An inquiry from a user is taken care of.

(1) General procedure for identifying a computer to be remote controlled

When connecting to a computer, you need to obtain user information to identify the target computer. By using the obtained user information, identify the computer to which to connect.

1. Obtain user information.

   Obtain user information to identify the computer to which to connect. For example, you can obtain this information from a user when the user contacts you asking for your assistance in solving a problem. Obtain the following information from the user:

   - Asset management number
   - User name
   - Department
   - Location of the computer
   - Phone number

2. Identify the computer.

   Based on the obtained user information, identify the target computer by using the **Device Inventory** view of the Device module. Use the filtering function to facilitate this processing.

Preparations for connection to a computer are complete.

(2) General procedure for connecting to a computer to be remote controlled

Connect to a computer. To establish a connection to a computer:

1. Inform the user that you are going to connect to the user's computer.

   Before establishing a connection to a computer, make a phone call to the user to inform the user of the following two points:

   - You are going to connect to the user's computer.
   - The user is expected to allow connection to the user's computer when a confirmation dialog box appears.

2. Connect to the computer.

   In the **Device Inventory** view of the Device module, select the computer, and then connect to it. If the authentication view appears, you need to enter your user ID and password.

   Depending on the agent configuration on the user's computer, a confirmation dialog box might appear on the user's computer to ask the user if the user allows connection to the user's computer. In order for you to start remote control, the user must allow you to connect to the user's computer. This dialog box serves as a reminder to the user that remote control is being started.

   Tip

   To connect to a user's computer, you need to have a controller installed on your computer. If no controller is installed on your computer, you can install a controller while establishing a connection to a user's computer from an operation view. If the controller is already installed, you can also establish a connection to a user's computer by directly starting the controller from the **Start** menu.

   Tip

   You can also connect to an agentless computer running the operating system, such as Linux or Mac OS.

Connect to the user's computer, and then start remote control.

Set a connection mode in advance when remote controlling a computer. For example, if you want to fix a problem in a user's computer, connect to the user's computer in Exclusive mode to prevent the user from performing any operations on the user's computer. On the other hand, if you want to monitor the operations performed by a user while providing instructions to the user, connect to the user's computer in View mode to allow the user to perform operations on the user's computer. Select a connection mode that is appropriate to your purpose.

Tip

You can start multiple controllers. This means that you can set up multiple computer screens side by side to make comparisons or to monitor them all at once.

Tip

If you are connecting to a computer with a slow communication speed, you can speed up remote control sessions by decreasing data traffic. You can specify a setting to speed up remote control sessions in the **Options** dialog box of a controller.

Tip

In an environment where your computer cannot access a user's computer (for example, in a NAT environment), you can have the user's computer make a request for establishing a connection to your computer.

Tip

If a connection destination computer supports AMT or Wake on LAN, even when the computer is turned off, the computer can be automatically turned on so that remote control can be started.

Related Topics:

- 7.1 Installing the controller
- 15.3.1 Managing agent configurations

(3) Investigating a problem in a computer by remote control

You can investigate and resolve a problem in a user's computer by remote control. While remote controlling a computer, you can perform the following operations:

- Send and receive files.

  You can send and receive files to and from the computer you are remote controlling. This operation is useful when you need to collect and analyze a log file, or when you have to transfer necessary data to the connection destination computer.
- Automatically reestablish connection to the connection destination computer after restarting that computer.

  After restarting the connection destination computer, you can automatically reestablish connection to that computer. This operation is useful when you need to restart the connection destination computer during maintenance or other similar tasks.
- Chat with users.

  By using the chat function, you can chat on screen with multiple users. In addition, you can keep logs of the chat content by saving or printing it. This operation is useful when you have to communicate with users in an environment where phone calls cannot be made, or when you have to provide instructions to multiple users.
- Save operations in a video file.

  You can record the operations performed while remote controlling a user's computer, and then save them in a video file. This operation is useful when you want to save the effort of explaining the same problem-solving procedure to other users.

When you have finished investigating and resolving the problem, end the remote control session and notify the result to the user.

Related Topics:

- 7.5.13 Rebooting a remotely controlled computer

1.5.2 General procedure for operating a server located at a remote site

You (administrator) can operate a server located at a remote site (different floor or location) by remote controlling the server from your computer. This saves you the effort of visiting or travelling to the location where the server is installed every time you need to work on the server or perform a data maintenance task.

This subsection shows an example of how you can operate a server located at a remote site. In this example, you reconfigure the operation system environment settings of the server by remote control.

1. Connect to the server.

   Connect to the server installed in the remote site from your computer.

2. Reconfigure the server.

   Transfer the environment settings files of the server to your computer, and then make changes to the configuration.

   Then transfer the reconfigured environment settings files to a test server to check the operation. If the environment settings files work correctly, then transfer and apply them to the actual server.

   Even in an environment where a file cannot be edited on the server, this procedure saves you the effort of carrying data back and forth between the server and your computer.

The environment settings of the server are reconfigured by remote control.

(1) General procedure for connecting to a server located at a remote site

To make changes to the environment settings files of the server, you need to first connect to the server and then transfer the environment settings files to your computer.

If you frequently connect to the server to perform routine operations, you can register the server in a connection list so that you can directly connect to the server from a controller. In this way, you do not have to search for the server in an operation view and then establish connection to the server each time.

To connect to the server:

1. Start the controller.

   Start the controller directly from the **Start** menu.

   Tip

   To connect to a computer, you need to have a controller installed on your computer. If no controller is installed on your computer, you can install a controller while establishing a connection to a computer from an operation view.

2. Register the connection destination server in a connection list.

   Display a connection list from the controller, and then register the connection destination server in the connection list.

3. Connect to the server.

   Select the connection destination server from the connection list. If an authentication view appears, enter authentication information. When authentication is successful, you can connect to the server.

   Tip

   To specify whether to display an authentication view, use the agent configuration. By default, an authentication view is displayed. We recommend that you configure the authentication view to be displayed

when an attempt is made to connect to a server to prevent users other than administrators from connecting to a server. Whether an authentication view is displayed when an attempt is made to connect to an agentless computer depends on the remote control function configured in the connection destination computer.

A connection to the server is established, and remote control is started.

Related Topics:

- 7.1 Installing the controller

(2) General procedure for reconfiguring the environment settings of a server located at a remote site

After connecting to the server, reconfigure the environment settings of the server.

You can also edit the environment settings files directly on the server. If this is not possible, or if you can edit the environment settings files more efficiently by using a tool available on your computer, first transfer the files located on the server to your computer. After editing the environment settings files, transfer them back to the server and apply them to the server.

Tip

For example, if environment settings consist of complex CSV files and software that can be used for efficient CSV file editing is installed on your computer, editing the environment settings files on your computer is more convenient.

To reconfigure the environment settings of a server by remote control:

1. Transfer the environment settings files to your computer.

   Transfer the environment settings files located on the server to your computer to edit the environment settings files on your computer.

2. Edit the environment settings files.

   Edit the environment settings files on your computer.

3. Transfer the environment settings files to a test server.

   After editing the environment settings files on your computer, transfer them to a test server.

4. Transfer the environment settings files to the actual server.

   If an operation test performed on the test server reveals no problem, transfer the environment settings files to the actual sever and apply them to the server.

The environment settings of the server are updated. You can reconfigure the environment settings of the server without travelling to the server room.

1.5.3 General procedure for giving instructions to users located at a remote site

You (administrator) sometimes have to give instructions to a user located at a remote site. If you use a phone call to give instructions to a user, it is difficult to tell if the user is following your instructions correctly. Visiting a user to give

instructions is extremely troublesome, because it takes time to travel to the user's location and also because you need to carry the data necessary for tasks with you.

By using the remote control function, you can correctly execute tasks by giving instructions to a user by phone call while monitoring the user's operations on screen. In addition, you also can reduce the time to travel to the user's location and avoid the risk of information leakage caused by carrying data with you.

To give instructions to a user located at a remote site:

1. Connect to the user's computer.

   After giving prior notice to the user, connect to the user's computer in View mode. By establishing a connection to the user's computer in View mode, you can monitor if the user is performing operations as instructed. In this mode of remote control, the user can perform operations on the user's computer but you cannot perform operations on the user's computer.

2. Give instructions to the user.

   Give instructions to the user by a phone call while monitoring the operations performed by the user. If the user's computer does not have the data necessary to perform the instructed operations, transfer the necessary data from your computer to the user's computer.

(1) Giving instructions to users

To give instructions to the user located at a remote site, you have to connect to the user's computer by using the remote control function. You can then give instructions to the user by a phone call while monitoring the user's operations in a controller view.

If the user's computer does not have the data necessary to perform the instructed operations, you can use the file transfer function to transfer data from your computer to the user's computer. You can transfer data in Shared or Exclusive mode of remote control. The file transfer function is not available in View mode.

Tip

In cases where a user becomes unable to perform the instructed operations, you can take over the user's operation by changing the remote control mode to Shared mode or Exclusive mode.

Related Topics:

- 7.5.10 Changing the connection mode

1.6 Controlling network access of devices

Virus infection or information leakage could occur when a network within an organization is accessed by privately-owned computers or computers that do not have adequate security protection. Administrators who are responsible for managing devices used within their organization must control network access of devices to prevent unauthorized network access and to immediately disable network access for devices that do not have adequate security protection.

With JP1/IT Desktop Management, you can use the following functions to control network access of devices:

- Specify devices to be denied network access (blacklist method).
  If new devices are allowed access to the network, you can use this function to disable network access for only the devices that have security flaws. This function allows you to control network access of computers by disabling network access for the specified computers.
- Specify devices to be allowed network access (whitelist method).
  Use this function if you want to deny network access from privately-owned computers in your organization. Because you can disable network access for devices other than the specified devices, you can maintain security more effectively.
- Disable network access for devices or allow network access to devices at any given time.
  While applying the blacklist or whitelist method, use this function to disable network access for only the devices that are found to have security flaws.

Important note

Before using the network monitoring function, make sure that you are fully aware of the devices that are allowed network access and those that are denied network access. 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.

Important note

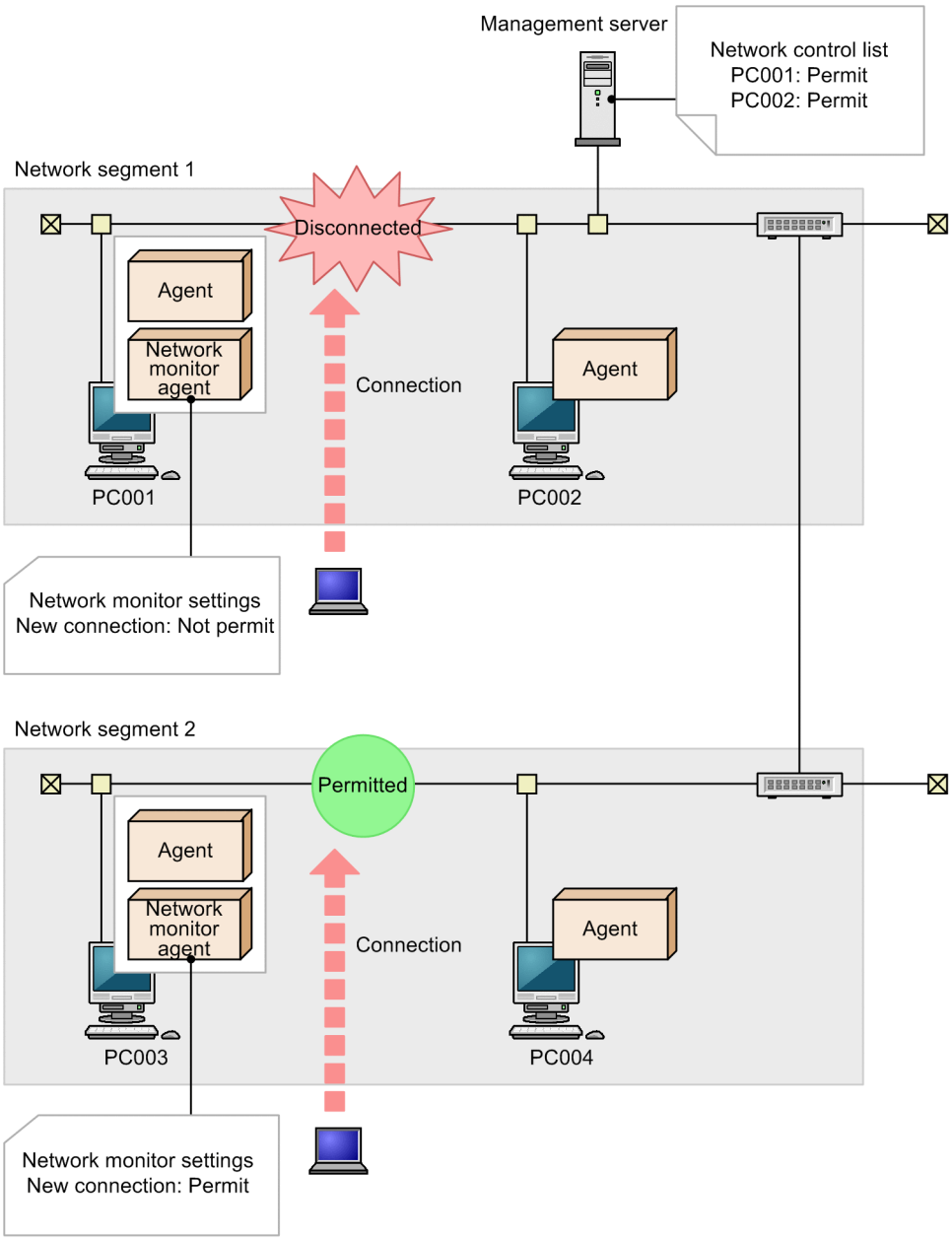
If you are implementing network access control by using the whitelist method, remember to register the devices that are not managed by JP1/IT Desktop Management (such as routers, switches, and network printers) as the devices that are allowed network access. In particular, if network devices, such as routers and switches, are not allowed network access, any subordinate devices that are connected to these network devices cannot access the network.

Important note

We recommend that you manually register, in a network control list, the IP addresses of devices that are important for business operations, including routers, printers, and servers. In this way, you can prevent these devices' network access from being disabled due to automatic updating of the network control list. If you enter a MAC address in a network control list, the entered MAC address might be deleted from the list when device information is updated. For this reason, leave the **MAC Address** field blank.

Control network access of devices by using the Device module and the Settings module.

The following figure shows a concept of how to control network access of devices:



To control network access of devices, you have to deploy agents to devices, with the network monitor enabled for each network segment. In this way, network access is controlled according to the network monitor settings assigned by the management server. In addition, by using a network control list, you can specify whether to allow or deny network access for each device.

For example, if you want to deny network access from privately-owned computers, first register the devices within your organization that are allowed network access in the network control list. Then, edit the network monitor settings to deny network access from new devices. In this way, you can maintain security of systems within your organization by automatically disabling network access for privately-owned computers.

Note that you cannot disable network access for management servers, database servers, site servers, or the computers on which network monitor agents are installed.

This section explains how to use JP1/IT Desktop Management to perform the operations described below. See the description of the operation that suits your purpose.

Deny network access from privately-owned computers.

You allow only the specified computers to access the network.

Disable network access for devices that have been infected with viruses.

You can disable network access for virus-infected devices. After taking proper anti-virus measures, you can enable network access for these devices.

Automatically control network access for devices in violation of a security policy.

Network access is automatically disabled or enabled according to the status of computers determined based on a security policy.

Temporarily allow network access for specified devices.

When network access for new devices is denied, you can allow only the specified computers to temporarily access the network.

Related Topics:

- 1.6.1 General procedure for denying network access for privately-owned personal computers
- 1.6.2 General procedure for disabling network access for devices that have been infected with viruses
- 1.6.3 General procedure for automatically controlling network access of devices in violation of a security policy
- 1.6.4 General procedure for temporarily allowing network access for specified devices

1.6.1 General procedure for denying network access for privately-owned personal computers

When a network within an organization can be freely accessed by privately-owned computers, computers accessing the network can cause virus infection or information leakage. To prevent privately-owned computers from accessing the network in your organization, register devices that are allowed network access in a network control list so that only the registered devices can access the network.

By preventing devices not registered in the network control list from accessing the network, you can avoid the risk of security problems caused by privately-owned computers accessing the network.

To deny network access for privately-owned computers:

1. Register devices in a network control list.

   Register devices that are allowed network access in a network control list.

2. Deny network access for unregistered devices.

   Specify a setting to prevent devices not registered in the network control list from accessing the network.

3. Check devices accessing the network.

   Check new devices accessing the network.

(1) Registering devices in a network control list

Register devices accessing the network within your organization in a network control list. You can view the network control list in the **Network Filter Settings** view of the Settings module. Make sure that you register all devices in your organization that are allowed network access in the network control list.

Important note

Network access control is also applied to network devices such as routers and switches. If network access is disabled for network devices, other devices cannot access the network. For this reason, make sure that all the network devices within the range of network access control are registered in the network control list.

Tip

In the **Network Filter Settings** view of the Settings module, you can specify whether to allow network access for each device. By default, network access is allowed for devices displayed in the Network Filter Settings view.

Tip

If you enable the network monitor, you can discover devices that are turned on without having to search for devices periodically.

Devices that are managed by JP1/IT Desktop Management

Devices that are included as management targets or excluded from being managed are automatically registered in a network control list. These devices are therefore allowed network access. This means that you do not have to add these devices to the network control list.

Devices that are not managed by JP1/IT Desktop Management

To register all devices, periodically search the network for devices. By periodically searching the network for devices, you can discover devices that have just been turned on or laptop computers taken out of the office that have just accessed the network.

In addition, by enabling the network monitor for each network segment, you can discover devices currently accessing the network and new devices that have just accessed the network. If you enable the network monitor for each network segment, make sure that you do not change the default network monitor setting (allow network access for newly discovered devices).

Devices that are included as management targets or excluded from being managed are automatically registered in a network control list.

Important note

If you replace a network device such as a router with a new one, the MAC address is updated. Network access is therefore disabled for the new network device. If you want the new network device to be allowed network access, register the MAC address of the new network device in advance. Alternatively, fix the IP address of the network device and then register that IP address in a network control list.

Related Topics:

- 8.1 Enabling the network monitor

(2) General procedure for denying network access for unregistered devices

After registering all the devices used within your organization in a network control list, specify a setting to prevent devices not registered in the network control list from accessing the network.

Tip

Confirm that no more devices are discovered by a network search or by the network monitor, and that all the discovered devices have been either included as management targets or excluded from being managed. When these are confirmed, you can be sure that all the devices used within your organization have been registered in a network control list.

To deny network access for unregistered devices:

1. Enable the network monitor.

   Enable the network monitor for the network segments within the range of network access control.

2. Change the network monitor settings.

   By default, even when the network monitor is enabled, unauthorized devices are allowed access to the network. To prevent devices not registered in a network control list from accessing the network, set the network monitor settings to **Deny Network Access**, and then assign the network monitor settings to all the network segments.

   Tip

   If you specify common network monitor settings in advance that can be assigned to all network segments, you can change the network control settings of all network segments by simply making a change to the common network monitor settings.

Devices that are not registered in the network control list can no longer access the network.

Related Topics:

- 8.1 Enabling the network monitor

(3) Checking devices accessing the network

Even when the network monitor settings do not allow network access for newly connected devices, you can still check new devices that have accessed the network.

New devices are discovered as soon as they access a network. You can view the discovered devices in the **System Summary** panel of the Home module or the **Discovered Nodes** view of the Settings module. As soon as the new devices are discovered, network access is automatically disabled for these devices. You can see whether network access has been disabled for new devices by checking events.

If a privately-owned computer accessing the network is found, you have to identify the user based on the device information of the discovered computer, and then ask the user for the reason of network access. If the user has accessed the network for non-work-related reasons, instruct the user not to bring a privately-owned computer to work.

(4) Monitoring the network access status of devices in real time

If you are controlling network access of devices with the network monitor enabled, you can discover new devices accessing the network in real time. You can also automatically deploy agents to and install them on the discovered devices. By using this function, you can identify the current status of the devices accessing the network within your organization.

To discover devices by performing a network search, the devices must meet the following conditions at the time when a search is performed:

- Devices are accessing the network.
- Devices are turned on.

When devices have not accessed the network for a long time or when devices have been connected to the network but turned off for a long time, such devices are not discovered during a network search.

By enabling the network monitor, you can automatically discover devices when they access the network or when they turn on. In addition, you can automatically include the discovered devices as management targets or deploy agents to them according to the network search settings.

Important note

Even when you have specified the network monitor settings to deny network access for unregistered devices, these devices are discovered and agents are deployed to them. Whether devices to which agents have been deployed are allowed or denied network access depends on the settings such as security policies. Check the network access status of devices by using a device list in the Device module.

To monitor the network access status of devices used within your organization in real time, prepare a computer for each network segment that meets all of the following conditions:

- An agent has been installed.
- The network monitor is enabled.
- The computer is operating 24 hours.

1.6.2 General procedure for disabling network access for devices that have been infected with viruses

When a virus is detected in a computer accessing the network within your organization, you must immediately disable network access for that computer to prevent the virus from spreading to other computers.

By using the network monitoring function, you can disable or enable network access for devices any time. This function is useful when you want to temporarily disable network access for virus-infected computers, take proper anti-virus measures, and then enable network access for these computers again.

To control network access for a virus-infected computer:

1. Disable network access for a virus-infected computer.
   When a virus is detected in a computer, disable network access for that computer, and then take measures to prevent the virus from spreading to other computers.
2. Enable network access for the computer after taking proper anti-virus measures.
   After taking proper anti-virus measures, enable network access for the computer.

The computer for which proper anti-virus measures have been taken can access the network again.

Tip

For security protection, even when network access is disabled for a computer, you can allow that computer to access certain servers by settings.

Related Topics:

- 1.7.5 Checking the anti-virus status when a virus infection occurs

(1) General procedure for disabling network access for virus-infected devices

When a virus is detected in a computer used within your organization, you need to disable network access for that computer, and then take measures to prevent the virus from spreading to other computers.

1. Receive notification from a user that the user's computer has been infected with a virus.

   Receive notification from a user that the user's computer has been infected with a virus. Confirm that the user has removed the LAN cable from the user's computer, and that the virus infecting the user's computer has been quarantined and deleted by the anti-virus product.

2. Disable network access for the computer.

   Disable network access for the computer and do not enable it until you verify that proper anti-virus measures have been taken.

   In the **Device Inventory** view of the Device module, select the virus-infected computer. From **Action**, select **Deny Network Access**.

   Tip

   By using filtering conditions such as **Operating System**, **User Name**, **Department**, and **Location**, you can find a computer of interest more quickly.

3. Check the anti-virus status.

   Although you have already confirmed that the virus has been quarantined and deleted, you have to check for the presence of suspicious software that can cause virus infection, and make sure that the anti-virus status of the computer has been updated.

Anti-virus measures for the computer are complete.

Related Topics:

- (1) Checking whether there is any problem with the computer where the virus was found
- (2) Checking the anti-virus status of computers

(2) General procedure for enabling network access for a device after taking proper anti-virus measures

After making sure that proper anti-virus measures have been taken for the virus-infected device, enable network access for the device.

1. Enable network access for the computer.

   After making sure that proper anti-virus measures have been taken, allow network access for the computer. To enable network access for the currently disabled device, select the device in the **Device Inventory** view of the Device module, and from **Action**, select **Allow Network Access**.

2. Inform the user that the user's computer is allowed network access.

   Inform the user that the user's computer is allowed network access.

   When the user reconnects the LAN cable to the computer, the computer is allowed network access, and the user can resume operations.

The computer from which the virus has been deleted can access the network again.

1.6.3 General procedure for automatically controlling network access of devices in violation of a security policy

Devices in violation of a security policy do not have adequate security protection. If you allow such devices to continue accessing the network, problems such as information leakage, invalid operation, or virus infection can occur due to security flaws.

By specifying the network control conditions in a security policy, you can automatically disable or enable network access for computers according to the status of computers determined based on the security policy. This function is useful when you want to deny network access for computers that lack security protection and prevent the computers from accessing the network until adequate security protection is implemented on the computers.

To automatically control network access of a device in violation of a security policy:

1. Specify the network control settings in a security policy.

   To automatically disable network access for computers that lack security protection, specify the security configuration items, message notification to a user, and the network connection control settings in a security policy.

2. Identify the device for which network access has been disabled.

   Network access is automatically disabled for a device according to the status of the device determined based on the security policy. Identify the device for which network access has been disabled, so that you can contact the user of the device and instruct the user to take appropriate measures.

3. Implement security protection on the device in violation of the security policy.

   Instruct the user of the device to implement security protection on the device. When the security status of the device is determined as satisfactory, network access is automatically enabled for the device.

You can automatically enable or disable network access for devices according to the status of devices determined based on the security policy.

Related Topics:

- 1.7.1 Setting a security policy

(1) Specifying network control settings in a security policy

To automatically disable network access for computers that lack security protection, specify the network control settings in a security policy. In the network control settings, you can specify whether to allow or deny network access for computers according to the violation level determined for each computer. You can also specify a condition for disabling network access for computers, such as a time limit (in days) to correct the violation.

For example, by using the automatic message notification function, you can have a message sent to a user after a routine security check to prompt the user to implement security protection measures on the user's computer. If the user continues to ignore this message, you can disable network access for the user's computer. You can perform this operation by specifying a security policy as follows:

- Specify the security configuration items.

  Specify mandatory security requirements. Network access is disabled for any computers in violation of these requirements. In addition, for each requirement, set violation levels that determine judgment results.

- Specify a message to be sent to users.

Set the violation level that triggers message notification and specify the text of a message.

Tip

Write a message stating that network access is disabled if the problem persists.

- Specify the network connection control settings.

  Set a violation level that causes network access to be disabled for a computer. If you want to disable network access for computers only when the violation persists for several days in a row, set a time limit (in days) in **Disconnect Condition**. You do not have to specify **Disconnect Condition** if you want to immediately disable network access for computers determined to be lacking security protection.

  When security protection measures have been implemented on a computer that was previously in violation of a security policy and the computer is determined to be *Safe*, network access is automatically enabled for the computer.

Important note

If you have manually disabled network access for a computer, network access is not automatically enabled for that computer even when the computer is determined to be *Safe* after implementation of proper security protection measures. If you want to automatically enable network access for a computer when the computer is no longer in violation of a security policy, do not manually disable network access for the computer.

After you specify a security policy, you can control network access of computers according to the security status determined for the computers.

Tip

For security protection, even when network access is disabled for a computer, you can allow that computer to access certain servers by settings.

Related Topics:

- 1.7.1 Setting a security policy

(2) Identifying the devices for which network access has been disabled

By specifying the message notification setting in a security policy, you can automatically send a message to a computer in violation of a security policy and prompt the user to implement security protection measures on the user's computer. In addition, by specifying the network control settings in a security policy, you can automatically disable network access for a computer in violation of the security policy.

When a computer is in violation of a security policy, a message is sent to the user of that computer after a routine security check. If the user continues to ignore this message and takes no measures to implement security protection on the computer, network access is automatically disabled for the computer according to the network control settings.

If a user finds out that network access has been disabled for the user's computer and contacts you (administrator) for assistance, you need to instruct the user to implement security protection measures on the user's computer. By identifying the status of the user's computer, you can give clearer instructions on what the user has to do to implement proper security protection measures on the user's computer.

To identify the computers for which network access has been disabled, display the devices whose **Connection Status** is  in the **Computer Security Status** view of the Security module. By using the filtering function, you can quickly

find the computer you are looking for. By identifying the status of the device for which network access has been disabled, you can understand the security flaws of the device.

Tip

You (administrator) can also have email notification sent out to you to inform you that network access has been disabled for a device. To enable email notification, in the **Event Notifications** view of the Settings module, select the **Warning** and **Security** check boxes. When you select these check boxes, email notification is sent out not only when network access is disabled for a device but also when other warning events occur.

After identifying what the problem is, ask the user to take appropriate measures.

Related Topics:

- (1) Recognizing a security policy violation through email

(3) Implementing security protection measures on a device in violation of a security policy

After appropriate measures are taken to correct the security flaws found in a device for which network access has been disabled due to violation of a security policy, network access is automatically enabled for the device.

When, according to a request made by an administrator or based on the content of a message, a user corrects all the problems that have led the violation of the security policy, the violation level of the computer becomes *Safe*. When the computer is determined as *Safe*, network access is automatically enabled for the computer.

Related Topics:

- 9. Managing the Security Status
- 1.7.2 Taking measures against a security policy violation

1.6.4 General procedure for temporarily allowing network access for specified devices

If you deny network access for new devices, you have to change the network control settings whenever employees from other locations or individuals responsible for maintaining the systems within the company have to access the network within your organization. By specifying computers for which to temporarily allow network access, you can allow the specified computers to access the network for a specified period of time.

To temporarily allow network access for specified devices:

1. Allow network access for specified devices for a specified period of time.
   Specify the computers for which to temporarily allow network access so that these computers can access the network for a specified period of time.
2. Extend the network access period during which network access is temporarily allowed for the specified devices.
   To extend the network access period, specify a new period.

(1) Specifying a period for which to allow network access for specified devices

When employees from other locations or individuals responsible for maintaining the systems within the company have to access the network within your organization, you can temporarily allow network access for their computers. In this way, the computers can access the network for a specified period of time.

1. Obtain information about the computers for which to allow network access.

   To register the computers for which to allow network access, obtain the following information from the users in advance:

   - User name
   - Department to which the user belongs
   - Start date and end date of network access
   - MAC address
   - Reason for application

2. Temporarily allow network access for the specified computers.

   In the **Network Filter Settings** view of the Settings module, specify the computers for which to temporarily allow network access.

   Click the **Add** button and register the information that you have previously obtained from the users. Allow network access for the specified computers, select the **Start Date/Time** and **End Date/Time** check boxes, and then specify the period for which to allow network access.

The registered computers can access the network for the specified period of time.

When the specified period expires, network access is automatically disabled for the computers.

(2) Extending the network access period during which network access is temporarily allowed

When employees from other locations or individuals responsible for maintaining the systems within the company are temporarily allowed to access the network within your organization, the specified network access period is sometimes not enough to complete the necessary tasks. In this case, you can extend the network access period by specifying a new period.

To specify a new network access period, in the **Network Filter Settings** view of the Settings module, select the applicable computers and then click the **Edit** button. In the displayed dialog box, change the **End Date/Time** setting.

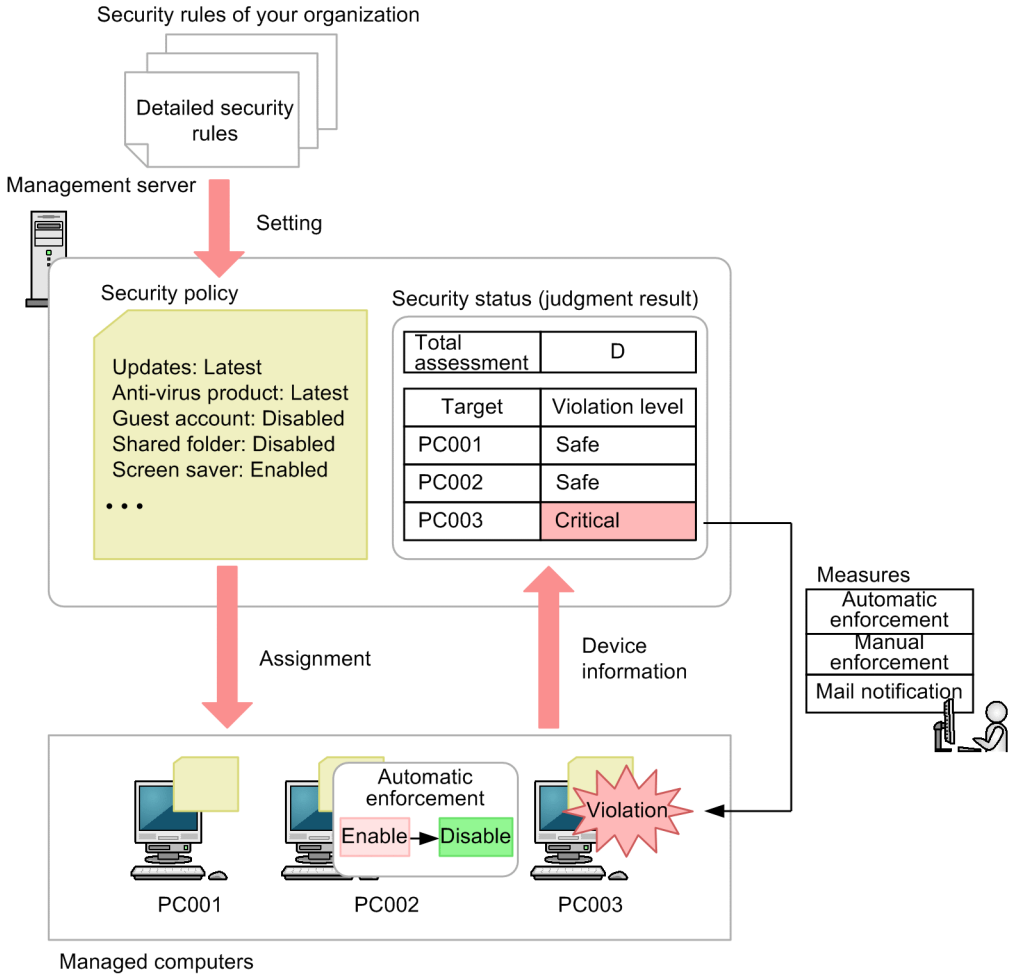
1.7 Managing the security status

To manage the security status of computers in your organization, you need to determine the security rules and make each computer user observe such rules. You also need to keep track of the current security status and correct security problems if necessary.

By using JP1/IT Desktop Management, you can do the following to efficiently manage computer security:

- Set a security policy based on the security rules of your organization and apply that policy to each computer.
- Keep track of the status of each computer's security policy compliance and security problems, using a list or report.
- Automatically take measures against security problems.

You can perform security management operations in the Security module. To manage the security status, set a security policy, keep track of the status of computers, and take measures against any detected security problem. By repeating the cycle of status tracking and taking measures against security problems, improve the security status of your organization. The following figure shows how to manage the security status:



Based on the security rules of your organization, set a security policy by using JP1/IT Desktop Management.

By assigning a security policy to computers, you can check the status of security policy compliance in a list or report. If you find any problem, take necessary measures. If you set automatic enforcement to the security policy, necessary measures are taken at the time when you assign the security policy to computers.

Using the security policy settings, you can also deter the use of some software or USB device, or obtain an operation log from each computer to detect a suspicious operation.

This section explains how to use JP1/IT Desktop Management in the operations described below. See the description of the operation that suits your purpose.

Set a security policy.

Set a security policy by using JP1/IT Desktop Management based on the security rules of your organization. By applying the set security policy to computers, you can check the status of security policy compliance (security status).

Take necessary measures against a security policy violation.

You (administrator) can set the configuration in such a way that if a security policy violation occurs, you are informed of that violation by email. Based on the email, you can take necessary measures against the security policy violation. There are two methods for taking measures against security policy violations: automatic enforcement and manual enforcement.

Automatically apply updates to computers.

JP1/IT Desktop Management obtains updates released by Microsoft and automatically distributes and applies them to computers. It takes a certain period time for JP1/IT Desktop Management to apply updates to computers after the updates have been released.

Manually apply updates to computers.

You (administrator) obtain updates released by Microsoft and then register them in JP1/IT Desktop Management to distribute and apply them to computers. You can immediately apply released updates to computers.

Check the anti-virus status when a virus infection occurs.

When the anti-virus product detects a virus, you can check the anti-virus status of computers.

Permit the use of authorized software only.

By checking the software installed on each computer, you can register and manage any software unnecessary for work as unauthorized software.

Check for information leakage.

If a suspicious operation is detected, you can check for information leakage.

Restrict the use of USB devices.

You can permit data to be read from and written to authorized USB devices only. You can also prohibit the use of USB devices in your entire organization and permit users in your organization to read data from and write data to a USB device only on the specific computer.

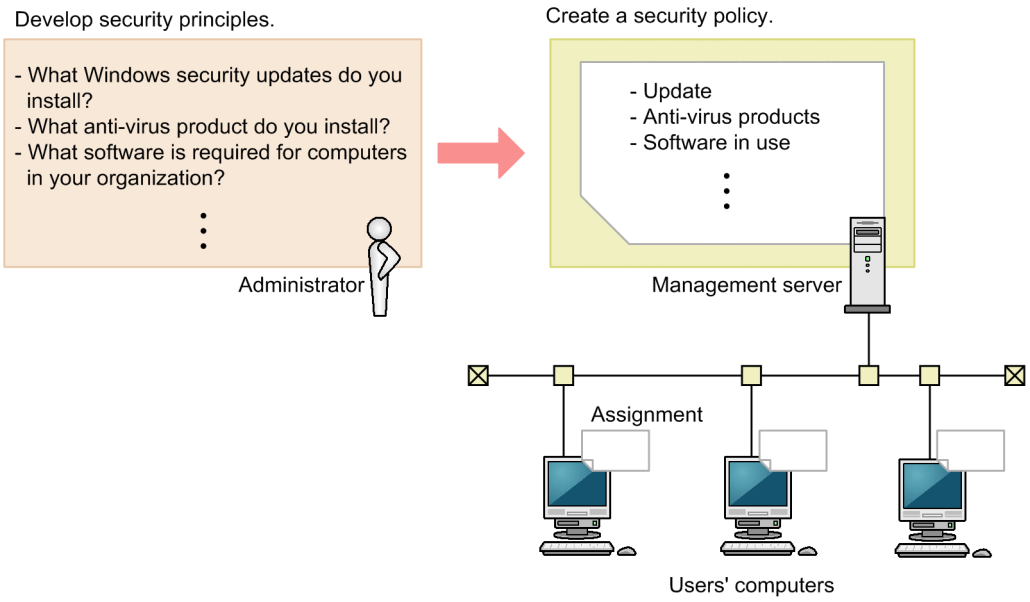
Respond to a security audit.

For a security audit to be conducted, you can provide proof that the security status in your organization is properly managed based on the security policy.

1.7.1 Setting a security policy

To manage the security status of computers in your organization, you need to develop security principles for your organization first. If your organization has no security principles, develop security principles before starting security management by using JP1/IT Desktop Management.

Based on the developed security principles, create a security policy by using JP1/IT Desktop Management. By assigning the created security policy to computers, you can check the status of security policy compliance (security status). Update the security policy if the latest security measures trends (security trends) change or your organization's security principles are changed.



Related Topics:

- (1) Developing security principles for your organization
- (2) Managing a security policy

(1) Developing security principles for your organization

If your organization has no security principles, develop security principles before starting security management by using JP1/IT Desktop Management. Based on the developed security principles, create a security policy by using JP1/IT Desktop Management. For that purpose, we recommend that you check the security policy items before developing security principles.

The points to consider when developing a security policy are as follows:

- Determine the updates to be installed on Windows.
- Determine the anti-virus product to be used in your organization.
- Create a list of software if some software must be installed on each computer or if you want to prohibit the use of some software.
- Create a list of prohibited services if you want to prohibit the operation of some services in your organization.
- Determine the principles on the security settings for computers used in your organization such as Widows Firewall settings and whether to use a shared folder.
- Create a list of deterrence-target operations if you want to deter some operations related to print operation, device operation, and software activation.
- Create a list if you want to monitor some emails and access to some Web sites, Web servers, and FTP servers.

To develop security principles, you need to keep track of security trends by checking newspaper articles, magazines, software development companies' Web sites, and others. By checking security trends based on your organization's operation policy, you can make your security management operation robust.

For example, you can choose the anti-virus product that matches your organization's operation policy by investigating in advance the virus detection rate and misdetection ratio of each anti-virus product.

Tip

If you find it difficult to obtain information about security trends, we recommend that your organization subcontracts information acquisition work to a tool vendor, VAR (Value Added Retailer), or external consultant.

When you finish developing security principles, create a security policy based on the developed security principles.

(2) 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.

1.7.2 Taking measures against a security policy violation

In JP1/IT Desktop Management, you can specify various settings to prepare for the occurrence of security policy violations. You can set the configuration in such a way as to automatically take measures against a security policy violation and automatically report the occurrence of a security policy violation by email.

In addition, JP1/IT Desktop Management is provided with functions for taking measures against a security policy violation after its occurrence. The functions include forcibly changing the settings of a computer that has violated a security policy and automatically sending the user of that computer a request message to take necessary measures.

By using these functions, you can smoothly take necessary measures when a security policy violation occurs.

(1) Recognizing a security policy violation through email

You (administrator) can set the configuration in such a way that if a security policy violation is found by the determination result of the security status, you are automatically informed of the violation by email. By specifying this mail notification setting, you can recognize in a timely manner that there is a problem with the security status and take action quickly.

If a security policy violation occurs, an event of the type *security control* is generated. Set the configuration in such a way that an email is automatically sent when this event is generated. Based on the sent email, check the security status and take necessary measures against a security policy violation.

1. Set mail notification.

   Set the event that triggers mail notification and the mail destination in the Event Notifications view, which is displayed by selecting **Events** in the Settings module and then **Event Notifications**.

   To report a security policy violation by email, set an event with the severity *Critical* or *Warning* and of the type *Security* as a mail notification target.

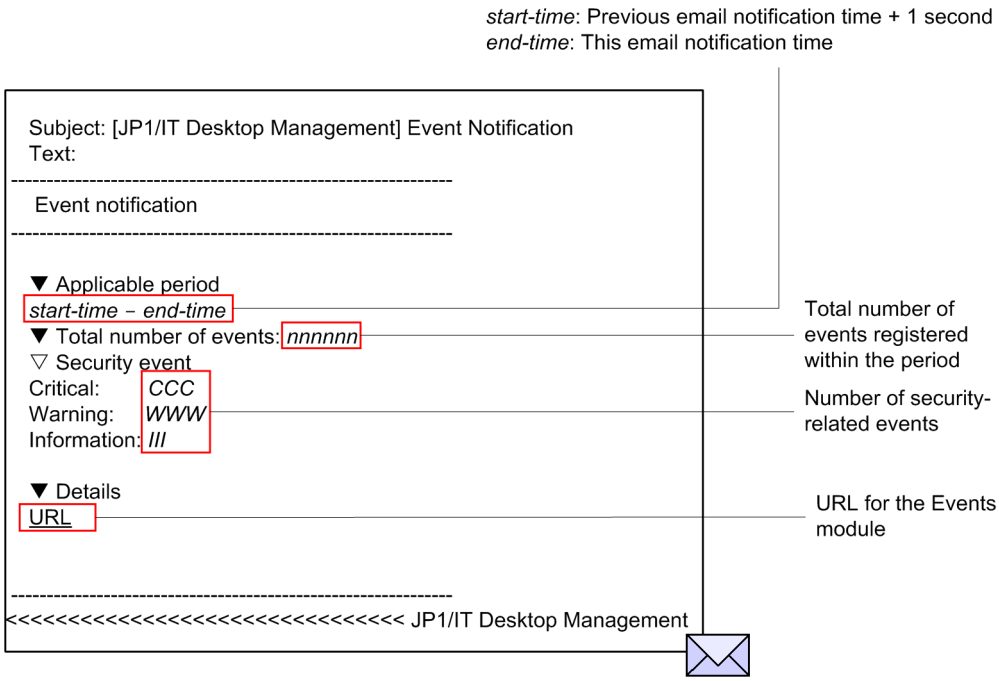
   The following table describes the correspondence between the severity of each event to be reported and the violation level of the security status:

Severity	Violation level
(Critical)	(Critical)
(Warning)	(Important)
	(Warning)
(Information)	(Safe)

2. Check the sent email.

   You can check the occurrence conditions of a security-related event in the email sent from JP1/IT Desktop Management. If a critical event has occurred, start the operation view of JP1/IT Desktop Management from the URL written in the email, check the security status, and then take necessary measures.

   The following figure shows the content of an email to be sent:



3. Check the security status.

   In the operation view of JP1/IT Desktop Management, you can obtain detailed information such as the details of a security policy violation and the location in which the security policy violation occurred. In the Home module or Security module, check the status of the computer judged as Critical and take action.

For mail notification, you need to specify the mail server to be used to send and receive emails.

Related Topics:

- (2) Automatically taking measures against a security policy violation

- (3) Manually taking measures against a security policy violation
- 15.8.1 Specifying settings for event notification
- 9.1 Checking the security status
- 15.9.1 Setting up mail servers

(2) Automatically taking measures against a security policy violation

If you enable automatic enforcement, when some security configuration item of a computer is in violation of a security policy, that security configuration item is automatically changed to its expected status.

If you set automatic enforcement to a security policy, the security configuration items of computers are automatically changed to their expected status at the time when a security policy is applied to computers. Automatic enforcement can save the administrator of JP1/IT Desktop Management and computer users the effort of taking necessary measures. According to the security principles and operation in your organization, examine the security configuration items for which automatic enforcement is enabled in a security policy.

Tip

For example, in an environment where Windows Firewall is disabled intentionally, if automatic enforcement enables Windows Firewall, a problem might occur with operation. In such a case, set a security policy not to apply automatic enforcement to the specified security configuration items.

You can see if necessary measures are taken against a security policy violation by confirming that Safe ( ) is displayed for the relevant item in the Security module.

Related Topics:

- 9.1 Checking the security status
- (3) Manually taking measures against a security policy violation

(3) Manually taking measures against a security policy violation

If you select manual enforcement, when you check the security status and find some security configuration item of a computer is in violation of a security policy, manually take measures against that violation.

Forcibly take measures.

For the security configuration items for which you can enable automatic enforcement, if some security configuration item is in violation of a security policy, you can forcibly take measures against that violation in an arbitrary timing.

Request the user to take measures.

You can set the configuration to automatically send an arbitrary message including details of a security policy violation to the user of the computer that is in violation of a security policy. Using this function with automatic enforcement, you can request the user to take measures in the security configuration items (such as password strength and power on password) to which automatic enforcement is not (cannot be) applied. To enable automatic message notification, specify the settings in **Action Items** in the **Add Security Policy** dialog box or the **Edit Security Policy** dialog box.

You can also set the configuration to send a message to a computer user in an arbitrary timing.

You can see if necessary measures are taken against a security policy violation by confirming that Safe ( ) is displayed for the relevant item in the Security module.

Related Topics:

- (2) Automatically taking measures against a security policy violation
- 9.1 Checking the security status
- 9.4 Enforcing the correction of security policy violations
- 6.22 Sending a notification to a user

(4) Taking measures against a security policy violation by a computer managed offline

Automatic enforcement does not work for computers managed offline. For that reason, if you check the security status and find that some security configuration item of a computer is in violation of a security policy, you (administrator) must directly instruct the user of the computer to take necessary measures.

After the user has taken necessary measures, obtain the device information of the computers managed offline again to check the security status.

You can see if necessary measures are taken against a security policy violation by confirming that Safe ( ) is displayed for the relevant item in the Security module.

1.7.3 General procedure for automatically distributing updates

When the OS of computers in your organization is Windows, to correct malfunctions or security problems, you must apply updates if necessary. JP1/IT Desktop Management can automatically distribute and apply updates released by Microsoft to computers according to a security policy.

To automatically apply updates to computers:

1. Obtain the latest information about updates.

   You can automatically obtain the latest information about updates released by Microsoft from the support service site. Check the information about the added updates and judge the necessity of their application.

2. Automatically distribute updates to computers.

   When you set the necessity of application of updates as a security policy judgment item, according to the result of judgment by a security policy, the updates that have not been applied to computers are automatically distributed.

3. Check the application status of updates.

   Check the application status of updates. If you find a problem, identify the cause and take necessary measures.

Updates have been applied to computers. The computers securely maintain their expected state.

(1) Obtaining the latest information about updates

To apply the latest updates to computers, you need to keep track of information about released updates.

You can automatically obtain the latest information about updates released by Microsoft from the support service site. You can check the obtained information about the updates in the **Update List** view of the Security module.

In addition, you can set the configuration in such a way that an email is automatically sent to you when an update has been added. By mail notification, you can check the added updates and also directly log in from the URL written in the email to check the **Update List** view.

Important note

To obtain the latest information about updates, you must have a support contract.

Important note

It takes about 10 working days for the information on the management server to be updated after updates are released by Microsoft.

Tip

Information about updates released on or after January 1, 2006 is registered in the Update List view by default.

Tip

If you cannot access the support service site because the management server cannot connect to the Internet or due to other reasons, distribute information about updates as follows: By using a computer that can access the support service site, manually download both updates and information about updates. Then, upload the updates and information to the management server.

Related Topics:

- 15.9.3 Setting information for connecting to the support service
- 15.9.1 Setting up mail servers

(2) Automatically distributing updates to computers

When you set the necessity of application of updates as a security policy judgment item, if a particular computer violates that security policy judgment item, you can take measures against the violation by automatically distributing the updates that have not yet been applied to the computer.

There are two methods for distributing updates. One is applying all the updates released by Microsoft and the other is applying specific updates only.

To apply all the updates

When you obtain information about updates from the support service site, the obtained information is applied to a security policy and the security state is determined based on the security policy. If some updates have not yet been applied to computers, these updates are automatically distributed to the computers. By specifying the update group in which the updates you want to exclude from application have been registered, you can also exclude specific updates from application.

To apply specific updates only

After you select the update group in which the mandatory updates have been registered, the updates included in the selected update group are distributed to computers according to the determination of the security status based on a security policy.

If you want to test updates before distributing them so as to avoid interference with operation in your organization, select the method for applying specific updates only.

How to set each method is described below.

Tip

You can specify the automatic distribution of updates on a security-policy basis. For example, if you want to apply all the updates to computers in the Sales Department and apply only specific updates to computers in the Development Department, create a security policy for each department. Then, set the appropriate application method of updates to each security policy.

To apply all the updates

Edit a security policy in the **Security Policy List** view of the Security module.

In **Windows Update** under **Security Configuration Items**, select **All updates are installed** for **Install Updates**. In addition, select the **Auto Enforce** check box, and then select **Distribute Updates**.

Based on information about all the updates registered in the management server, the application status of each computer is determined. If any updates that have not yet been applied are found, the updates are automatically distributed.

Tip

If you want to exclude some updates from application, create an update group in advance in the **Update List** view of the Security module. Then, specify the created update group in **Excluded Update Group:**.

To apply specific updates only

1. Select the updates applicable to computers.

   Create an update group in the **Update List** view of the Security module.

   At the beginning of operation of JP1/IT Desktop Management, register in the update group the updates that have already been applied to computers and the updates that you judge as applicable among the updates registered by default.

   Tip

   There are many updates registered by default. It is useful for you to select all the updates and then clear the check boxes for the unnecessary updates when you want to apply most of the updates.

2. Set a security policy.

   Edit a security policy in the **Security Policy List** view of the Security module.

   In **Windows Update** under **Security Configuration Items**, select **Selected updates are installed** for **Install Updates**. At this time, specify the group created in step 1 for the update group. In addition, select the **Auto Enforce** check box, and then select **Distribute Updates**.

   If you make the settings above, only the updates registered in the update group become security policy judgment targets. In addition, if some updates are judged as unapplied, the updates are automatically distributed.

3. Check for newly added updates.

   When you obtain information about new updates from the support service site, judge the necessity of application of the updates.

   If you judge the updates as applicable, register the updates in the update group. If you make this registration, you can add the updates as security policy judgment targets. If you judge updates as not applicable, enter the reason in the **Notes** tab of the **Update List** view.

Tip

When you test whether an update is applicable, it is useful for you to set an update group and a security policy for testing purposes and then assign that security policy to a computer for testing purposes. Simply by registering an update to be tested in the update group for testing, you can automatically distribute that update to the computer for testing.

The updates registered in the update group are automatically distributed to computers according to the determination of the security status based on the security policy.

(3) General procedure for checking the application status of updates

Using the **Windows Update** tab in the **Security Policy List** view of the Security module, you can check whether there is any problem with the application status of updates.

After checking the device security status, if you find that the violation level is *Safe*, there is no problem. However, if the violation level is *Important* or *Critical*, some updates might not have been applied. Keep track of the status and take necessary measures as follows:

1. Keep track of the application status of updates.

   In the **Security Policy List** view, you can only check whether a problem exists. Therefore, to check the application of which update has a problem, display the **Windows Update Installation Status** report in **Security Detail Reports**. In this report, you can identify the update that has not been applied to computers.

2. Check for the cause of non-application.

   After checking the report, if you find that some update has not been applied to computers, distribution of that update might have failed. In the **Task List** view of the Distribution module, select the task whose type is **Policy Based Task(Windows Update)**, and then check the status of the computer to which the update was not distributed. By checking the details of the task status at this time, you can check the cause of distribution failure.

3. Take measures against the non-application of the update.

   You can redistribute the update to the computers to which the update has not been applied.

   In the **Security Policy List** view of the Security module, select the **Windows Update** tab, and under **Action**, click the **Distribute Updates** button. The update is redistributed to the computers to which that update has not been applied.

   Tip

   You can also redistribute an update by using the **Enforce** button in the **Computer Security Status** view.

You have now finished checking the application status of the update and taken necessary measures. If there are multiple updates that have not been applied, repeat this procedure to take necessary measures.

Tip

You can also check the distribution status of updates by using the task execution result. If an update distribution failed, check the task status in details to correct the cause. Check the status of update application to computers by using the **Not Applied Computers** tab in the **Security Policy List** view of the Security module.

1.7.4 Manually registering and distributing an update

If an urgent update that must be immediately applied to computers in your organization is released, you need to manually register such an update before distributing and applying it.

Tip

JP1/IT Desktop Management can automatically distribute and apply updates released by Microsoft to computers according to a security policy. However, it takes about 10 working days after release of updates for JP1/IT Desktop Management to be able to automatically distribute the updates whose information is registered in the support service site.

To manually distribute an update:

1. Prepare an update to be distributed.

   Download an update to be distributed from Microsoft's Web site. Then, when registering information about the update in JP1/IT Desktop Management, create an update file. If you have set the configuration in such a way as to apply only specific updates, add the update to the update group.

2. Check the application status of the update.

   Check the application status of the update. If you find a problem, identify the cause and take necessary measures.

(1) General procedure for preparing an update to be distributed

Download the executable file of an update to be distributed. In addition, register the information about the update in JP1/IT Desktop Management to register the update file.

1. Download the executable file of an update to be distributed.

   If you manually register and distribute an update, download the executable file of the update to be distributed from Microsoft's Web site in advance.

   Tip

   To check information about updates, from the top page of Microsoft's Web site, move to the security page (Security Home), and then click the link to the target update.

2. Register the information about the update and the update file.

   In the **Update List** view of the Security module, register the information about the update to be distributed and the update file. By registering the information about the update, you can check the application status of the update after distributing the update. By registering the update file, you can register data for distributing the update to the users' computers.

Important note

There are multiple types of command to be executed when updates are distributed. Check the detailed information of updates in Microsoft's Web site to select the appropriate command for individual updates.

Tip

If you have set the configuration in such a way as to apply only specific updates, add the update to the update group. According to the automatic enforcement settings in the security policy to which the update group is set, the update is applied to the target computers.

Related Topics:

- 9.8.3 Manually adding program updates to the Update List

(2) General procedure for checking the application status of updates

Using the **Windows Update** tab in the **Security Policy List** view of the Security module, you can check whether there is any problem with the application status of updates.

After checking the device security status, if you find that the violation level is *Safe*, there is no problem. However, if the violation level is *Important* or *Critical*, some updates might not have been applied. Keep track of the status and take necessary measures as follows:

1. Keep track of the application status of updates.

   In the **Security Policy List** view, you can only check whether a problem exists. Therefore, to check the application of which update has a problem, display the **Windows Update Installation Status** report in **Security Detail Reports**. In this report, you can identify the update that has not been applied to computers.

2. Check for the cause of non-application.

   After checking the report, if you find that some update has not been applied to computers, distribution of that update might have failed. In the **Task List** view of the Distribution module, select the task whose type is **Policy Based Task(Windows Update)**, and then check the status of the computer to which the update was not distributed. By checking the details of the task status at this time, you can check the cause of distribution failure.

3. Take measures against the non-application of the update.

   You can redistribute the update to the computers to which the update has not been applied.

   In the **Security Policy List** view of the Security module, select the **Windows Update** tab, and under **Action**, click the **Distribute Updates** button. The update is redistributed to the computers to which that update has not been applied.

   Tip

   You can also redistribute an update by using the **Enforce** button in the **Computer Security Status** view.

You have now finished checking the application status of the update and taken necessary measures. If there are multiple updates that have not been applied, repeat this procedure to take necessary measures.

Tip

You can also check the distribution status of updates by using the task execution result. If an update distribution failed, check the task status in details to correct the cause. Check the status of update application to computers by using the **Not Applied Computers** tab in the **Security Policy List** view of the Security module.

1.7.5 Checking the anti-virus status when a virus infection occurs

If a virus infection is detected among computers used in your organization, after the anti-virus product quarantines the virus, you need to check whether there is any problem with the anti-virus status and usage status of all the computers under your management.

By using JP1/IT Desktop Management, you can check the anti-virus status and usage status of each computer.

1. Check whether there is any problem with the computer where the virus was found.

   Using JP1/IT Desktop Management, check the device information of the computer where the virus was found. If the computer has a problem such as illegal software installed on that computer, that problem might have caused the virus infection. In such a case, take appropriate measures.

2. Check the anti-virus status of the computers.

   Check the anti-virus status of the computers in your organization by using the **Antivirus Software Status** report in JP1/IT Desktop Management.

By following the above procedure, you can check the anti-virus status in your organization.

Related Topics:

- 1.7 Managing the security status
- 1.6.2 General procedure for disabling network access for devices that have been infected with viruses

(1) Checking whether there is any problem with the computer where the virus was found

If a virus is detected on a computer in your organization, that virus is quarantined by the anti-virus product. After the virus has been quarantined, by using JP1/IT Desktop Management, you need to check whether suspicious software leading to virus infection is used on that computer and whether the anti-virus status of that computer is the latest.

1. Receive notification from a user that the user's computer has been infected with a virus.

   Receive notification of a virus infection from the user of the managed computer. Confirm with the user that the anti-virus product has quarantined and deleted the virus that infected the user's computer.

2. Display information about the relevant computer.

   To check the usage status of the computer, using the **Device Inventory** view of the Device module, display the computer where the virus was found.

   Tip

   By using filtering conditions such as **Operating System**, **User Name**, **Department**, and **Location**, you can find a computer of interest more quickly.

3. Check whether suspicious software is installed.

   If any software downloading a virus into a computer is installed on the target computer, another virus infection might occur. Using the **Installed Software Details** tab in the **Device Inventory** view, check the software installed on the target computer.

   If any suspicious software is installed on the target computer, instruct the user to uninstall the software.

4. Check whether the anti-virus status is the latest.

   If the anti-virus status of the target computer is not the latest, the computer might be infected by a virus again. Using the **Security Details** tab in the **Device Inventory** view, check whether the versions of the anti-virus product's engine and virus definition are the latest.

In addition, check information about the virus and how to handle the virus infection in the Web site of the anti-virus product, if necessary.

If there is any problem with the anti-virus status of the target computer, take appropriate measures.

5. Perform a virus scan.

To confirm that no file infected by the virus remains on the computer, instruct the user to perform a virus scan on the entire computer. If the scan result shows no problem, your checking operation is complete.

By following the above procedure, you can check whether there is any problem with the computer where the virus was found.

Related Topics:

- (2) Checking the anti-virus status of computers

(2) Checking the anti-virus status of computers

If a virus is detected on a computer in your organization, that virus is quarantined by the anti-virus product. After the virus has been quarantined, you need to check whether the anti-virus status of all the computers in your organization is the latest to prevent damage by the virus.

You can check the anti-virus status of the computers by using the **Antivirus Software Status** report. In the report, information such as whether the anti-virus software is installed and whether the virus definition file is the latest version is displayed.

If there is any problem with the anti-virus status, check the target computer, and then take appropriate measures.

To inform your superior, the security-related department, and others of the anti-virus status, output a report and submit it to the personnel or department concerned. You can print out a report by clicking the **Print** button in the **Antivirus Software Status** report.

1.7.6 General procedure for permitting the use of authorized software only

Various types of software used for work are installed on computers in your organization. If you do not manage the software allowed for use in your organization, software that potentially causes information leakage and computer virus infection might be installed on a particular computer. To eliminate this danger, keep track of what software is installed on computers in your organization and permit the use of authorized software only.

Using JP1/IT Desktop Management, you can manage information about software installed on computers. You can also register software unauthorized in your organization and monitor the installation status of the unauthorized software. For computers managed online, you can deter unauthorized software from starting or automatically uninstall such software.

Tip

In addition to unauthorized software, you can register mandatory software and monitor the installation status of the mandatory software. For computers managed online, you can automatically install mandatory software on such computers.

To manage software by checking the software installed on computers in your organization and permitting the use of authorized software only:

1. Check any software installed recently.

   Using JP1/IT Desktop Management, check whether any new software is recently installed on computers. If there is newly installed software, investigate whether the new software is necessary for work.

2. Restrict the use of software.

   If the new software is not necessary for work, register it in JP1/IT Desktop Management as unauthorized software and restrict its use.

   In addition, set the configuration in such a way that any unauthorized software installed on the relevant computers from now on is automatically uninstalled.

Then, only the authorized software is used in your organization.

Related Topics:

- 1.7 Managing the security status

(1) General procedure for checking recently installed software

Check whether any file-sharing software that causes a security problem or software that is not related to work is installed on computers in your organization. If any of such software is installed, information leakage or computer virus infection might occur. For that reason, periodically check whether any new software is installed on computers to keep track of the software installed on computers in your organization.

If there is any newly installed software, investigate information about the software, and then ask the user about the intended use.

1. Check newly installed software.

   Check whether any new software is recently installed on computers in the **New Software** panel. To open the **New Software** panel, in the Device module, select **Overview** and then **Dashboard** to display the Dashboard view. If there is newly installed software, investigate whether the new software is necessary for work.

2. Investigate information about software.

   New software that is recently installed on a particular computer is displayed in the **New Software** panel in the Dashboard view, which is displayed by selecting **Overview** in the Device module and **Dashboard**. Click the link of the software name to navigate to the **Software Inventory** view of the Device module. In the **Software Inventory** view, check information about the software and the computer where the software is installed.

   Using the Internet or others, investigate whether the new software is necessary for work. If the new software is not necessary for work, ask the user about the intended use.

3. Ask the user about the intended use.

   In the **Software Inventory** view of the Device module, select the **Installed Computers** tab. Inform the user of the displayed computer that software not necessary for work is installed on the computer, and ask the user about the intended use.

   If the intended use is not justified, instruct the user to uninstall the software or use the distribution function to uninstall the software. In addition, advise the user not to install any unauthorized software from now on.

If the new software is not necessary for work, register it as unauthorized software and restrict its use.

Tip

If you set the configuration in such a way as to collect operation logs, you can investigate traces of software usage (program activation logs) in the **Operations Logs** view of the Security module.

Related Topics:

- 12.3 Uninstalling software from a computer
- 10.3 Viewing operation logs

(2) General procedure for restricting the use of software

If you find that the software newly installed on a particular computer is not necessary for work, register the new software as unauthorized software and restrict the use of the new software.

1. Register software as unauthorized software.

   To restrict the use of the software, in the **Software Inventory** view of the Device module, register the software in a security policy as unauthorized software.

   Tip

   You can also register unauthorized software when setting a security policy.

   After registering the software as unauthorized software, you can check the installation status of the unauthorized software by using the **Unauthorized Software Installation Status** report in the **Security Detail Reports** view of the Reports module. For computers managed online, you can deter unauthorized software from starting or automatically uninstall unauthorized software.

2. Check the installation status of unauthorized software.

   Check the **Unauthorized Software Installation Status** report in the **Security Detail Reports** view of the Reports module. Check the usage trends of unauthorized software and the status of countermeasures taken against unauthorized software, and if there is any problem, take action.

Tip

You can also register mandatory software in a software use policy. After registering mandatory software, you can check the installation status of the mandatory software by using the **Mandatory Software Installation Status** report. For computers managed online, you can automatically install mandatory software on such computers.

Then, only the authorized software is used in your organization.

Related Topics:

- 6.20 Setting unauthorized software
- 9.3.1 Adding security policies

1.7.7 Restricting the use of USB devices

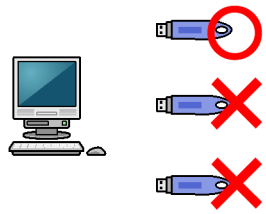
Various types of data such as customer data, sales data, and development data exist on computers in your organization. If any of these types of confidential information leaks out, there is huge damage and your organization's social reputation is also ruined. For that reason, you need to take security measures to protect confidential information by preventing data from being brought out or lost.

Using JP1/IT Desktop Management, you can deter the operation to read from and write to external media. By using this function, you can prevent information leakage caused by data brought out.

This subsection explains how to restrict the use of USB devices. To restrict the use of USB devices, the following two methods are available:

- Permit the use of registered USB devices only.
- Permit only specific computers to use USB devices.

Permit the use of registered USB devices only.



Permit only specific computers to use USB devices.

To lend a USB device so as to prohibit the use of privately-owned USB devices:

1. Register authorized USB devices.

   Prepare USB devices to be lent, and then register them in JP1/IT Desktop Management as authorized USB devices.

2. Deter the use of any USB devices other than the authorized USB devices.

   Using JP1/IT Desktop Management, deter the operation to read from and write to USB devices. At the same time, permit the use of only the USB devices registered in step 1.

3. Lend an authorized USB device.

   Have a user who wants to use a USB device submit an application to you, check the content of the application, and then lend a USB device to that user.

   Using JP1/IT Desktop Management, change the asset status of the USB device when it is lent and when it is returned.

4. Check the usage log of the lent USB device.

   Check whether the lent USB device has been used as the submitted application.

Then, the usage status of the USB devices can be properly managed and data cannot be brought out unnecessarily.

Related Topics:

- (5) Permitting users to bring out data through only a specific computer
- 1.7 Managing the security status
- (6) Handling the loss of a USB device

(1) Registering authorized USB devices

To prevent information leakage caused by data brought out, permit the use of specific USB devices and prohibit the use of any USB devices other than the specific USB devices. For example, you can deter the use of privately-owned USB devices by permitting the use of only the USB devices owned by your organization.

To permit the use of specific USB devices only, you need to register authorized USB devices first.

1. Register USB devices.

   Prepare USB devices to be lent, and then register them as authorized USB devices. When registering the USB devices, set registrant information to make clear who registers these USB devices.

   When you have registered the USB devices, hardware asset information about the USB devices is registered in the **Hardware Asset** view of the Assets module.

   > **Tip**
   >
   > If you want the user to register a USB device, set the authentication information for USB device registration in the agent configuration, and then assign the agent configuration to the user's computer in advance. Then, inform the user about the authentication information and registration method if necessary, and ask the user to register a USB device.

2. Edit the hardware asset information.

   Unconfirmed is displayed under **Asset Status** for the hardware asset information of the registered USB devices. Also, only the information that is collected from the USB devices and the user information that has been set at the time of registration are registered. Therefore, manually register information that is not automatically collected such as **Asset #** and **Asset Status** (**In Stock**). Set **Asset Status** to any value other than **Unconfirmed** and **Disposed** to register the USB devices as authorized USB devices.

Then, the authorized USB devices are registered.

Related Topics:

- 9.7 Registering USB devices
- 11.1.2 Editing hardware asset information
- (2) Deterring the use of any USB device other than the authorized USB devices

(2) Deterring the use of any USB device other than the authorized USB devices

To prevent information leakage caused by data brought out, permit the use of specific USB devices and prohibit the use of any USB devices other than the specific USB devices. For example, you can deter the use of privately-owned USB devices by permitting the use of only the USB devices owned by your organization.

After registering authorized USB devices, you need to deter the use of any USB devices other than the authorized USB devices.

Set a prohibited operation policy.

To deter the use of any USB devices other than the authorized USB devices, set a prohibited operation policy. At the same time, permit the use of the authorized USB devices only.

Then, the use of any USB devices other than the authorized USB devices is deterred.

Related Topics:

- 9.6 Suppressing the use of external media
- (1) Registering authorized USB devices

(3) Lending a USB device to a user

When you permit the use of only the USB devices owned by your organization (USB devices already registered in JP1/IT Desktop Management), you need to lend such a USB device to a user who intends to use a USB device. In such a

case, have the above user submit an application for USB device use, and when the intended use is appropriate, lend a USB device to the user.

1. Have the user submit an application for USB device use.

   Obtain the following information to manage the USB device lending operation:

   - Date of usage
   - Date of return
   - Intended use
   - Department
   - User name
   - Email address
   - Phone number
   - Asset management number of the computer to use the USB device
   - Name of the file containing the data to be written to the USB device

2. Lend a USB device to the user.

   When the intended use is appropriate, lend a USB device to the user.

   To manage the borrower of the USB device, edit the asset information of that USB device and change the user information of that USB device to the borrowing user's information. If you do not want to change the user information of the USB device, add a management item for borrower management or save a history in the **Notes** tab such as the date of lending and the borrower.

   After lending the USB device, to make it clear that the USB device is being lent, change the value for **Asset Status** by adding a new status (such as `On Loan`) to **Asset Status** in the hardware asset status information.

   Also, to keep track of the return schedule, set the values for **Planned Asset Status** and **Planned Date**. If the USB device is scheduled to be returned one week later, set **In Stock** for **Planned Asset Status** and set the date one week later for **Planned Date**.

   Tip

   By setting a value for **Planned Asset Status**, you can check the USB device scheduled to be returned in **Hardware Asset Status (Planned)** on the Summary Reports.

When the user finishes using the USB device, ask the user to return the USB device.

When the USB device is returned, change the value for **Asset Status** of the hardware asset information from **On Loan** to **In Stock** to make the USB device ready to be lent again.

Related Topics:

- 11.1.6 Changing the asset status
- 11.1.7 Changing the planned asset status
- 11.1.2 Editing hardware asset information
- 15.5.1 Adding asset management items

(4) Checking the usage history of a USB device

You can check the usage history of a USB device from an operation log.

Tip

To obtain operation logs, you need to specify the operation log settings during setup, or build a site server configuration system. In addition, you need to enable the operation log policy.

1. Display the operation log of the user.

   You can check an operation log in the **Operations Logs** view of the Security module (the **Operation Log List (Distributed Operation Logs)** view if operation logs are stored in the site server). To check the history of a USB device, examine operation logs whose **Operation Type** is **External Device Operation** by using the filtering function. To check the usage history of a specific USB device, perform filtering on operation logs by **Source** or **User Name**.

2. Examine detailed information in the operation log.

   To check whether a USB device was used properly, examine detailed information in the operation log. Examine the following information:

   - Information about the computer that operated the external medium
   - Information about the user who operated the external medium
   - Information about the files copied to the external medium

You can check whether the USB device was used properly. If you find any problem with the usage status, check with the user about the usage status, and then take necessary measures.

Related Topics:

- 10.6 Viewing suspicious operation logs

(5) Permitting users to bring out data through only a specific computer

You can restrict the use of USB devices to prevent information leakage caused by data brought out unnecessarily.

As a way of restricting the use of USB devices, you can permit users to bring out data through only a specific computer. For example, you can operate JP1/IT Desktop Management in such a way as to permit only a shared computer to use USB devices and prohibit the users' computers from using USB devices.

This subsection explains how to permit only a specific computer to use USB devices.

1. Assign a policy to deter the use of USB devices to every computer.

   Apply a security policy to deter the use of USB devices to every computer.

   Using the prohibited operation policy, create a security policy in which the deterrence of USB devices is enabled, and then assign that security policy to every computer.

2. Assign a dedicated policy to a computer that is authorized to use USB devices.

   Apply a dedicated policy to a computer that is authorized to use USB devices.

   Using the prohibited operation policy, create a security policy in which the deterrence of USB devices is disabled, and then assign that security policy to a computer that is authorized to use USB devices.

Then, only a specific computer can use USB devices.

Related Topics:

- 9.3.1 Adding security policies
- 1.7.7 Restricting the use of USB devices

- (6) Handling the loss of a USB device

(6) Handling the loss of a USB device

When a USB device used in your organization becomes lost, it can lead to leakage of confidential information that is stored in the USB device, including customer data, sales data, and development data. An immediate action must therefore be taken when a USB device becomes lost.

If you specify the following settings by using the prohibited operation policy, you can check information about the files stored in the lost USB device:

- Deter the operation to read from and write to USB devices.
- Permit the use of registered USB devices.

Check whether any file containing confidential information is stored in the lost USB device.

Check the files stored in the USB device.

Using the **File List** tab displayed in the **Hardware Asset** view of the Assets module, you can check information about the files stored in the USB device. Note that the **File List** tab appears only when the target USB device is registered and the value for **Device Type** is **USB Device**. Identify the stored files by **File Path** and **Last Modified Date Time**, and then investigate the detailed information of the files.

Tip

Information displayed in the **File List** tab is the information of the files stored in the USB device when that USB device was last connected to a computer in your organization. If there is any file stored in that USB device from an external computer, check with the user who lost the USB device about the content of that file.

In addition, to keep a record of the loss of the USB device, register information about the loss in the USB device's hardware asset information.

Register information about the loss.

To prohibit the use of the lost USB device, in the **Hardware Asset** view of the Assets module, change the value for **Asset Status** of the lost USB device to **Disposed**. Then, that USB device is treated as unregistered, and data cannot be read from and written to that USB device through any computer to which the prohibited operation security policy is applied.

Also, in the **Notes** tab, save information such as the date of loss, lost by, and how the device was lost.

Tip

Any problems that can potentially lead to information leakage must be disclosed to all employees, and make sure that all employees are fully aware of good security practices.

Related Topics:

- 11.1.6 Changing the asset status

1.7.8 General procedure for responding to a security audit

In order to perform a security audit on your organization, you need to check such points as whether the environment in your organization complies with the security rules, whether a problem related to security management occurred, and if such a problem occurred, whether the problem has already been corrected.

When you perform security management by using JP1/IT Desktop Management, you can check whether security management is correctly performed, by outputting the following information:

Security policy judgment result
: You can check the status of security policy compliance.

Events related to security management
: You can check problems related to security management that have occurred. If there is no problem with the status of security policy compliance, you can confirm that these problems have already been corrected.

Status of the deterrence of prohibited operation
: You can check whether any prohibited operation is deterred based on the security policy.

List of computers connected to the network
: By creating a list of managed computers, you can check security management target computers.

To respond to a security audit:

1. Output the security policy judgment result.
   Using JP1/IT Desktop Management, output the **Violation Level Status** report in **Security Detail Reports**.
2. Output event data related to security management.
   Using JP1/IT Desktop Management, output event data related to security management.
3. Output the status of the deterrence of prohibited operation.
   Using JP1/IT Desktop Management, output the **Other Access Restrictions Top N** report in **Security Detail Reports**.
4. Output a list of managed computers.
   Using JP1/IT Desktop Management, output a list of managed computers.

Then, submit the above output information at the time of a security audit.

Related Topics:

- 1.7 Managing the security status

(1) General procedure for outputting the security policy judgment result

For a security audit or in a status report to your superior, to present the status of security policy compliance, check and print out the **Violation Level Status** report in **Security Detail Reports**.

1. Check the **Violation Level Status** report.
   To check the status of security policy compliance, display the **Violation Level Status** report in **Security Detail Reports** in the Reports module.
   Check whether the violation level of every device is **Safe**. If there is any device showing a violation level other than **Safe**, click the link of the quantity displayed in the **breakdown**, check the status of the relevant device, and take action, if necessary.
2. Print out the **Violation Level Status** report.
   Output the report by clicking the **Print** button in the **Violation Level Status** report.

Submit the printed report, if necessary.

Related Topics:

- 1.7.2 Taking measures against a security policy violation
- 9.3.1 Adding security policies

(2) General procedure for outputting event data related to security management

For a security audit or in a status report to your superior, to present the status of the occurrence of problems related to security management and the status of problem correction, check and print out the event data related to security management. If there is no problem with the status of security policy compliance, the problems that you can check from the event data are already corrected.

1. Check events related to security management.

   In the Events module, check whether a problem related to security management occurred, or if a problem occurred, check whether the problem has already been corrected.

   Using the filtering function, check events with **Security** displayed for **Type**. If there is any event with **Critical** or **Warning** displayed for **Severity** and **Not Ack** displayed for **Status**, identify the cause from the error details, and then take necessary measures. When you finish taking measures, change the setting for **Status** to **Ack**.

   Tip

   In this case, you need to be operating JP1/IT Desktop Management in such a way that the event status is changed to **Ack** after the problem is corrected.

2. Print out the security management event information.

   Export the security management event information, and then print out the output CSV file.

Submit the printed event information, if necessary.

Related Topics:

- 13.2 Exporting event information
- 13.1 Viewing event details

(3) General procedure for outputting the status of the deterrence of prohibited operation

For a security audit or in a status report to your superior, if you need to show that no prohibited operation has been performed in compliance with the security policy, use the **Other Access Restrictions Top N** report. By using this report in **Security Detail Reports**, you can confirm that any prohibited operation is deterred in compliance with the security policy, and then print out the report.

Tip

To deter any prohibited operation, you need to set the operations to be deterred in a security policy in advance.

1. Check the **Other Access Restrictions Top N** report.

   To check the status of the deterrence of prohibited operation, display the **Other Access Restrictions Top N** report by selecting **Security Detail Reports** in the Reports module and then **Other Access Restrictions Top N**.

   In the **Other Access Restrictions Top N** report, you can check the statuses of printing restriction, blocked software, and external device restriction.

   If the number of occurrences of deterrence is unnaturally large, check whether there is any security problem by inquiring of the relevant user about the circumstances.

2. Print out the **Other Access Restrictions Top N** report.

   Print out the report by clicking the **Print** button in the **Other Access Restrictions Top N** report.

Submit the printed report, if necessary.

Related Topics:

- 9.3.1 Adding security policies

(4) Outputting a list of managed computers

For a security audit or in a report to your superior, to show the security management target computers, output a list of managed computers.

> **Tip**
>
> The default policy is automatically assigned to the managed computers even if a specific security policy is not assigned to them. For this reason, by outputting a list of managed computers, you can present the security management target computers in list form.

In the **Device Inventory** view of the Device module, display only computers by using the filtering function and export the device information of the computers. Then, print out the exported CSV file.

Submit the printed list of the computers, if necessary.

Related Topics:

- 6.17 Exporting device information
- 9.3.1 Adding security policies
- 9.3.5 Assigning security policies

1.8 Checking for the occurrence of information leakage

If information leakage occurs, not only important data in your organization leaks out, but also your organization's social reputation might be ruined.

If any suspicious operation that can lead to information leakage is performed, you need to quickly investigate the situation to see if there is any problem. JP1/IT Desktop Management can detect the occurrence of a suspicious operation and automatically notify you (administrator) of that occurrence by email. Based on the received email, you can investigate the occurred suspicious operation in a timely manner.

Note that information data brought out by an outside intruder can cause information leakage. If such a situation occurs, you need to investigate traces of the information data brought out of a particular computer and quickly check whether there is any problem. Using JP1/IT Desktop Management, you can investigate operation logs collected from each computer, check traces of network connection for a computer brought in from outside, and check the status of the security settings related to illegal access for each computer.

Related Topics:

- 1.8.1 General procedure for investigating a detected suspicious operation
- 1.8.2 General procedure for investigating traces of information being brought out
- 1.7 Managing the security status

1.8.1 General procedure for investigating a detected suspicious operation

To investigate a suspicious operation that can lead to information leakage in a timely manner, you (administrator) need to immediately recognize the occurrence of a suspicious operation and quickly investigate the situation.

To immediately recognize the occurrence of a suspicious operation, by using JP1/IT Desktop Management, set the configuration in such a way as to automatically notify you of a suspicious operation by email if a suspicious operation is detected. Also, according to the operation logs collected from each computer, you can check the location from which the data was brought out and the user who brought out the data first.

To investigate a detected suspicious operation:

1. Set the automatic notification of a suspicious operation.

   Set the configuration in such a way as to notify you of a suspicious operation by email when a suspicious operation is detected.

2. Investigate a suspicious operation.

   If a suspicious operation is detected, check the detected details. If there is any problem, also check operation logs.

You can check whether there is any problem by investigating the details of the detected suspicious operation.

To have JP1/IT Desktop Management detect a suspicious operation, you need to set the configuration in such a way as to collect operation logs and setting the conditions for detection in a security policy.

Related Topics:

- 10.6 Viewing suspicious operation logs

(1) Setting the automatic notification of a suspicious operation

Set the configuration in such a way as to notify you of a suspicious operation by email when a suspicious operation is detected.

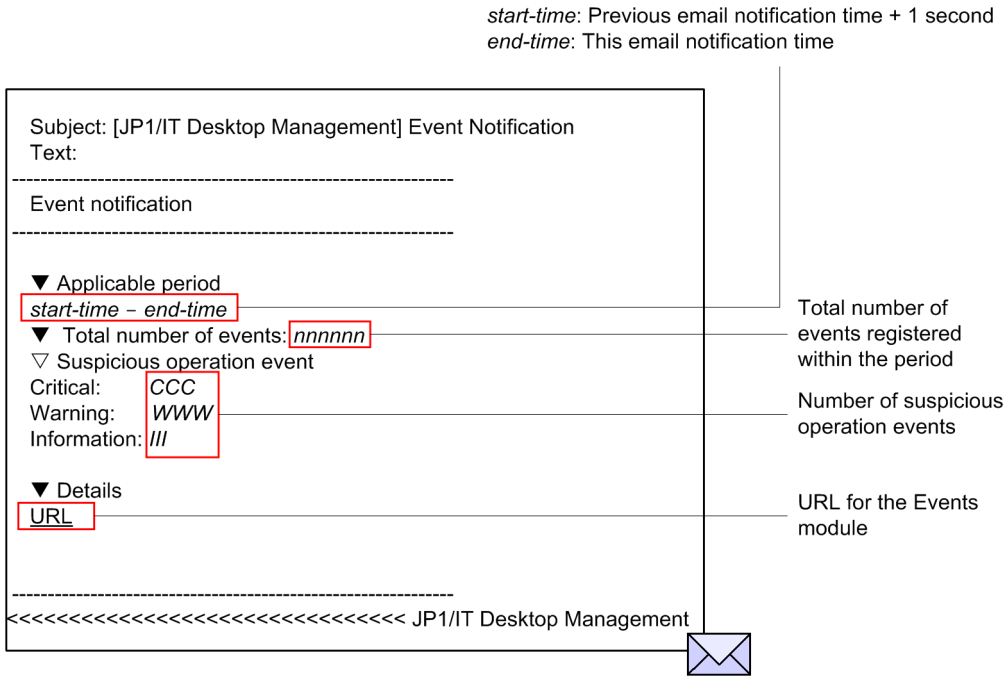
If a suspicious operation is detected, an event with **Suspicious Operation** set for **Type** is generated. Set the configuration in such a way that an email is sent to you when this event is generated.

To set the automatic notification of a suspicious operation:

1. Display the Settings module.
2. In the menu area, select **Events** and then **Event Notifications**.
3. Specify the mail notification target events.
   At this time, select the **Suspicious Operations** check box for each severity.
4. Check the user ID of the mail notification destination.
   If no address is set in the field, select the user ID to set the email address.
5. Click the **Apply** button.

If a suspicious operation is detected and a *Suspicious Operation* event is generated, an email is sent to the specified email address.

The following figure shows the content of an email to be sent:



If you confirm that the event written in the email occurred, start the operation view of JP1/IT Desktop Management from the URL written in the email, check the security status, and take necessary measures.

Related Topics:

- 9.1 Checking the security status

(2) General procedure for investigating a suspicious operation

If a suspicious operation is detected, check the detected details. If there is any problem, also check operation logs.

For a suspicious bringing-out file operation, investigate that suspicious operation by following the procedure described below. For a suspicious printing operation, investigate that suspicious operation by checking operation logs. For details about investigation by checking operation logs, see (1) Checking operation logs.

1. Check the detected details.

   If a suspicious operation is detected, an event with **Suspicious Operation** set for **Type** is generated. For the occurrence status of this event, you can check the number of occurrences for **Suspicious** displayed in the **Not Ack Event Summary** panel of the Home module.

   In the **Not Ack Event Summary** panel, click the number of occurrences enclosed in parentheses to move to the Events module and check events with **Suspicious Operation** for **Type** and **Not Ack** for **Status**.

   Click the link in the **Description** column in the list of events. In the displayed dialog box, you can check the operation log for the detected operation. Based on the details displayed here, judge whether investigation of information leakage is necessary. If you judge that an investigation is necessary, in the list of events, click the link in the **Source** column. You can navigate to the **Operations Logs** view (the **Operation Log List (Distributed Operation Logs)** view for a system where distributed operation logs are obtained) of the Security module, and check the related operation logs.

   Tip

   For a system where both operation logs and distributed operation logs are obtained, you can navigate to the **Operation Log List (Distributed Operation Logs)** view. Note that if the target is a suspicious operation during the time frame in which only operation logs have been obtained, you can navigate to the **Operations Log List** view.

2. Investigate operation logs by data tracing.

   In the **Operations Logs** view (the **Operation Log List (Distributed Operation Logs)** view if distributed operation logs are obtained) of the Security module, you can investigate operation logs by data tracing.

   To investigate operation logs by data tracing, click the **Trace** button for the operation you want to investigate by data tracing, and then check the information in the displayed **Trace Operation Log** dialog box. Note that operation logs with the corresponding **Trace** button disabled are excluded from the investigation targets.

   In the **Trace Operation Log** dialog box, you can check the first and last operations of a series of operations including the selected operation log. For example, if it is detected that a file was copied to a USB device, you can identify which stored data was brought out (first operation) and whether the data was eventually copied to a USB device (last operation). By checking the first and last operations, you can check whether important data was brought out.

An investigation of a suspicious operation by data tracing is complete.

If the investigation finds that information leakage might have occurred, check with the user who performed the suspicious operation about the circumstances, and then consider measures to be taken.

1.8.2 General procedure for investigating traces of information being brought out

If information might have been brought out, you need to investigate traces of the information and quickly check whether there is any problem.

Using JP1/IT Desktop Management, you can check the following points: whether there are any traces of each computer being operated, whether an unknown device is connected to the network, and whether the security settings related to illegal access are specified for each computer.

To investigate traces of information being brought out:

1. Check operation logs.

   By checking operation logs collected from each computer, you can check the operation status of each computer. If you find any trace of a third party login or any suspicious bringing-out operation, you need to identify the brought out data by checking operation logs, and then consider measures to be taken.

2. Check a newly connected device.

   If an unknown device is connected to the network in your organization, information might leak out of that device. By searching the network, you can check whether there is any device newly connected to the network in your organization.

3. Check the security settings of computers.

   If a computer is vulnerable to illegal access, that computer might be manipulated by a third party and information leakage might occur. Check the security settings of the managed computers, and then take necessary measures if there is any problem.

By following the above procedure, you can check whether there are any traces of information being brought outside.

(1) Checking operation logs

By checking operation logs collected from each computer, you can check the operation status of each computer. If you find any trace of a third party login or any suspicious bringing-out operation, you need to identify the brought out data by checking operation logs, and then consider measures to be taken.

You can check operation logs in the **Operations Log List** view, which is displayed by selecting **Operations Logs** in the Security module and then **Operations Log List**. You can check distributed operation logs in the Extraction Results view, which is displayed by selecting **Operation Log List (Distributed Operation Logs)** and then **Extraction Results**.

You need to investigate the collected operation logs by data tracing, one by one. We therefore recommend that you narrow down target operation logs from several view points for investigation. For example, if information might have been brought out, check operation logs from the following view points to investigate operation logs:

Check the operation logs during the time frame in which the relevant operation was performed.

If you already know the time frame in which the operation related to bringing-out occurred, you can efficiently check operation logs by narrowing down based on that time frame. In the list of operation logs, specify the value for **Operation Time (Source)** and the time frame as the filtering conditions to narrow down operation logs to be checked, along the time axis.

Check operation logs by limiting the type of operation.

By narrowing down to operations related bringing-out, you can efficiently check operation logs. Using the filtering function in the list of operation logs, specify, for example, the following conditions:

- **Operation Type** is **File Operation**, **Print Operation**, or **External Device Operation**.
- **Operation Type (Detail)** is **Logon**, **Copy file**, **Web Access (Upload)**, **FTP (Send File)**, or **Attach External Device**.

Check operation logs based on the computer from which data was brought out.

You can check whether data was brought out from a specific computer such as the server where important data is stored and NAS. In the list of operation logs, specify the value for **Source** and the computer name to check whether information was brought out from a specific computer.

If the result of checking finds that information might have been brought out, check with the user of the computer for which the operation logs were obtained about the circumstances, and then consider measures to be taken.

(2) Checking a newly connected device

If an unknown device is connected to the network in your organization, information might leak out of that device. By searching the network, you can check whether there is any device newly connected to the network in your organization.

To view the search results, in the Settings module, select **Discovery**, **Last Discovery Log**, and then **IP Address Range** to display the IP Address Range view.

Check whether there is any unknown device in the devices displayed in the **IP Address Range** view. In the list of **Last Discovery Log**, use the **Newly Discovered** filter to quickly check a newly connected device.

If you find any unknown device, check it based on its network address.

Related Topics:

- 6.4 Searching for devices connected to the network

(3) Checking the security settings of computers

If a computer is vulnerable to illegal access, information leakage might occur. Check the security settings of the managed computers, and then take necessary measures if there is any problem.

Check the status of the security settings of computers in the **Device List** view, which is displayed by selecting **Computer Security Status** in the Security module and then **Device List**. A computer with the violation level **Critical**, **Important**, or **Warning** might have a problem with its security settings. By selecting the device you want to check in the **Device List** view and then selecting the **OS Security Settings** tab or the **User-Defined Security Settings** tab, you can check whether the status of each security configuration item is safe.

If you find any security configuration item that is not safe, you can forcibly change the setting to take necessary measures. Click the **Enforce** button. In the displayed dialog box, select the item for which you want to take security measures, and then click the **OK** button.

Tip

You can also check the status of security settings in the detailed security report. To display the detailed security report related to the security settings, in the Reports module, select **Security Detail Reports** and then **Security Settings Status**.

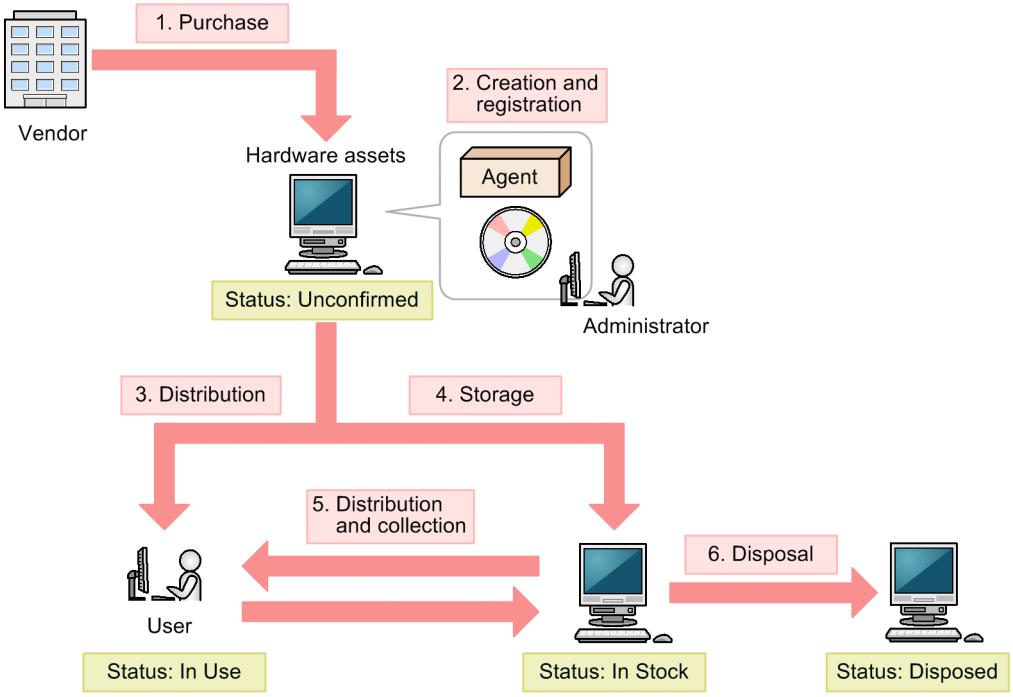
1.9 Managing hardware assets

There are various hardware assets used for work in your organization such as computers, servers, smart devices, printers, network devices, and USB devices. You need to keep track of the status of hardware assets to cope with periodical device replacement according to the operation in your organization and with sudden problems.

By using JP1/IT Desktop Management, you can do the following to efficiently manage hardware assets:

- Keep track of the owned assets in list form just like a ledger.
- Easily keep track of the status of assets by using graphical views such as panels and reports.
- Quickly obtain information about the hardware asset you want to work on by using the filtering function.

You can perform hardware asset management operations in the **Hardware Asset** view of the Assets module. To manage hardware assets, register hardware asset information, and then maintain the information by following the procedure for managing hardware assets. The following figure shows how to manage hardware assets:



Legend:
Agent: Agent

After purchasing a hardware asset, build a hardware asset environment, and then register hardware asset information about that asset. Then, distribute the hardware asset to users. If you do not use the hardware asset, store it as a stock item. According to operations such as replacement and rental of a substitute device, collect a hardware asset in use or distribute a hardware asset in stock. Discard and dispose of any unwanted hardware assets.

This section explains how to use JP1/IT Desktop Management in the following operations:

Purchase devices.

Purchase new devices in your organization due to increase of employees and addition of equipment. Register information about purchased devices in JP1/IT Desktop Management so that you can manage them as assets.

Replace devices.

Replace devices in your organization due to relocation of employees or renewal of devices.

Take inventory of devices.

Take inventory of devices in your organization.

Check devices that are not used.

Check redundant assets in your organization.

Discard devices.

Collect old devices from workplaces, and then discard those devices.

Respond to a device failure.

When a failure occurs on a device in your organization, request the maintenance service company for repair or lend a substitute device.

Related Topics:

- 1.9.3 General procedure for purchasing devices
- 1.9.4 General procedure for replacing devices
- 1.9.5 General procedure for taking inventory of devices
- 1.9.6 General procedure for checking devices that are not used
- 1.9.7 General procedure for discarding devices
- 1.9.8 General procedure for handling a device failure

1.9.1 Registering information contained in a management ledger

By importing a management ledger, you can collectively register hardware asset information.

1. Prepare a CSV file to be imported.

   To import asset information, convert data contained in the management ledger into a CSV file.

2. Import the management ledger.

   By importing the management ledger, you can register information contained in the management ledger as hardware asset information. For details about how to import asset information, see 11.4.1 Importing hardware asset information.

   When importing asset information, associate the items used in the management ledger with the asset management items used in JP1/IT Desktop Management. By this association, you can import all information contained in the management ledger to the asset management items in JP1/IT Desktop Management.

   Tip

   Without changing the order of items and the item names used in the management ledger, you can associate the items in the management ledger with the asset management items. If some item in the management ledger does not correspond to any asset management item, you can create a new asset management item and associate the item in the management ledger with the new asset management item when importing information.

   If some device has been included as management targets of JP1/IT Desktop Management in advance, the device information about that device is collected and the hardware asset information of that device is automatically registered.

   To import information, specify the value for **Mapping Key** that associates information to be imported with registered hardware asset information. When you perform an import, an existing entry of the hardware asset information in JP1/IT Desktop Management is updated if that entry has the mapping key that matches the mapping key of any entry

in the management ledger. If an entry in the management ledger has the mapping key that does not match the mapping key of any existing entry of the hardware asset information, that entry is registered as a new entry of the hardware asset information.

You can select a mapping key from the items described below. Specify the item that can uniquely identify a hardware asset.

- Asset management number
- Serial number#
- IP address
- MAC address
- Host name
- IMEI
- Contract phone number

#: BIOS information serial number

> **Important note**
>
> To specify an item as a mapping key, select an item for which a value exists both in JP1/IT Desktop Management and in the management ledger to be imported. For example, if **Serial #** appears in the management ledger but no value for **Serial #** is registered as hardware asset information, entries imported from the management ledger cannot be associated with entries of the hardware asset information correctly. In this case, all hardware assets in the management ledger are registered as new entries of the hardware asset information.

3. Check the imported result.

After importing information, in the **Hardware Asset** view of the Assets module, check whether information contained in the management ledger has been correctly registered as hardware asset information.

When you intend to update the registered entries of the hardware asset information, some entry of the hardware asset information with **Unconfirmed** set for **Asset Status** might exist after you import the entries in the management ledger. In this case, the relevant asset might not be registered in the management ledger or the mapping key of that entry might not match the mapping key of any entry in the management ledger.

For the relevant asset whose information is not registered in the management ledger, manually register the asset information of the relevant asset. In the case of an unmatched mapping key, the entry in the management ledger that is supposed to correspond to the entry of the hardware asset information with the unmatched mapping key is registered as a new hardware asset. Therefore, check and change the correspondence between the relevant hardware asset information and the device, and then delete the unnecessary information.

The import operation is complete, and the information contained in the management ledger is registered in the hardware asset information.

After you finish registering hardware asset information, maintain asset information according to the operation in your organization. Note that when hardware asset information is associated with device information, **Inventory Information** of hardware asset information is automatically updated based on the collected device information.

Related Topics:

- 11.1.14 Changing the device information associated with the hardware asset information
- 1.9.2 Maintaining hardware asset information

1.9.2 Maintaining hardware asset information

Maintain hardware asset information according to the operation in your organization and keep the information up-to-date. To maintain hardware asset information, there are three methods described below.

> **Tip**
>
> When hardware asset information is associated with device information, **Inventory Information** of hardware asset information is automatically updated based on the collected device information.

Collectively edit hardware asset information by using the import function.

By importing a hardware asset information CSV file, you can collectively update hardware asset information.

You can create a hardware asset information CSV file by exporting hardware asset information. To update hardware asset information, edit and import the output CSV file.

For details about how to export hardware asset information, see 11.5 Exporting asset information. For details about how to import hardware asset information, see 11.4.1 Importing hardware asset information.

> **Important note**
>
> To export hardware asset information, you need to export one or more items (items to be used as mapping keys) that can uniquely identify hardware asset information during import. The items to be used as mapping keys are **Asset #**, **Serial #**, **IP Address**, **MAC Address**, **Host Name**, **IMEI**, and **Contract Phone**.

Edit hardware asset information manually.

To manually register hardware asset information, in the **Hardware Asset** view of the Assets module, select the asset that you want to register as hardware asset information, and then click the **Edit** button. You can register the asset information of the selected asset in the displayed dialog box. You can also select multiple assets and then collectively register information about them.

For details about how to manually edit hardware asset information, see 11.1.2 Editing hardware asset information.

Automatically update hardware asset information by collecting user information.

For a computer managed online, if hardware asset information is associated with the device information of the managed computer, you can display the **End User Form** view on the computer to collect information entered by the user. For a computer managed offline, you can display the **End User Form** view on the target computer when you collect the device information by executing the `getinv.vbs` command. Note that you need to install an agent on the target computer to display the **End User Form** view on it.

The following information can be collected:

- Department
- Installation location
- User name
- Account
- Email address
- Phone number
- Management items optionally added

By collecting information entered by the user, you can save yourself (administrator) the effort of maintaining asset information. For example, by operating JP1/IT Desktop Management in such a way that each user in your organization periodically enters the latest information, you can keep track of the latest user information without

maintaining any user information. Even when a large number of users are relocated to different departments, you do not need to maintain large amounts of user information.

Note that you can also delete hardware asset information that does not need to be managed anymore. For details about how to delete hardware asset information, see 11.1.3 Removing hardware asset information.

Related Topics:

- 11.1.4 Setting the display interval for the **End User Form** view in the Assets module
- 11.1.6 Changing the asset status

1.9.3 General procedure for purchasing devices

When you introduce new devices in your organization due to increase of employees and addition of equipment, register the devices and then start managing the devices as assets.

To purchase new computers and start asset management of them by using JP1/IT Desktop Management:

1. Purchase new devices.

   Research the specifications and price of computers to be purchased and consider the quantity of computers to be purchased. In addition, obtain information about the expected computer users (departments, installation locations, user names, and others).

2. Register the asset information of the devices.

   When you purchase computers, before distributing them to the users, install an agent on each of them so that each computer is included as a management target of JP1/IT Desktop Management.

   When you connect a computer on which an agent is installed to the network, the device information of that computer is automatically registered.

   In addition to the device information, the hardware asset information is registered at the same time. Then, manually register the computer user information that you have obtained in advance.

3. Distribute the devices.

   Using JP1/IT Desktop Management, output the information of the destinations to which you distribute the computers. Based on the output information, distribute the computers.

After you finish distributing the computers, start asset management by using JP1/IT Desktop Management.

(1) Purchasing new devices

When you introduce new computers in your organization due to increase of employees and addition of equipment, make a purchase plan in advance. In addition, to identify the expected users of new computers, obtain user information.

Make a purchase plan.

Before purchasing computers, make a purchase plan. For example, consider the following items:

- Contract type (purchase, rental, lease, and others)
- Purpose (general OA, development, special purpose, and others)
- Specifications
- Price
- Quantity

Tip

To check the specifications of the recently purchased computers, in the Assets module, select **Overview** and then **Dashboard** to display the Dashboard view. In the Dashboard view, find the **Customized HW Assets (Group/Filter)** panel, and then click the **Registered Assets (last 6 months)** link. Use this information as a reference when you purchase computers.

Obtain user information.

Obtain, in advance, user information that is required when you register computers. Obtain the following information from the user:

- Department
- Installation location
- User name
- Email address
- Phone number

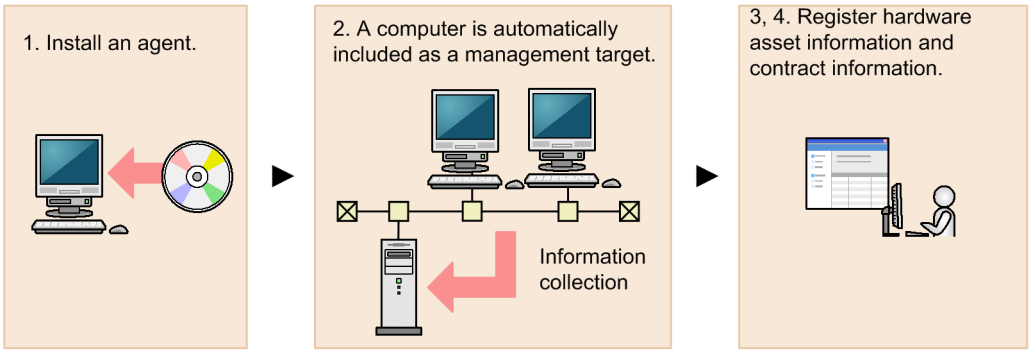
After purchasing computers, register the obtained user information in JP1/IT Desktop Management.

When you have determined the computers to purchase, place an order with the vendor.

(2) General procedure for registering the asset information of devices

When you purchase new computers, before distributing them to the users, install an agent on each of them so that each computer is included as a management target of JP1/IT Desktop Management. After including the computers as management targets, register the hardware asset information and contract information of the computers.

The figure below shows a general procedure for the above operation. Perform the operation described here by using the network for system management purpose.



1. Install an agent.

Install an agent on each computer to include the computer as a management target of JP1/IT Desktop Management.

Tip

Install an agent on a model machine in which an environment has been created in advance, and then copy the contents of a hard drive of the model machine to a hard drive of other computers. This copy method can save you the effort of building an environment on each computer.

2.Include the computers as management targets of JP1/IT Desktop Management.

When you connect the computers on which an agent is installed to the network, these computers are automatically included as management targets and information collected from these computers is displayed in the **Device Inventory** view of the Device module. In addition, the information of these computers is automatically registered as new hardware asset information in the **Hardware Asset** view of the Assets module.

3. Register hardware asset information.

Unconfirmed is displayed for **Asset Status** for the automatically registered hardware asset information. In addition, only the information collected from the computers is registered as the hardware asset information. Therefore, manually register information that is not automatically collected from the computers such as **Asset #** and **Asset Status** (In Use, In Stock, and others), and user information.

Tip

You can also ask each user to enter user information in the End User Form view.

4. Register contract information.

For a contract hardware asset, register contract information in the **Contracts** view of the Assets module.

By setting the contract target hardware asset when registering contract information, you can manage the cost and contract period of that hardware asset.

Tip

When you use a bar-code reader, create an asset management number sticker for your bar-code reader, and then attach the sticker to each computer. When you take inventory of computers, read the sticker attached to each computer by using a bar-code reader to efficiently perform a physical inventory count.

Tip

You can also register only hardware asset information manually in advance and register device information later by connecting a computer to the network. For example, import a list of hardware asset information containing serial numbers, and then register only hardware asset information in advance. When the user connects the distributed computer to the network, the device information is collected. If the serial number of the collected device information is identical to the serial number of the exiting hardware asset information, the collected device information is associated with the exiting hardware asset information and registered as hardware asset information.

Now you finish registering necessary information. After registering necessary information, distribute the computers to the users. If there is any computer you want to store as a stock item, move that computer to the storage location.

Related Topics:

- 1.1 Installing agents
- 11.1.2 Editing hardware asset information
- 6.14 Obtaining user information
- 11.3.1 Adding contract information
- 11.4.1 Importing hardware asset information

(3) General procedure for distributing devices to users

After registering information of the purchased computers in JP1/IT Desktop Management, distribute the purchased computers to the users. Before distribution, create a list of computers, and then distribute the computer to each user according to that list.

1. Create a list of computers to be distributed.

   To distribute the computers to the users, create a list of the computers to be distributed. Export the hardware asset information of the computers to be distributed to a CSV file. Make sure that you export all the hardware asset information items that you need to distribute computers to users. For example, export **Asset #** that identifies each computer to be distributed, **Department** and **Location** that identify the locations to which to distribute computers, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently distribute computers to users. To sort the hardware asset information items, click an item name in the operation view.

2. Distribute the computers.

   Using an exported list of computers, distribute computers to appropriate users. If you are asking delivery companies to deliver computers to users, give them the list and ask them to use the list when they deliver the computers. By having users put their signatures on the list when they receive a computer, you can confirm later that the computers have been delivered to all destinations.

After you finish distributing the computers, start asset management by using JP1/IT Desktop Management. When new tasks arise, update the hardware asset information as necessary to keep it up to date.

Tip

When hardware asset information is associated with device information, **Inventory Information** of hardware asset information is automatically updated based on the collected device information.

Related Topics:

- 11.5 Exporting asset information
- 11.4.1 Importing hardware asset information
- 11.1.2 Editing hardware asset information

1.9.4 General procedure for replacing devices

If you need to replace the devices used in your organization due to relocation of employees or renewal of devices, by using JP1/IT Desktop Management, identify the devices to be replaced, distribute new devices, and then collect old devices.

To replace devices:

1. Make a device replacement plan.

   Use JP1/IT Desktop Management to identify the devices that need to be replaced. After determining the devices to be collected for replacement, prepare replacement devices.

2. Distribute new devices to users.

   Using JP1/IT Desktop Management, output information about the locations to which to distribute new devices. Use the output information to distribute a new device to each applicable user.

   After distributing new devices to users, instruct users to transfer the data stored in an old device to a new one.

3. Collect old devices from user.

   When users have transferred the data stored in an old device to a new one, ask users to return the old devices.

   Using JP1/IT Desktop Management, output information about the locations from which to collect old devices. Use the output information to collect an old device from each applicable user.

The replacement of devices is complete.

(1) General procedure for planning the replacement of smart devices

If you need to replace the devices used in your organization due to relocation of employees or renewal of devices, identify the devices that need to be replaced, determine the devices to be replaced, and then prepare replacement devices. In addition, notify the users in advance about the replacement.

1. Determine the devices to be replaced.

   In the **Hardware Asset** view of the Assets module, identify if there are any devices that need to be replaced. For example, if there is a policy to replace any devices that have been used for three years or more, use the filtering function to identify devices whose **Registered Date/Time** is over three years ago.

   > **Tip**
   >
   > By saving frequently used filtering conditions, you can save the effort of specifying the filtering condition every time you have to identify devices that need to be replaced. To apply the saved filtering condition to a list, select a filtering condition in the menu area.

   If you find devices that need to be replaced, access the **Hardware Asset** view of the Assets module, set **Planned Asset Status** to **In Stock**, and then enter the date of collection under **Planned Date**. In this way, you can identify devices that are due to be collected.

2. Prepare replacement devices.

   Prepare replacement devices to be distributed to users.

   - To distribute in-stock devices to users:

     In the **Hardware Asset** view of the Assets module, identify devices whose **Asset Status** is **In Stock**. To limit the information to be displayed in the view, use the filtering function. Check the specifications of the identified devices. If you do not find any problems in the specifications, set **Planned Asset Status** to **In Use** and enter the date of distribution under **Planned Date**. In this way, you can identify devices that are due to be distributed.

   - To distribute newly purchased devices to users:

     After purchasing new devices, include them as the management targets of JP1/IT Desktop Management, and then register both the hardware asset information and contract information for each device. Set **Planned Asset Status** to **In Use** and enter the date of distribution under **Planned Date**. In this way, you can identify devices that are due to be distributed.

3. Notify each user about the replacement.

   To facilitate the replacement processing, inform applicable users about the reason why their devices need to be replaced and the date on which the devices are to be replaced.

Preparation for replacement of devices is complete.

Related Topics:

- 11.1.7 Changing the planned asset status
- 1.9.3 General procedure for purchasing devices

(2) General procedure for distributing new devices to users

After preparing for replacement, create a list of new devices to be distributed to users. Using the created list, distribute the new devices to users. After distributing the new devices to users, update the hardware asset information.

1. Create a list of devices to be distributed.

   Before distributing devices to users, create a list of devices to be distributed. Export the hardware asset information whose **Planned Asset Status** is **In Use** to a CSV file. Make sure that you export all the hardware asset information items that you need to distribute devices to users. For example, export **Asset #** that identifies each device to be distributed, **Department** and **Location** that identify the locations to which to distribute devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently distribute devices to users. To sort the hardware asset information items, click an item name in the operation view.

2. Distribute the devices.

   Using an exported list of devices, distribute devices to appropriate users. If you are asking delivery companies to deliver devices to users, give them the list and ask them to use the list when they deliver the devices. By having users put their signatures on the list when they receive a device, you can confirm later that the devices have been delivered to all destinations.

3. Update the hardware asset information.

   After distributing the new devices to users, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change the **Asset Status** of each distributed device from **In Stock** to **In Use**. In addition, update **Department**, **Location**, and user information.

The distribution of devices is complete. Instruct users to transfer the data stored in an old device to a new one.

Related Topics:

- 11.5 Exporting asset information
- 11.1.6 Changing the asset status

(3) General procedure for collecting the devices that are no longer in use

If you want to put the devices that are no longer in use back in stock, collect them when the planned date of collection arrives. Before collecting the devices from users, create a list of devices to be collected. Using the created list, collect the devices from users. After collecting the devices from users, update the hardware asset information. Also, transfer the software licenses assigned to the collected devices to other devices if transferring of these software licenses is permitted.

Tip

In **Hardware Asset Status (Planned)** on the Summary Reports, you can check the number of devices that are due to be collected from users (devices whose **Planned Asset Status** is **In Stock**). You can also send a summary report by email.

Tip

To facilitate the collection processing, we recommend that you notify the users of devices to be collected in advance about the reason for collecting the device and the planned date of collection.

1. Create a list of devices to be collected.

   Before collecting devices from users, create a list of devices to be collected. Export the hardware asset information whose **Planned Asset Status** is **In Stock** to a CSV file. Make sure that you export all the hardware asset information items that you need to collect the devices from users. For example, export **Asset #** that identifies each device to be collected, **Department** and **Location** that identify the locations from which to collect devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently collect devices from users. To sort the hardware asset information items, click an item name in the operation view.

2. Collect old devices from user.

   Use the exported list to collect the devices from users. If you are asking delivery companies to collect devices from users, give them the list and ask them to use the list when they collect the devices from users.

   After collecting all the devices from users, check the collected devices against the information in the exported list to confirm that all the devices have been collected from users.

3. Update the hardware asset information.

   After collecting devices from users, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change the **Asset Status** of each collected device from **In Use** to **In Stock**. In addition, specify the location where the collected devices are stored in **Location**, and change **Department** and user information for the collected devices so that a system administrator is now in charge of these devices.

4. Transfer the software licenses to other devices.

   To effectively use the software licenses assigned to the collected devices, transfer such software licenses to other devices.

   Tip

   If you do not transfer these software licenses to any devices, cancel the assignment of these software licenses.

The collected devices are managed as in-stock devices.

Related Topics:

- 15.7.2 Setting recipients of summary reports
- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information

- 11.1.6 Changing the asset status
- 11.2.13 Transferring software licenses
- 11.2.12 Allocating software licenses to computers

1.9.5 General procedure for taking inventory of devices

To manage the assets used in your organization, you need to take inventory on regular basis to keep accurate inventory records. For this purpose, you need to register the physical inventory records in JP1/IT Desktop Management, so that you can easily identify the devices for which a physical inventory has not been conducted.

To take inventory of devices:

1. Conduct a physical count.

   Create a list of hardware asset information, and then perform a physical count of the inventories found in your organization.

2. Update the information with the physical inventory records.

   To manage the status of the device inventory, update the information in JP1/IT Desktop Management with the physical inventory records.

3. Investigate the devices for which a physical inventory has not been conducted.

   Identify the devices for which a physical inventory has not yet been conducted to investigate the usage status of the devices. Update the information in JP1/IT Desktop Management with the information of the devices found during the investigation.

Now the information in JP1/IT Desktop Management is updated with the physical inventory records of the devices.

Tip

If you use a bar-code reader for inventory of devices, you can perform a physical count of devices and update the information with the results more easily.

Related Topics:

- 11.1.11 Taking stock by using a barcode reader

(1) General procedure for performing physical inventory count

To perform a physical inventory count of the devices, output a list of hardware asset information, and then check the devices against the list.

1. Export a list of hardware asset information.

   Create a list of hardware asset information for physical inventory count. In the **Hardware Asset** view of the Assets module, export the hardware asset information to a CSV file. To identify devices, export the items such as **Asset #**, **Last Tracked Date**, **Department**, **Location**, and **User Name**. You will use the exported CSV file when you update the information in JP1/IT Desktop Management with the result of physical inventory count. Make sure that you export the **Asset #** and **Last Tracked Date** items.

Tip

When you export the hardware asset information items, sort them by **Department** and **Location** so that you can easily check devices against a list. To sort the hardware asset information items, click an item name in the operation view.

2. Perform a physical inventory count based on the list of hardware asset information.

   Perform a physical inventory count based on the exported list. When you have completed the inventory count, place a checkmark next to the corresponding device on the list. Update the stocktaking date for the devices with a checkmark by using JP1/IT Desktop Management.

Now the physical inventory count is complete, and the list of devices with the inventory results has been prepared.

Related Topics:

- 11.5 Exporting asset information

(2) General procedure for updating the information with the physical inventory records

To manage the status of the device inventory, update the information in JP1/IT Desktop Management with the physical inventory records. When you have updated the information with the physical inventory records, the values for **Last Tracked Date** of hardware asset information are updated in the **Hardware Asset** view of the Assets module.

1. Create a CSV file that contains the updated stocktaking dates.

   To collectively update the stocktaking dates, create a hardware asset information CSV file that contains the updated stocktaking dates. Edit the CSV file used in the physical inventory count to update the values for **Last Tracked Date** of the devices for which the physical inventory count has been confirmed.

   Tip

   If the hardware asset information such as **Department**, **Location**, and **User Name** has been changed since the last inventory count, edit the CSV file to update the corresponding values in addition to the values for **Last Tracked Date**.

2. Update the stocktaking dates.

   After you have created the hardware asset information CSV file, import it to collectively update the stocktaking dates.

For the devices for which the physical inventory count has been confirmed, the values for **Last Tracked Date** of the hardware asset information are updated.

Tip

If you want to check the hardware assets that you have in hand one by one, manually update the stocktaking date for each asset.

Tip

You can automatically update a value for **Last Tracked Date** with the value for **Last Alive Confirmation Date/Time** of a device or the date on which a user finished entering all the items in the **End User Form** view.

Related Topics:

- 11.1.8 Manually updating a stocktaking date
- 11.1.10 Setting automatic update for the stocktaking date

(3) General procedure for inspecting devices for which physical inventory has not been completed

You need to inspect the usage status and perform a physical inventory count again for the devices for which a physical inventory count has not been completed.

1. Inspect the devices for which the physical inventory has not been completed.

   In the **Hardware Asset** view of the Assets module, identify the hardware asset information of the devices whose **Last Tracked Date** has not been updated. Using the filtering function, display the hardware asset information of the devices whose **Last Tracked Date** is older than the latest stocktaking date.

2. Export a list of hardware asset information.

   Create a list of hardware asset information for inspection. Export the hardware asset information of the devices whose stocktaking date has not been updated to a CSV file. To identify devices, export the items such as **Asset #**, **Department**, **Location**, and **User Name**.

   Tip

   When you export the hardware asset information items, sort them by **Department** and **Location** so that you can easily check devices against a list. To sort the hardware asset information items, click an item name in the operation view.

3. Check with the users of the relevant devices about the circumstances.

   After creating a list of hardware asset information, check with the users of the devices about the location of each device.

   If the devices are found

   Make a note on the list to indicate that the physical inventory count has been successfully completed for the devices. Make a correction to the hardware asset information at the same time, if necessary.

   If the devices are not found

   The devices might be lost. Check with the users about the circumstances. If you have confirmed that the devices have been lost, change the value for **Asset Status** of the relevant devices to **Disposed**. Also, enter comments in the **Notes** tab, describing the remarks such as reason or date and time of loss.

4. Update the information with the physical inventory records.

   Update the information in JP1/IT Desktop Management with the results for the devices for which the physical inventory count has been completed.

Now you finish taking inventory of devices.

Related Topics:

- 11.5 Exporting asset information

- (2) General procedure for updating the information with the physical inventory records
- 1.9.7 General procedure for discarding devices

1.9.6 General procedure for checking devices that are not used

To efficiently manage assets, check the usage status of devices and collect devices that are not used.

To collect devices that are not used:

1. Investigate the usage status of devices.

   To find devices that are not used, narrow down devices that are managed by JP1/IT Desktop Management based on the updated date, and then identify devices whose information has not been updated for a certain period of time. Check with the users of devices whose information has not been updated about the necessity and usage status of these devices.

2. Collect devices.

   Among the devices whose usage status you have checked, collect the devices that are not needed so much.

   Make a collection plan, and then inform the users that their devices are due to be collected. When the planned date of collection arrives, collect the devices.

The collected devices become in-stock devices. Manage the assets efficiently by distributing any of the collected devices, if necessary.

(1) Checking the usage status of devices

To find devices that are not used, check the last modified date and time of the device information. For devices that are not used for a long period of time, check with the users about the usage status of these devices to judge whether to collect these devices.

1. Check devices that are not used.

   In the **Device Inventory** view of the Device module, narrow down device information based on **Last Modified Date/Time**. For example, to identify any devices that are not used for a long period of time, create a filter to display any devices with the date for **Last Modified Date/Time** of device information being 31 or more days ago.

   Inform the users of the devices that their devices have not been used, and then check with the users about the necessity and usage status of the devices.

   Tip

   In the **Customized Device Inventory (Group/Filter)** panel displayed in the Dashboard view, which is displayed by selecting **Overview** in the Device module and then **Dashboard**, you can check the number of managed devices by created filters or custom groups. If you want to quickly identify device information, we recommend that you use this panel.

2. Judge whether to collect the devices.

   After checking the usage status and finding that the devices are not needed so much, make a device collection plan. In addition, if the device information of the devices has not been updated due to some error, investigate the cause of that error and take necessary measures.

3. Set the planned date of device collection.

   In the Assets module, set the planned date of device collection for the devices that you judged as being not used. Change the value for **Planned Asset Status** to **In Stock** and enter the planned date for collecting devices in **Planned Date**.

   Tip

   When you set the planned date of device collection, we recommend that you sort the entries in the asset list by **Location** or **Department**. You can collect devices efficiently by setting the same date for the planned date of device collection for the devices located in the same place.

You can check the devices that are not used and identify the devices to be collected.

Tip

You can change the update interval of device information by using the agent configuration applied to each device. To create an agent configuration, display the Agent Configurations view by selecting **Agent** in the Settings module and then **Agent Configurations**.

Related Topics:

- 11.1.7 Changing the planned asset status
- 15.3.1 Managing agent configurations

(2) General procedure for collecting the devices that are no longer in use

If you want to put the devices that are no longer in use back in stock, collect them when the planned date of collection arrives. Before collecting the devices from users, create a list of devices to be collected. Using the created list, collect the devices from users. After collecting the devices from users, update the hardware asset information. Also, transfer the software licenses assigned to the collected devices to other devices if transferring of these software licenses is permitted.

Tip

In **Hardware Asset Status (Planned)** on the Summary Reports, you can check the number of devices that are due to be collected from users (devices whose **Planned Asset Status** is **In Stock**). You can also send a summary report by email.

Tip

To facilitate the collection processing, we recommend that you notify the users of devices to be collected in advance about the reason for collecting the device and the planned date of collection.

1. Create a list of devices to be collected.

   Before collecting devices from users, create a list of devices to be collected. Export the hardware asset information whose **Planned Asset Status** is **In Stock** to a CSV file. Make sure that you export all the hardware asset information items that you need to collect the devices from users. For example, export **Asset #** that identifies each device to be collected, **Department** and **Location** that identify the locations from which to collect devices, and **User Name**, **E-mail**, and **Phone** that allow you to contact users.

Tip

When you export the hardware asset information items, sort them by **Department** and **Location** so that you can efficiently collect devices from users. To sort the hardware asset information items, click an item name in the operation view.

2. Collect old devices from user.

   Use the exported list to collect the devices from users. If you are asking delivery companies to collect devices from users, give them the list and ask them to use the list when they collect the devices from users.

   After collecting all the devices from users, check the collected devices against the information in the exported list to confirm that all the devices have been collected from users.

3. Update the hardware asset information.

   After collecting devices from users, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change the **Asset Status** of each collected device from **In Use** to **In Stock**. In addition, specify the location where the collected devices are stored in **Location**, and change **Department** and user information for the collected devices so that a system administrator is now in charge of these devices.

4. Transfer the software licenses to other devices.

   To effectively use the software licenses assigned to the collected devices, transfer such software licenses to other devices.

Tip

If you do not transfer these software licenses to any devices, cancel the assignment of these software licenses.

The collected devices are managed as in-stock devices.

Related Topics:

- 15.7.2 Setting recipients of summary reports
- 11.5 Exporting asset information
- 1.9.2 Maintaining hardware asset information
- 11.1.6 Changing the asset status
- 11.2.13 Transferring software licenses
- 11.2.12 Allocating software licenses to computers

1.9.7 General procedure for discarding devices

If devices collected for replacement or repair are too old or damaged to be reused, discard these devices.

To discard devices:

1. Determine the devices to be discarded.

   If the collected devices are no longer to be used, set them as the devices to be discarded. To prevent information leakage, erase all data stored in the disk of the devices to be discarded.

2. Dispose of the devices.

   When the planned date of disposal arrives, dispose of the applicable devices.

The unwanted devices are disposed of and the discard operation is complete.

Related Topics:

- 1.9.4 General procedure for replacing devices

(1) General procedure for determining the devices to be discarded

If devices collected for replacement or repair are too old or damaged to be reused, set them as the devices to be discarded. If the collected devices are still usable, keep them in stock.

1. Identify the devices that are no longer to be used.

   Check the collected devices for any devices that are no longer to be used.

   For example, if there is a policy to discard any devices that have been used for five years or more, check how long the collected devices have been used. To do this, access the **Hardware Asset** view of the Assets module, and then check **Registered Date/Time** or **Contract Date** of the collected devices. To limit the information to be displayed in the view, use the filtering function.

   If neither **Registered Date/Time** nor **Contract Date** is displayed in the view, right-click an item name in the list, and then select **Select Columns**. In the displayed dialog box, select the **Registered Date/Time** or **Contract Date** check box, and then click the **OK** button. **Registered Date/Time** or **Contract Date** is then displayed in the view. If no contract information is registered for hardware assets, **-** is displayed under **Contract Date**.

2. Set as the devices to be discarded.

   If there are devices that are no longer to be used, set **Planned Asset Status** to **Disposed**, and then enter the planned date of disposal under **Planned Date**. In this way, you can identify devices that are due to be discarded.

3. Clear all data stored in the hard disk.

   To prevent information leakage, erase all data stored in the hard disks of the devices to be discarded by using a tool specifically designed for this purpose.

   If you are discarding the smart devices, initialize them. To initialize the smart devices, click the **Go to Device List** button in the **Hardware Asset** view to display the Device module, and then from **Action**, select **Initialize Smart Device**.

   If you are keeping the smart devices in stock, make a disk copy of them so that they can be put to use without delay when necessary.

The devices to be discarded are ready for disposal at any time.

Related Topics:

- 11.1.7 Changing the planned asset status
- 1.11 General procedure for managing asset contract information

(2) General procedure for disposing of devices

When the planned date of disposal arrives, dispose of all devices that are no longer to be used. Before disposing of the devices, create a list of devices to be disposed of. Using the created list, dispose of the devices. After disposing of the devices, update the hardware asset information.

1. Create a list of devices to be disposed of.

   Before disposing of the devices, create a list of the devices to be disposed of. Export the hardware asset information whose **Planned Asset Status** is **Disposed** to a CSV file. Make sure that you export all the hardware asset information items that you need to dispose of the devices. For example, export an item such as **Asset #**, which identifies each device to be disposed of.

2. Dispose of the devices.

   Use the exported list to dispose of the devices. If you are asking a waste disposal contractor to dispose of the devices, give the contractor the list and ask the contractor to use the list to dispose of the devices.

3. Update the hardware asset information.

   After disposing of the devices, update the hardware asset information. In the **Hardware Asset** view of the Assets module, change **Asset Status** of each device that has been disposed of from **In Stock** to **Disposed**.

> **Tip**
>
> If you change **Asset Status** of hardware assets to **Disposed**, the corresponding device information is deleted.

> **Tip**
>
> If you change **Asset Status** of hardware assets to **Disposed** when the network monitor is enabled, the corresponding device information is removed from the network control list. If, however, agents are installed on the corresponding devices and these devices are connected to the network, the devices are automatically included as management targets and re-registered in the network control list.

The disposal of devices is complete. The hardware asset information of the devices that have been disposed of is retained, with their **Asset Status** set to **Disposed**.

Cancel the contracts relevant to the discarded devices as necessary.

Related Topics:

- 11.5 Exporting asset information
- 11.1.6 Changing the asset status

1.9.8 General procedure for handling a device failure

If a failure occurs on a device used in your organization, obtain the failure details based on the inquiry from the user in the field and request, if necessary, the contract company that your organization has a maintenance service contract with to repair that device. When you send the failed device for repair, lend a substitute device to the user. Also, record the details of troubleshooting.

To handle a device failure by using information managed by JP1/IT Desktop Management:

1. Check the failure details.

   Check the failed device based on the inquiry from the user to obtain the failure details.

2. Use maintenance service.

   Contact the contract company to use their maintenance service for the failed device.

3. Lend a substitute device to the user.

   When you send the failed device for repair, temporarily lend a device in stock to the user as a substitute device.

4. Return the repaired device to the user.

   When the failed device has been repaired, return it to the user and collect the device lent to the user.

5. Record a failure history.

   Record the failure details, date of occurrence, troubleshooting details, and others in JP1/IT Desktop Management.

Then, the device repair operation is complete and the failure history is recorded in JP1/IT Desktop Management.

(1) Checking the failure details

If a failure occurs on a device used in your organization, you need to obtain the failure details.

If the failure details you obtain by phone or email are not clear enough, go to where the failure occurred to check the details. Therefore, when you receive an inquiry from the user by phone or email, ask the user about the information from which you can identify the failed device such as the user name, department, and phone number of the device's user.

Tip

By using the remote control function, you can directly operate the failed device to check the failure details. Even if a failure occurs on a device located in a remote place, you can quickly handle the failure without visiting the place of failure occurrence.

Check the failed device.

In the **Hardware Asset** view of the Assets module, display the relevant hardware asset information. At this point, you can quickly check the relevant hardware asset information by using the filtering function based on the information you obtained when you received an inquiry from the user (such as user name, department, and phone number).

Related Topics:

- 1.5 Remote controlling devices
- (5) Recording a failure history

(2) General procedure for using maintenance service

If a failure occurs on a device, contact the contract company to use their maintenance service.

To check the contact point of the contract company, check the contract information of the failed device.

1. In the **Hardware Asset** view of the Assets module, select the failed device.
   By using the filtering function based on the information you obtained when receiving an inquiry from the user (such as user name, department, and phone number), you can quickly display the failed device.
2. In the **Contract Information** tab, click the link in **Contract Vendor Name** for the relevant contract information.

In the displayed dialog box, you can check the contact point and contact person of the contract company.

Note that to display information about the contract company, you need to register the following information in advance:

Contract company information

You can register the phone number and contact person of the contract company in the **Contract Vendor List** view, which is displayed by selecting **Assets** in the Settings module and then **Contract Vendor List**.

Maintenance service contract information

You can register contract information in the **Contracts** view. To register contract information, specify the relevant contract company information. Also, specify the contract target hardware asset.

Related Topics:

- 15.5.8 Managing contract vendor information
- (5) Recording a failure history

(3) Lending a substitute device to the user

When you send the failed device for repair, temporarily lend a device in stock to the user of the failed device as a substitute device. At this point, verify the asset management numbers of the failed device and the lent device.

For the failed device, change the value for **Asset Status** of hardware asset information to **In Stock** to make it clear that the failed device is under repair and not used. Also, for the lent device, change the value for **Asset Status** of hardware asset information to **In Use** to make it clear that the lent device is being used. In the **Hardware Asset** view of the Assets module, display the relevant hardware asset information. At this point, use the filtering function based on the relevant asset management numbers.

In addition, because you temporarily lend the substitute device to the user, register the schedule to collect the device later in the hardware asset information. If you are scheduled to receive the repaired device, collect the lent device, and put the collected device back in stock one week later, set **In Stock** for **Planned Asset Status** and the date one week later for **Planned Date**.

Tip

By setting a value for **Planned Asset Status**, you can check the device scheduled to be collected in **Hardware Asset Status (Planned)** on the Summary Reports. You can also send a summary report by email.

Related Topics:

- 11.1.6 Changing the asset status
- 11.1.7 Changing the planned asset status
- 15.7.2 Setting recipients of summary reports

(4) Returning the repaired device to the user

When the failed device has been repaired, return it to the user and collect the substitute device lent to the user. After collecting the substitute device from the user, update the hardware asset information.

1. Return the repaired device.

   Return the repaired device to the user.

2. Collect the substitute device.

   When returning the repaired device to the user, collect the temporarily lent device.

3. Update the hardware asset information.

   Change the value for **Asset Status** of the returned device from **In Stock** to **In Use** because the returned device is put into use. In addition, change the value for **Asset Status** of the collected device from **In Use** to **In Stock** because the collected device is put back in stock.

   To display the relevant hardware asset information in the **Hardware Asset** view of the Assets module, use the filtering function based on the asset management numbers.

If the MAC address has been changed

Where the network monitoring function rejects the connection of any new device, if the MAC address of an existing device is changed due to replacement of the device's network card, the device might be recognized as a different device. If the existing device is recognized as a different device, it cannot connect to the network.

A computer on which an agent is already installed or an agentless computer already authenticated through sharing of Windows management data can connect to the network. Even if the MAC address of such a computer has been changed, the computer is recognized as the same device and the MAC address registered in the network control list is automatically updated.

If the MAC address of an agentless device that is authenticated through SNMP or confirmed to be alive through ICMP is changed, the device is recognized as a different device and its connection to the network is rejected. To permit such a device to connect to the network, you need to manually change the device's MAC address registered in the network control list.

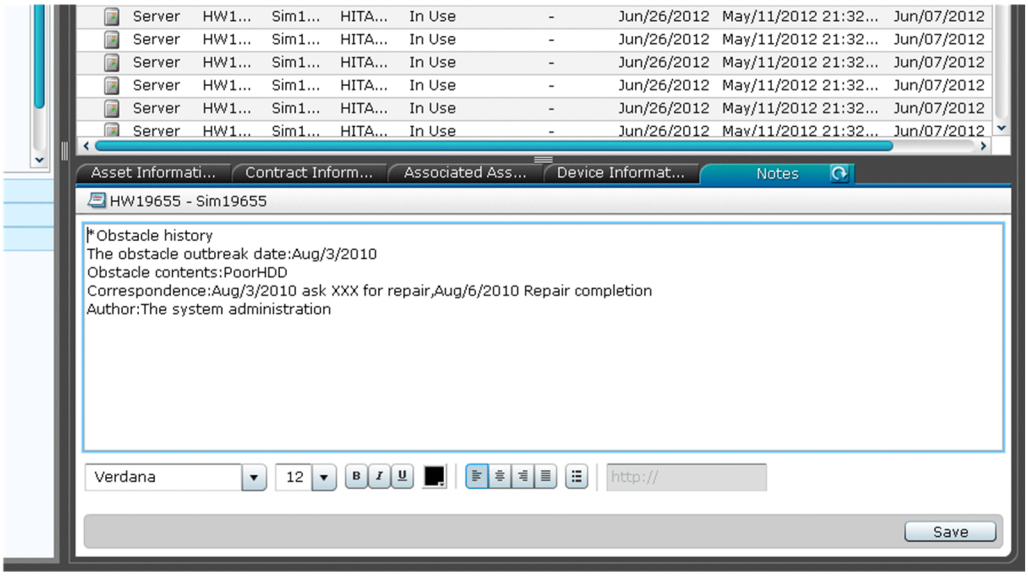
You can check the updated MAC address information in the **Device Inventory** view of the Device module and in the Network Filter Settings view. To display the **Network Filter Settings** view, in the Settings module, select **Network Access Control** and then **Network Filter Settings**.

Related Topics:

- (3) General procedure for collecting the devices that are no longer in use
- 11.1.6 Changing the asset status
- 8. Managing Network Connections of Devices

(5) Recording a failure history

You can save a failure history such as the failure details, the date of failure occurrence, and the personnel who handled the failure in the **Notes** tab in the Assets module as a record.



We recommend that you record a failure history in the **Notes** tab for the relevant hardware asset information when a failure occurs on a device or when a repaired device is returned to you.

To keep a record in the **Notes** tab, enter the details you want to record in the tab, and then click the **Save** button.

1.9.9 General procedure for investigating unauthorized changes to device information

In an organization, users might sometimes insert a flash drive into (or remove a flash drive from) a computer, or install (or remove) software without permission. These user activities might change the computer configuration. To determine whether a problem exists in the changes to device information like these, perform the procedures below to check the revision history of the device information acquired by using JP1/IT Desktop Management, and then investigate the unauthorized changes made to the device information.

1. In the operation view of JP1/IT Desktop Management, check the revision history of the device information.

   In the **Revision History** view of the Device module, periodically check the changes to the device information.

2. Determine whether any unauthorized change exists in the device revision history.

   For example, check the following to determine whether unauthorized changes exist:

   - If a hardware component has been changed: Check the ledger in which the change was recorded.
   - If software has been installed or removed: Display the tasks in the Distribution module of JP1/IT Desktop Management, and then check whether the software has actually been installed or removed.

3. If you find an unauthorized change, ask the person in charge of device management to investigate further.

   If you find an unauthorized change, contact the person is in charge of device management and that person's manager. Ask the person in charge of device management to identify the device and to investigate the actual device.

4. Take action based on the results of the investigation by the person in charge of device management.

   If the results of the investigation by the person in charge of device management indicate that a problem exists, take action to solve the problem.

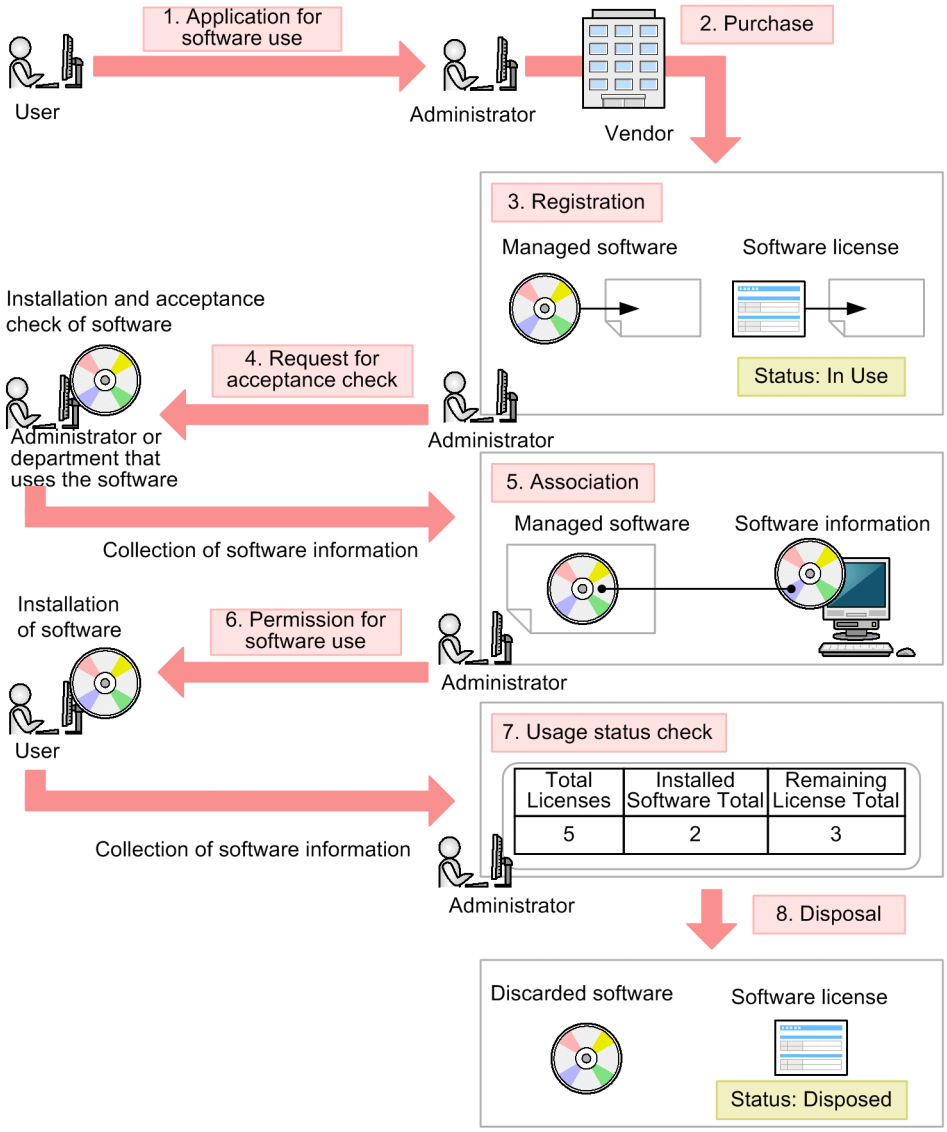
1.10 Managing software licenses

Various types of software used for work are installed on computers in your organization. To use the software, you often need a software license. You need to manage software licenses and monitor the software license usage to prevent license violation and maximize the license usage.

By using JP1/IT Desktop Management, you can do the following to efficiently manage the software licenses:

- Keep track of the owned software licenses in list form just like a ledger.
- Easily keep track of the usage status of software licenses by using graphical views such as panels and reports.
- Assign the software licenses to the computers and monitor the compliance to the license contract.

You can perform software license management tasks in the **Managed Software** view and the **Software License** view of the Assets module. To manage the software licenses, register managed-software information and software license information in JP1/IT Desktop Management, and monitor the software license usage according to the general procedure of software license management. The following figure shows the general procedure of software license management:



When you receive an application for software use from a user, review the application and purchase the software. After you purchase the software, assign a name to the software (managed software) and register the software license

information in JP1/IT Desktop Management. Also, register the managed-software information in JP1/IT Desktop Management (in the figure above, steps 1 through 3).

Request the relevant department that uses the software to check and accept the software before making it available to the user. When the administrator of the relevant department installs the software on the managed computer for acceptance check, the software information is collected and stored on the management server. Then you need to associate the collected software information with the managed-software information. This enables you to monitor the installation status of the managed software (in the figure above, steps 4 and 5).

When the above procedure is complete, review the application from the user and allow the user to start using the software. After the software is installed on the user's computer, the software information is collected and stored on the management server, which enables you to view the software license usage status. When the software is no longer necessary, dispose of and discard it (in the figure above, steps 6 through 8).

This section explains how to use JP1/IT Desktop Management in the following operations:

Purchase software.

Purchase software due to increase of employees and new software implementation. After you purchase new software, register its license information in JP1/IT Desktop Management so that you can monitor the usage status of the software licenses.

Utilize surplus licenses.

Check whether your organization has any surplus licenses. If it does, assign the surplus licenses to the appropriate computers to maximize the license usage.

Control unauthorized usage of the licenses.

Check and control any unauthorized usage of the software licenses.

Take inventory of software licenses.

Take inventory of the software licenses in your organization.

Discard software licenses.

Collect the software that is no longer in use from workplaces, and then discard the software.

Related Topics:

- 1.10.1 General procedure for purchasing software
- 1.10.2 General procedure for utilizing surplus licenses
- (3) General procedure for controlling unauthorized use of the software license
- 1.10.3 General procedure for taking inventory of software licenses
- 1.10.4 General procedure for discarding the software licenses

1.10.1 General procedure for purchasing software

After you purchase software due to increase of employees and new software implementation, register the relevant information in JP1/IT Desktop Management to start the software license management tasks.

To purchase software and start the software license management tasks:

1. Purchase software.

   Review the application for software use from the user to determine whether to purchase the software. If you decide to purchase the software, place an order with the vendor.

2. Register software information.

   When the software is delivered, register the software license information and the managed-software information in JP1/IT Desktop Management.

3. Check and accept software.

   Install the new software on the computer for testing where an agent is installed, and then check whether the software functions as expected.

   When you install the software, the software information is automatically collected.

4. Specify settings for managing the installation status.

   Based on the collected software information, specify the installed software as a part of the managed-software information. By specifying the installed software, you can view the installation status of the software.

5. Lend the software media to the users.

   After the software functions are verified, lend the software media to the users so that they can install the software on their computers.

6. Check the usage status of software licenses.

   Use JP1/IT Desktop Management to check the usage status of the software licenses.

Now you can start the software license management tasks by using JP1/IT Desktop Management.

Related Topics:

- 1.10 Managing software licenses
- 1.10.2 General procedure for utilizing surplus licenses

(1) General procedure for purchasing software

When a user needs new software, the user submits an application for using software. You need to confirm that the intended use of the software is appropriate and then determine whether to purchase the software.

1. Have the user submit an application for software use.

   Ask the user to submit the information about the new software and its user as follows:

   - Software name
   - Software version
   - Number of licenses
   - Intended use
   - Department
   - User name
   - Email address
   - Phone number
   - Asset management number of the computer where the software is used

2. Make a purchase decision.

   Review the information submitted by the user to determine whether to purchase the software. The following are examples of decision-making criteria:

   - The intended use of the software is appropriate.
   - The number of software licenses required.
   - The purchase amount does not exceed the budget.

> **Tip**
>
> If the software is the one you have purchased before, check the usage status of the software licenses. If there is any surplus software license, use the existing ones first and purchase new software licenses to meet the requirement.

If you decide to purchase the software, place an order with the vendor.

Related Topics:

- (6) Checking the usage status of the software licenses

(2) General procedure for registering software information

After you purchase the software, you need to register the managed-software information and the software license information in JP1/IT Desktop Management to start the software license management tasks. By registering the managed-software information and the software license information, you can view the usage status of the software licenses.

If the software is provided with a license contract, you also need to register the contract information associated with the software license information. By registering the details of the software license contract, you can view the terms and conditions of the contract associated with each software license.

1. Register the software license information.

   After you purchase the software, register the software license information in the **Software License** view of the Assets module, based on the software license certificate.

   > **Tip**
   >
   > By assigning the software licenses to computers, you can identify a computer that has unauthorized software and a software license that is available but unused.

2. Register the managed-software information.

   Register the managed-software information in addition to the software license information.

   To register the managed-software information, in the **Add Software License** dialog box, select **(Add New One)** for **Managed Software Name**. At this point, enter only a name in **Managed Software Name**. Do not specify the installed software associated with the managed-software information. You need to specify that software later.

3. Register the contract information.

   If the software is provided with a license contract, register the contract information of the software license (including purchase conditions and support service) in the **Contracts** view of the Assets module.

Now you finish registering necessary information. After the registration, check whether the software functions properly.

Related Topics:

- 11.2.4 Adding software license information
- 11.3.1 Adding contract information
- 11.4.2 Importing software license information
- 11.4.4 Importing contract information

(3) Checking and accepting the software

After you register the software information, you need to verify that the software functions properly. For this purpose, install the software on the computer for testing where an agent is already installed.

After you install the software, check whether the software functions properly.

> **Tip**
>
> When you install the software, the software information is collected and displayed in the **Software Inventory** view of the Device module.

(4) Specifying the settings for managing the installation status

If you specify the installed software as a part of the managed-software information, you can view the installation status of the software.

Specify the installed software information collected during the acceptance check procedure by editing the managed-software information in the **Managed Software** view of the Assets module.

Related Topics:

- 11.2.2 Editing managed software information

(5) Lending the software media to the users

When you complete the software registration and the software function verification, lend the software media to the users so that they can install the software on their computers.

> **Tip**
>
> You can also use the distribution function to install the software on the users' computers.

Related Topics:

- 1.13.1 General procedure for installing software

(6) Checking the usage status of the software licenses

When you complete the registration of the software license information and the managed-software information, you can view the usage status of the software licenses. By checking the usage status of the software licenses, you can make sure that the number of software licenses is optimal and there is no violation or surplus.

You can check the usage status of the software licenses in the **Software License Status** view of the Assets module. The **Software License Status** view shows the total number of existing licenses and remaining licenses for each managed software product.

If **Remaining License Total** shows a positive value, it indicates the number of surplus software licenses.

If it shows a negative value, the software license is violated. In this case, resolve the violation by taking an appropriate action, such as purchasing additional software licenses.

1.10.2 General procedure for utilizing surplus licenses

When you plan to purchase additional licenses of the software currently in use, check whether there is any surplus license before placing an order.

If there is a surplus license, you can efficiently use it by assigning it to the computer for the user who needs the software.

> **Tip**
>
> To check the usage status of the software licenses, you need to register the software license information and the managed-software information in the Assets module.

To utilize the surplus software licenses:

1. Check the usage status of software licenses.

   Use JP1/IT Desktop Management to check for any surplus license by viewing the usage status of the software licenses.

2. Assign the surplus licenses.

   When there is a surplus software license, assign it to the computer for the user who needs the software.

   Also, notify the user to install the software on the user's computer.

Now the software is installed on the computer that you have assigned the license, and the surplus license has been utilized efficiently.

Related Topics:

- 1.10 Managing software licenses

(1) Checking the usage status of the software licenses

When you complete the registration of the software license information and the managed-software information, you can view the usage status of the software licenses. By checking the usage status of the software licenses, you can make sure that the number of software licenses is optimal and there is no violation or surplus.

You can check the usage status of the software licenses in the **Managed Software** view of the Assets module. The **Managed Software** view shows the total number of existing licenses and remaining licenses for each managed software.

If **Remaining License Total** shows a positive value, it indicates the number of surplus software licenses.

If it shows a negative value, the software license is violated. In this case, resolve the violation by taking an appropriate action, such as purchasing additional software licenses.

(2) General procedure for assigning the surplus licenses

When you recognize that there is a surplus license by checking the usage status of the software license, assign the surplus license to the computer for the user who needs the software so that the surplus license is efficiently utilized.

Also, notify the user to install the software, and then confirm that the software is installed properly when the installation is complete.

1. Assign the software license to the computer.

   Assign the surplus license to the computer for the user who needs the software so that the surplus license is efficiently utilized.

2. Instruct the user to install the software.

   After you assign the software license, notify the user to install the software.

3. Confirm that the software is installed properly.

   To confirm that the software has been installed properly, in the **Software License Status** view of the Assets module, select the **Installed Computers** tab.

   The **Installed Computers** tab shows the computers with certain software installed. Confirm that the software has been installed on the computer you have assigned the software license.

Now the software is installed on the computer that you have assigned the license, and the surplus license has been utilized efficiently.

Related Topics:

- (3) General procedure for controlling unauthorized use of the software license
- 11.2.12 Allocating software licenses to computers

(3) General procedure for controlling unauthorized use of the software license

If the number of the software licenses is limited, you need to make sure that the software is installed only on the computers with a license. To monitor any unauthorized use of the software, you can use JP1/IT Desktop Management every day to detect any software installed on the computers without a license. If you have detected an unauthorized use of the software license, investigate which user is responsible and what is the user's intended use, and then take an appropriate action.

Tip

You can check the number of license violations in **License Violation** on the Summary Reports. You can also send a summary report by email.

To control unauthorized use of the software license:

1. Assign the software license to the computer.

   Use JP1/IT Desktop Management to assign the software license to the computer you have selected.

2. Monitor the usage status of the assigned software license.

   Use JP1/IT Desktop Management to monitor any software installed on the computer without a license.

3. Control the software license violation.

   If you have detected software installed on the computer without a license, investigate which user is responsible and what is the user's intended use. If the user has a justifiable reason, assign a software license to allow the user to use the software.

Now the software licenses are used appropriately.

Related Topics:

- 1.10 Managing software licenses
- 15.7.2 Setting recipients of summary reports

(4) Assigning the software license to the computer

If you assign the software license to the computer in the **Software License** view of the Assets module, you can check whether the software is installed only on the computers with an appropriate software license.

Related Topics:

- 11.2.4 Adding software license information
- 11.2.1 Adding managed software information
- 11.2.12 Allocating software licenses to computers

(5) Monitoring the usage status of the assigned software licenses

After you assign software licenses to the computers, you need to confirm that the software is utilized in an appropriate manner by performing the following checks on a regular basis:

Check for surplus license or license violation.

Check the license usage status of the managed software in **License Total**, **Number of Used Licenses**, and **Remaining License Total** in the **Software License Status** view of the Assets module.

License Total indicates the number of owned licenses of the managed software. **Number of Used Licenses** indicates the number of licenses of the managed software currently in use. **Remaining License Total** is calculated by subtracting the value for **Number of Used Licenses** from the value for **License Total**.

> **Tip**
>
> If **Remaining License Total** shows a positive value, it indicates the number of surplus software licenses. If it shows a negative value, the software license is violated.

Check whether the software is installed only on the computers with a software license.

Check the usage status of the assigned software licenses.

In the **Software License Status** view of the Assets module, check whether the values for **Number of Used Licenses** and **Assigned License Total** are equal. If the values for **Number of Used Licenses** and **Assigned License Total** are not equal, check the usage status of the software licenses.

If **Assigned License Total** is not displayed in the view, right-click an item name in the list, and then select **Select Columns**. In the displayed dialog box, select the **Assigned License Total** check box, and then click the **OK** button. **Assigned License Total** is displayed in the view.

License Total	Number of Used Licenses	Remaining License Total	Assigned License Total
12000	4063	7937	1000

- If **Number of Used Licenses** is greater than **Assigned License Total**

  Software might be installed on a computer without a license. Select the **Installed Computers** tab, and then select the **Show Only Computers Not Licensed** check box. You can identify the computers that have software installed without a relevant license.

- If **Number of Used Licenses** is less than **Assigned License Total**

  The software licenses might be underutilized. Select the **Licensed Computers** tab, and then select the **Show Only Computers Not Installed** check box. You can identify the computers that have a software license but do not have relevant software installed.

Tip

If more than one software license is shown on the **Software Licenses** tab, identify which software license is underutilized. Compare the values in the **Remaining License Total** columns for the software licenses. The license with the highest value is the most underutilized.

(6) General procedure for controlling the software license violation

If you have detected the software installed on the computer without a license by viewing the usage status of the software licenses, investigate which user is responsible and what is the user's intended use. If the user has a justifiable reason, assign a software license to allow the user to use the software.

1. Ask the user about the intended use.

   In the **Software License Status** view of the Assets module, select the **Installed Computers** tab, and then select the **Show Only Computers Not Licensed** check box. Inform the user of the displayed computer that the software has been installed on the computer without a license, and ask the user about the intended use.

2. Assign the software license to the computer.

   If the user has a justifiable reason, assign a software license to the user's computer to allow the user to use the software.

   If the intended use is not justified, instruct the user to uninstall the software or use the distribution function to uninstall the software. In addition, advise the user not to install any software without a license.

3. Check the usage status of software licenses.

   In the **Software License Status** view of the Assets module, check whether the values for **Number of Used Licenses** and **Assigned License Total** are equal. Also use the value for **Remaining License Total** to make sure that there is no software license violation.

When you have confirmed that **Number of Used Licenses** is equal to **Assigned License Total** and there is no software license violation, the software licenses are properly utilized.

Even after you have confirmed that the software licenses are properly utilized, monitor the usage status of the software licenses on regular basis.

Related Topics:

- 11.2.12 Allocating software licenses to computers
- 12.3 Uninstalling software from a computer

1.10.3 General procedure for taking inventory of software licenses

To effectively manage the software licenses in your organization, you need to take inventory on regular basis to keep accurate inventory records. For this purpose, you need to register the physical inventory records in JP1/IT Desktop Management, so that you can easily identify the software licenses for which a physical inventory has not been conducted.

To take inventory of the software licenses:

1. Conduct a physical count.

   Create a list of software license information, and then perform a physical count of the inventories found in your organization.

2. Update the information with the physical inventory records.

   To manage the status of the software license inventory, update the information in JP1/IT Desktop Management with the physical inventory records.

3. Investigate the software licenses for which a physical inventory has not been conducted.

   Identify the software licenses for which a physical inventory has not yet been conducted to investigate the usage status of the software licenses. Update the information in JP1/IT Desktop Management with the information of the software licenses found during the investigation.

Now the information in JP1/IT Desktop Management is updated with the physical inventory records of the software licenses.

Related Topics:

- 1.10 Managing software licenses

(1) General procedure for performing physical inventory count

To perform a physical inventory count of the software licenses, you need to output a list of software license information and then check the software licenses against the list.

1. Export a list of software license information.

   Create a list of software license information for physical inventory count. In the **Software License** view of the Assets module, export the software license information to a CSV file. To identify software licenses, export the items such as **License #**, **Last Tracked Date**, **License Name**, **Total Licenses**, and **License Type**. You will use the exported CSV file when you update the information in JP1/IT Desktop Management with the result of physical inventory count. Make sure that you export the **License #** and **Last Tracked Date** items.

2. Perform a physical inventory count based on the list of software license information.

   Perform a physical inventory count based on the list of software license information.

   You need to check the following:

   - Media
   - Software license certificate (Purchase and sale contract)

   Check the software license certificates and the software media against the list of software license information to make sure that the software licenses actually exist. When you have completed the inventory count, place a checkmark next to the corresponding software license on the list. Update the stocktaking date for the software licenses with a checkmark by using JP1/IT Desktop Management.

Now the physical inventory count is complete, and the list of software licenses with the inventory results has been prepared.

Related Topics:

- 11.5 Exporting asset information
- (2) General procedure for updating the information with the physical inventory records

(2) General procedure for updating the information with the physical inventory records

To manage the status of the software license inventory, update the information in JP1/IT Desktop Management with the physical inventory records. When you have updated the information with the physical inventory records, the values for **Last Tracked Date** of software license information are updated in the **Software License** view of the Assets module.

1. Create a CSV file that contains the updated stocktaking dates.

   To collectively update the stocktaking dates, create a software license information CSV file that contains the updated stocktaking dates. Edit the CSV file used in the physical inventory count to update the values for **Last Tracked Date** of the software licenses for which the physical inventory count has been confirmed.

   Tip

   If the software license information such as **Total Licenses** and **License Status** has been changed since the last inventory count, edit the CSV file to update the corresponding values in addition to the values for **Last Tracked Date**.

2. Update the stocktaking dates.

   After you have created the software license information CSV file, import it to collectively update the stocktaking dates.

For the software licenses for which the physical inventory count has been confirmed, the values for **Last Tracked Date** of the software license information are updated.

Tip

If you want to check the software licenses that you have in hand one by one, manually update the stocktaking date for each software license.

Related Topics:

- 11.1.8 Manually updating a stocktaking date

(3) General procedure for inspecting software licenses for which physical inventory has not been completed

You need to inspect the usage status and perform a physical inventory count again for the software licenses for which a physical inventory count has not been completed.

1. Inspect the software licenses for which the physical inventory has not been completed.

   In the **Software License** view of the Assets module, identify the software license information of the software licenses whose **Last Tracked Date** has not been updated. Using the filtering fraction, display the software license information of the software licenses whose **Last Tracked Date** is older than the last stocktaking date.

2. Export a list of software license information.

   Create a list of software license information for inspection. Export the software license information of the software licenses whose stocktaking date has not been updated to a CSV file. To identify software licenses, export the items such as **License #**, **License Name**, **Total Licenses**, and **License Type**.

3. Inspect the software licenses.

   Based on the list of software license information, find the software licenses (software license certificates and software media).

   If you find the software licenses:

   If you find a software license certificate or media, make a note on the list to indicate that the physical inventory count has been successfully completed for the software license. Make a correction to the software license information at the same time, if necessary.

If you cannot find the software licenses:

The software license certificate or media might be lost. Check with the administrator in charge of software license management about the circumstances. If you have confirmed that the software license certificate or media have been lost, change the value for **License Status** of the relevant software license to **Expired** in the **Software License** view of the Assets module. Also, enter comments in the **Notes** tab, describing the remarks such as reason or date and time of loss.

4. Update the information with the physical inventory records.

   Update the information in JP1/IT Desktop Management with the results for the software licenses for which the physical inventory count has been completed.

Now you finish taking inventory of software license.

Related Topics:

- 11.5 Exporting asset information
- (2) General procedure for updating the information with the physical inventory records
- 1.10.4 General procedure for discarding the software licenses

1.10.4 General procedure for discarding the software licenses

You need to discard a software license when the software is obsolete and no longer used.

To discard a software license:

1. Determine whether the software license is necessary.

   When a user requests termination of the software license, determine whether the relevant software license is required by any other user. To decide whether the software license can be discarded, make sure that the depreciation of the software has been complete and no user is using the software.

2. Discard the software license and update the information.

   If you decide to discard the software license, discard the software media and make sure that the software has been uninstalled from the computers. Update the software license information in JP1/IT Desktop Management with the discarded software license.

Now the record of the discarded software license in JP1/IT Desktop Management has the *Expired* status.

Related Topics:

- 1.10 Managing software licenses

(1) General procedure for determining whether the software license is necessary

When a user requests termination of the software license, you need to determine whether the relevant software license can be discarded. Based on the usage status and depreciation terms of the software license, decide to discard the unnecessary software license.

1. Check the number of installed software.

   Confirm that no user is using the software license to be discarded. In the Assets module, in the**Software License Status** view of the Assets module, check the value for **Number of Used Licenses** of the relevant software. If the number of used licenses is not 0, a user who is using the software. In such a case, do not discard the software license.

The user who requested the termination of the software license is supposed to have already uninstalled the software from the user's computer.

2. Make sure that the depreciation has been completed.

   Make sure that the depreciation of the software license to be discarded has been completed. Select the **Contract Information** tab in the **Software License** view of the Assets module to display the details of the software license. Based on **Total Amount** and **Contract Date**, determine whether the depreciation has been completed.

3. Check whether any other user is using the software.

   Notify all users that the software license is due to be discarded by email to make sure that no user needs the software anymore. If a user requests the software license, assign the license to the user's computer.

After all the above steps, discard only the software licenses that are no longer necessary.

Related Topics:

- (2) General procedure for discarding the software license and updating the information

(2) General procedure for discarding the software license and updating the information

When you determine that the software license is no longer necessary, you need to discard it. After you dispose of the media, make sure that the relevant software has been uninstalled from the computers, and then update the software license information in JP1/IT Desktop Management.

1. Dispose of the software media.

   Dispose of the media so that the software cannot be reused. For CD or DVD, destroy the surface or cut the media into small pieces with a special equipment to make the content completely unreadable.

2. Make sure that the software has been uninstalled.

   After you dispose of the media, make sure that the relevant software has not been installed since you decided to discard the software license. In the Assets module, in the **Software License Status** view, on the **Installed Computers** tab, make sure that the relevant software does not exist on the computers. If you find a computer with the software installed, instruct the user to uninstall it.

3. Update the software license status.

   When you confirm that the software has been uninstalled, update the software license information in JP1/IT Desktop Management. In the **Software License** view of the Assets module, change **License Status** of the discarded software license from **In Use** to **Expired**.

Now the software license has been discarded and the software license information in JP1/IT Desktop Management has been updated.

Related Topics:

- 11.2.8 Changing a license status

1.11 General procedure for managing asset contract information

When you manage contract information by using JP1/IT Desktop Management, you can do the following to efficiently keep track of the contract status:

- Easily keep track of the status of hardware assets and software licenses under contract.
- Quickly obtain information about the contracts close to expiry to help future operation planning.
- Evaluate the cost on hardware assets and software licenses.

You can perform the contract information maintenance tasks in the **Contracts** view of the Assets module. To start the contract information management tasks, you need to register the contract information, and then maintain the contract information according to events such as addition of contract target devices, contract termination, or renewal.

To manage the asset contract information:

1. Maintain the contract information.

   Register the contract information. Keep the contract information up-to-date by editing or deleting the relevant contract information as required.

2. Identify the contracts close to expiry.

   Identify the contracts close to expiry by using the email notification automatically sent by JP1/IT Desktop Management. Renew the contract, or terminate it if it is no longer necessary.

3. Renew the contract.

   Renew the contract to meet the ongoing needs of your organization. Obtain the contract renewal information from the contract vendor and sort out the obtained information into two groups, termination and renewal.

4. Terminate the contract.

   Terminate the contract that is no longer necessary. Update the contract status in JP1/IT Desktop Management, and then discard the assets or return them to the vendor.

1.11.1 Identifying the contracts close to expiry

You can configure JP1/IT Desktop Management to send an email containing the information about the contracts close to expiry. The email is sent automatically, and you do not need to check the contracts close to expiry on regular basis in the operation view of JP1/IT Desktop Management.

The email contains the details of the contracts close to expiry and expired contracts, which are also shown on the Summary Reports. When you click the link showing the number of contracts in the email, the operation view of JP1/IT Desktop Management opens and a list of the relevant contract information is displayed in the **Contracts** view of the Assets module. To view the details of the relevant contract information, click the link in the email.

1.Configure JP1/IT Desktop Management to send an email to notify the contracts close to expiry.

   In the **Summary Report Notifications** view of the Settings module, you can specify a recipient of the email with a summary report. If no recipient is specified, a summary report is not sent. Also, the mail server information must be specified for email transmission.

2. Identify the contracts close to expiry.

   Open the email sent by JP1/IT Desktop Management to check the information about the contract that is close to expiry or has already expired. For the contract close to expiry, determine whether the contract is to be renewed or terminated. For the expired contract, review the details of the relevant hardware assets and software licenses, and then renew or terminate the contract.

Related Topics:

- 15.7.2 Setting recipients of summary reports
- 15.9.1 Setting up mail servers
- 11.3.1 Adding contract information
- 1.11.2 Renewing the contract
- 1.11.3 Terminating the contract

1.11.2 Renewing the contract

After you have identified the contracts close to expiry, renew the contract that needs to be extended.

Tip

When you extend the contract, maintain the relevant contract information by creating two sets of data (records of the expired contract and the extended contract) so that you can access the contract information of the previous contract.

1. Obtain the renewal information from the contact person.

   Ask the contact person of the contract vendor to send the renewal information.

2. Register the contract information of the contract to be extended.

   Based on the renewal information from the vendor, register the contract information of the extended contract by copying the existing contract information. In the **Contracts** view of the Assets module, select the relevant contract information, and then click the **Edit** button. In the displayed dialog box, click the **Save as** button.

   Edit the new contract information to update the values for the items such as **Contract Term**, **Contract Date**, and **Contract Status** according to the extended contract.

3. Change the status of the expired contract.

   When the contract expiry date arrives, change **Contract Status** of the expired contract. In the **Contracts** view of the Assets module, click the **Change Status** button. In the displayed dialog box, select **Expired**.

4. Update the relevant assets.

   If there is any change in the contract target software license or hardware assets, update the corresponding asset information. In the **Contracts** view of the Assets module, select the **Software Licenses** tab or the **Hardware Assets** tab, and then edit the asset information as required.

Related Topics:

- 11.3.2 Editing contract information
- 1.11.3 Terminating the contract

1.11.3 Terminating the contract

After you have identified the contracts close to expiry, terminate the contract of the asset that is no longer necessary.

To terminate the contract, in the **Contracts** view of the Assets module, click the **Change Status** button. In the displayed dialog box, select **Expired**.

If the value for **Contact Type** of the hardware asset is **Lease** or **Rent**, you need to return the asset. After you have returned the asset to the vendor, delete the corresponding hardware asset information or change the value for **Asset Status** to **Disposed**.

In case of software license termination, you do not need to return the asset to the vendor.

Important note

The amounts of the contract cost in the **Hardware Assets Cost** and **Software License Cost** reports are calculated up to the contract end date specified in **Contract Term** of the contract information. If you cancel the contract before expiration, you need to change the contract end date by editing **Contract Term** of the contract information.

Related Topics:

- 11.3.2 Editing contract information
- 1.11.2 Renewing the contract

1.12 General procedure for considering the asset cost savings

By using JP1/IT Desktop Management, you can understand the cost involved in the operation of hardware assets and software licenses. JP1/IT Desktop Management also supports your task when you assign unused assets to the users who need these assets or cancel any surplus licenses to save cost.

To understand the cost of hardware assets and software licenses and then manage the assets efficiently:

1. Review the monthly asset cost.

   Review the cost trend report to identify high-cost hardware assets and software licenses. Cancel the contract that is no longer necessary. You need to specify the cost as a part of the contract information to generate the cost trend report.

2. Identify any unused assets.

   Check for any hardware assets or software licenses that are not currently in use. If an unused asset is found, you can reduce the cost by canceling the contract that is no longer necessary.

3. Identify any surplus license.

   Check whether you have purchased a new software license when you have a surplus. To prevent you from purchasing any unnecessary software license, thoroughly check the usage status of software licenses.

Related Topics:

- 1.12.1 Reviewing monthly asset cost
- 1.12.2 Identifying unused assets
- 1.12.3 Identifying surplus licenses

1.12.1 Reviewing monthly asset cost

Review the monthly cost on hardware assets and software licenses. You can reduce the cost by canceling the contracts that are no longer necessary.

1. Review the cost reports.

   In the Reports module, review the **Hardware Assets Cost** and **Software License Cost** reports. If you find any hardware assets or software licenses with a large amount of cost for the previous month, check the contract type in the Assets module.

2. Review the details of the contract information.

   Display the **Contracts** view of the Assets module. In the menu area, select the **Hardware Assets** or **Software Licenses** filter. You can also select the **Contract Status** and **Contract Type** filters in the information area to narrow down the information entries in the list. For **Contract Status**, select **Active**. For **Contract Type**, select a contract type for which you have found a contract with a high cost in the report you reviewed. After narrowing down the information entries in the list, click the **Contract Information** tab to display the details.

3. Cancel unnecessary contracts.

   Check the details in the tab at the bottom of the information area to determine whether there is any unnecessary contract. For example, if you find a software license that is not currently in use and will not be used anymore, contact the contract vendor for cancellation.

4. Change the status in **Contact Status** to **Canceled**.

   After the contract cancellation, change the status in **Contract Status** from **Active** to **Canceled**.

Important note

The amounts of the contract cost in the **Hardware Assets Cost** and **Software License Cost** reports are calculated up to the contract end date specified in **Contract Term** of the contract information. If you cancel the contract before expiration, you need to change the contract end date by editing **Contract Term** of the contract information.

Related Topics:

- 11.3.5 Changing the contract status

1.12.2 Identifying unused assets

Check for any hardware assets or software licenses that are not currently in use. If an unused asset is found, you can reduce the cost by canceling the contract that is no longer necessary. This subsection explains how to identify the software currently not in use.

First step is to find any software license that is high cost and not in use. You can maximize the usage of the assets by canceling unnecessary software licenses or assigning a surplus license to a user who needs that license.

1. Identify software with a large license fee in the list.

   Display the **Contracts** view of the Assets module. In the menu area, select the **Software Licenses** filter.

   While the contract information of the software license is displayed, click **Total Amount**. The contract information entries are sorted by **Total Amount**.

   If **Total Amount** is not displayed in the view, right-click an item name in the list, and then select **Select Columns**. In the displayed dialog box, select the **Total Amount** check box, and then click the **OK** button. **Total Amount** is then displayed in the view.

   ### Tip

   If you create a filter that shows only the managed software with a certain amount or more, you can easily narrow down the list to identify the managed software with a large license fee.

2. Check the usage status of software licenses.

   Select the software with a large license fee to check the value for **Remaining License Total** in the **Software Licenses** tab. If the value is 0, there is no surplus and the licenses are efficiently utilized. If the value is 1 or more, there is a surplus and the licenses might not be used efficiently. Find a user who needs the license, and then assign the license to that user's computer.

3. Check with the users about the usage status of the managed software.

   For the software with a large license fee and no surplus license, check with the users about the usage status.

4. Instruct the user to uninstall the managed software.

   If you find a user who is not currently using the managed software, instruct the user to uninstall the managed software.

Related Topics:

- 1.9.6 General procedure for checking devices that are not used
- 11.2.12 Allocating software licenses to computers

1.12.3 Identifying surplus licenses

Review the usage status of the software licenses. If you find managed software with many surplus licenses, make sure that you have not purchased additional licenses to maximize the software license usage.

1. Identify software with many surplus licenses.

   In the Assets module, display the **Software License Status** view. In the information area, click **Remaining License Total**. The list is sorted by the number of remaining licenses of the managed software. Check the software licenses with many surpluses. Such licenses might not be efficiently utilized.

2. Check whether a new software license has been added when there is a surplus.

   After identifying the software with many surplus licenses, check whether an additional software license has been recently purchased. Investigate the software that has a recent date in **Registered Date/Time** in the **Software Licenses** tab.

   If **Registered Date/Time** is not displayed in the view, right-click an item name in the list, and then select **Select Columns**. In the displayed dialog box, select the **Registered Date/Time** check box, and then click the **OK** button. **Registered Date/Time** is then displayed in the view.

   If a new software license has been purchased when there is a surplus, advise the administrator who purchased the new license that the administrator needs to make sure that there is no surplus before ordering a new license.

Related Topics:

- 11.2.1 Adding managed software information
- 11.2.2 Editing managed software information
- 11.3.3 Deleting contract information
- (2) General procedure for assigning the surplus licenses

1.13 Distributing software and files

By using the distribution function, you can install required software on the computers in your organization and uninstall software no longer necessary. You can also distribute files to these computers.

This function can reduce the time and effort required for software implementation and management by releasing each user from the tasks of installing or uninstalling software. This function also facilitates software maintenance by the features such as batch installation of the most updated software version.

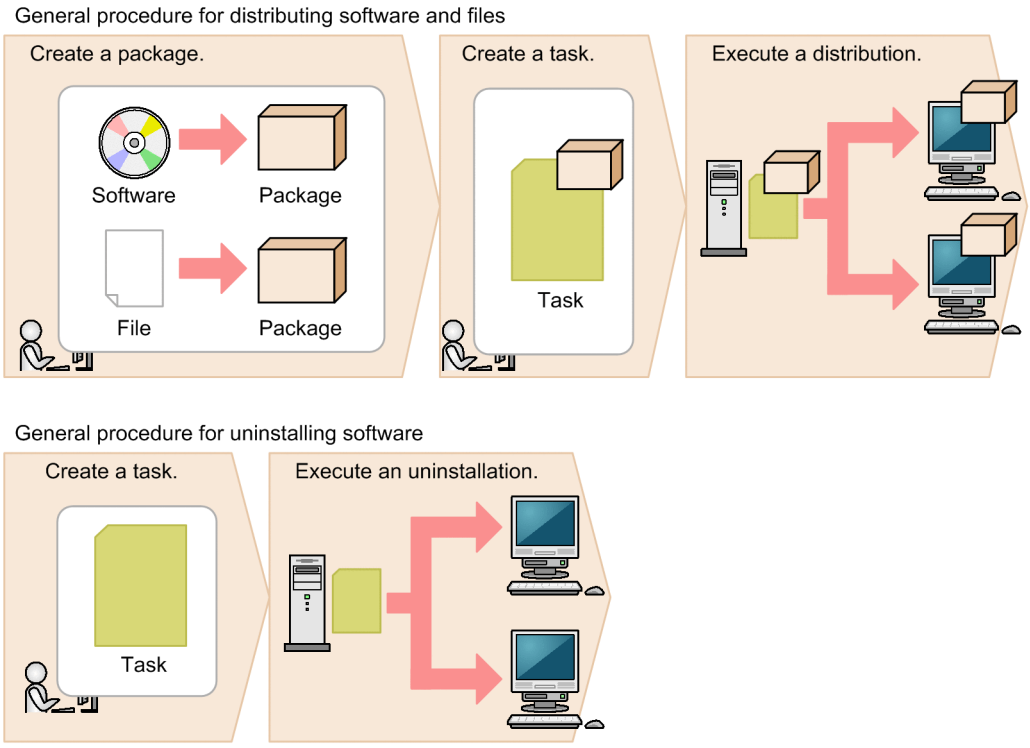
Important note

You can distribute software and files by using the distribution function to only the computers managed online.

By using the distribution function, you can do the following to efficiently install or uninstall software and distribute files:

- Install or uninstall software without user's intervention.
- Set the distribution schedule and installation timing depending on business operations.
- Easily keep track of the distribution status by using graphical views such as panels and reports.

The following figure shows how to distribute software and files and uninstall software by using the distribution function:



First, register the software to be installed or files to be distributed as a package on the management server. Next, create a task that defines the schedule to start the package distribution and how to run the task on the target computer. After you create the task, the package is distributed according to the specified schedule. To uninstall software, you also need to create a task for uninstallation, but do not need to create a package.

This section explains how to use JP1/IT Desktop Management in the operations described below. See the description of the operation that suits your purpose.

Install software.

This step describes how to install software with an installer on computers in your organization, which is required in the events such as new software implementation or version upgrade.

Distribute files.

This step describes how to distribute files to target computers in your organization, which is required in the events such as to update a configuration file stored in each computer, and implement in-house software that requires no installation procedure.

Uninstall software.

This step describes how to uninstall unnecessary or unauthorized software from the computers in your organization.

1.13.1 General procedure for installing software

You can use the distribution function to install software on the computers in your organization in case of new software implementation or version upgrade.

To distribute and install software on the computers in your organization by using the distribution function:

1. Check the software installation status.

   When you plan to upgrade the software or add new licenses, check the software installation status to determine how many licenses are necessary. When you decide on the number of necessary licenses, purchase them from the vendor.

2. Create a software distribution plan.

   Create a software distribution plan before you begin the procedure. Also notify the users in advance of the details of the distribution plan.

3. Install software on the computers.

   In order to install the software, create a package in which the software to be installed is registered and a task to distribute the package. The package is distributed according to the schedule specified in the task.

4. Review the results of the task execution.

   Review the execution status of the software distribution. If a failure occurs on the computer during the distribution or installation, find the cause of the failure to solve the problem, and then re-execute the task.

Now the software has been installed on all the target computers.

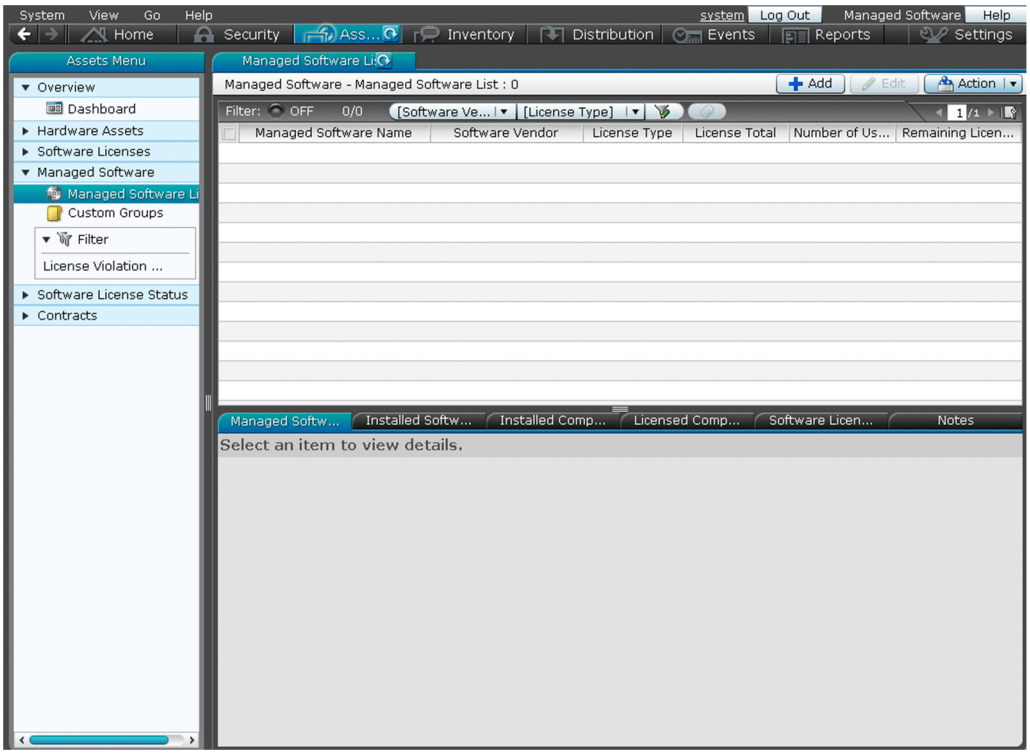
Related Topics:

- 1.13 Distributing software and files

(1) Checking the software installation status

When you upgrade the software version or add new licenses, you need to check the software installation status to determine how many licenses are necessary. When you decide on the number of necessary licenses, purchase them from the vendor.

You can view the software installation status and the usage status of the licenses in the **Managed Software** view of the Assets module.



In case of software version upgrade, determine how many computers you have with the old version to be upgraded. In case of new software license addition, determine how many computers you have for installation.

> **Tip**
>
> Also in case of new software license addition, we recommend that you check whether you have any surplus license. To optimize the license usage, you can use the surplus to fill the request and order additional licenses as required.

If you decide on the number of the licenses to purchase, place an order with the vendor. Register the details of the purchased software as the asset information (software license information and managed-software information) in JP1/IT Desktop Management so that you can view the usage status of the software license.

Related Topics:

- 1.10.2 General procedure for utilizing surplus licenses
- 1.10.1 General procedure for purchasing software

(2) Creating a software distribution plan

Create a software distribution plan before you begin the procedure. Also notify the users in advance of the details of the distribution plan.

1. Create a software distribution plan.

   Consider the following items included in the software distribution plan:

   - Computers to which the software is to be distributed
   - Date and time on which the software is to be distributed

When you set the date and time on which the software is to be distributed, you need to consider the load placed on the network. For example, you can schedule the distribution during night to avoid business hours, or divide the target computers into groups to perform distribution over several days.

Also, you need to do some preparation before you use the distribution function.

Tip

Before you start the software distribution procedure, we recommend that you make sure that the software is successfully distributed and installed by using the computer for testing.

2. Notify the users of the details of the software distribution plan.

   Notify the users in advance of the details of the software distribution plan to successfully install the software as scheduled and to avoid confusion among the users. For example, notify the users of the following information:

   - Software name
   - Software version
   - Reason of distribution
   - Distribution date and time
   - Cautions

Now the preparation for the software distribution is complete.

Related Topics:

- 12.1 Installing software on the computers

(3) Installing software on the computers

You can use the **Install Software** wizard to distribute and install software on users' computers.

By using the **Install Software** wizard, you can create a package in which the software to be installed is registered and a task to distribute the package. When the wizard is complete, the package is distributed according to the schedule specified in the task.

To install the software on the computers:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, from **Action**, select **Launch Install Wizard** to start the wizard.
4. In the **What is this Wizard?** view, read the instruction, and then click the **Next** button.
5. In the **Select Software** view, select **Create New Package**, specify the files to be registered in the package, and then click the **Next** button.

   If you have created a package already, you can select it in this step.
6. In the **Specify Package** view, set the package information, and then click the **Next** button.
7. In the **Create Package Distribution Task** view, set the schedule to perform distribution and so on, and then click the **Next** button.

By clicking **Execute Option**, you can specify option settings such as the installation timing, email message to notify the users, and so on.

8. In the **Select Target Computers** view, click the **Change** button.
9. In the **Select Target Computers** dialog box, select the computers on which the software is installed, and then click the **OK** button.
10. Click the **Next** button.
11. In the **Confirm Settings** view, check the settings, and then click the **Complete** button.
12. In the **Distribution Settings Configure**d view, click the **Close** button.

The software is distributed and installed on the specified target computers according to the schedule specified in the task. You can view the execution status of the task in the **Tasks** view of the Distribution module.

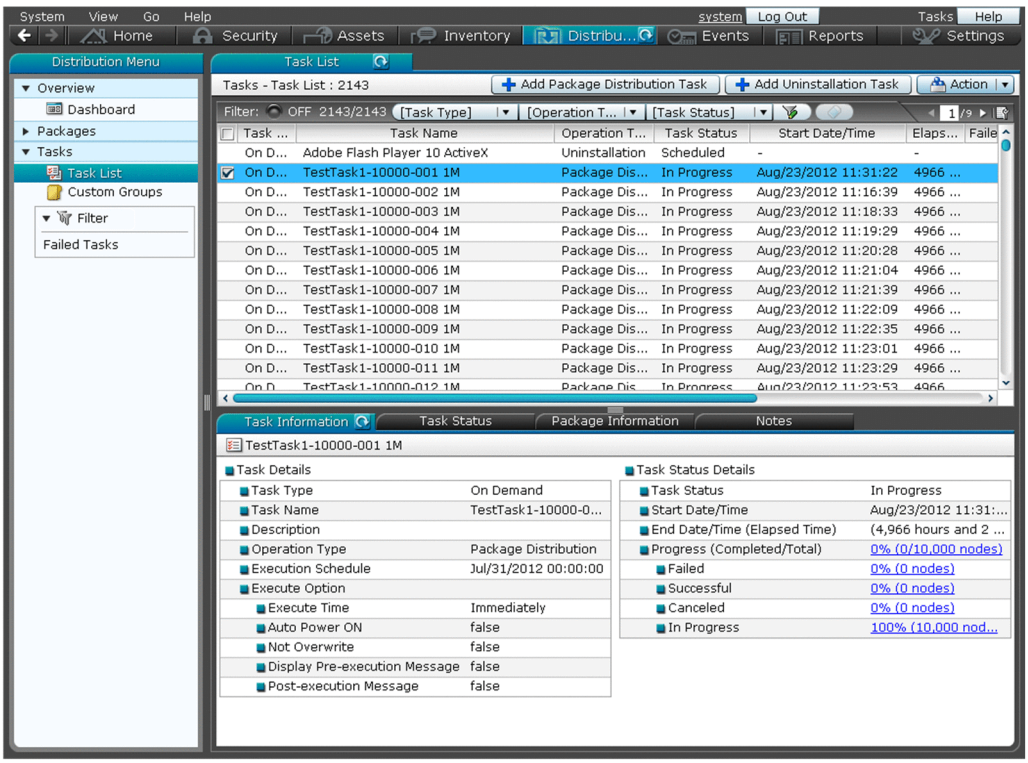
> **Tip**
>
> The users can change the schedule to execute the installation later if more urgent or important operation is in progress on their computers.

Related Topics:

- 12.6 Postponing downloads and installation as a user
- 12.5.5 Stopping tasks

(4) Reviewing the results of the task execution

You can review the task execution status in the **Tasks** view of the Distribution module.



We recommend that you check the task execution status on regular basis until the task is complete. If a failure occurs on the computer during the task execution, find the cause of the failure to solve the problem, and then re-execute the task.

Tip

You can also configure JP1/IT Desktop Management to automatically send an email when a distribution management event occurs (such as task completion and task failure).

1. Review the execution status of the task.

   In the **Tasks** view of the Distribution module, select a task to view its execution status. After you select a task, the detailed information of the task is displayed in the tab at the bottom of the information area. In the **Task Information** tab, select **Task Status Details** and then **Progress (Completed/Total)** to check whether the task has been completed successfully.

2. Find the cause of the task failure, and then solve the problem.

   If a failure occurred on the computer during the task execution, click the **Failed** link in the **Task Information** tab. The **Task Status** tab opens with a list of computers on which the task has failed.

   Click the link in **Task Status** to display a dialog box showing the details of the task status. Find the cause of the task failure, and then solve the problem.

3. Re-execute the task.

   When the problem has been resolved, re-execute the task.

   If you re-execute the task with the same settings:

   You can just re-execute the task with the same settings as the previous execution.

   If you re-execute the task with different settings:

   If you need to change the settings such as execution schedule or target computer, edit or copy the settings, and then re-execute the task.

Now the task will be re-executed on the target computers.

Related Topics:

- 15.8.1 Specifying settings for event notification
- 12.5.6 Re-executing tasks
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.5 Stopping tasks

1.13.2 General procedure for distributing files

You can use the distribute function to distribute files to target computers in your organization, which is required in the events such as to update a configuration file stored in each computer, and implement in-house software that requires no installation procedure.

To distribute files to the computers in your organization:

1. Create a file distribution plan.

   Create a file distribution plan before you begin the procedure. Also notify the users in advance of the details of the distribution plan.

2. Distribute files to the target computers.

   In order to distribute the files, create a package in which the files to be distributed are registered and a task to distribute the package. The package is distributed according to the schedule specified in the task.

3. Review the results of the task execution.

   Review the execution status of the task. If a failure occurs on the computer during the distribution, find the cause of the failure to solve the problem, and then re-execute the task.

Now the files have been distributed to all the target computers.

Related Topics:

- 1.13 Distributing software and files

(1) Creating a file distribution plan

Create a file distribution plan before you begin the procedure. Also notify the users in advance of the details of the distribution plan.

1. Create a file distribution plan.

   Consider the following items included in the file distribution plan:

   - Computers to which the files are to be distributed
   - Date and time on which the files are to be distributed

     When you set the date and time on which the files are to be distributed, you need to consider the load placed on the network. For example, you can schedule the distribution during night to avoid business hours, or divide the target computers into groups to perform distribution over several days.

   Also, you need to do some preparation before you use the distribution function.

   Tip

   Before you start the file distribution procedure, we recommend that you make sure that the files are successfully distributed by using the computer for testing.

2. Notify the users of the details of the file distribution plan.

   Notify the users in advance of the details of the file distribution plan to successfully distribute the files as scheduled and to avoid confusion among the users. For example, notify the users of the following information:

   - File name
   - Target folder
   - Reason of distribution
   - Distribution date and time
   - Cautions

Now the preparation for the file distribution is complete.

Related Topics:

- 12.2 Distributing files to the computers

(2) Distributing files to the computers

You can use the **File Distribution** wizard to distribute files to users' computers.

By using the **File Distribution** wizard, you can create a package in which the files to be distributed are registered and a task to distribute the package. When the wizard is complete, the package is distributed according to the schedule specified in the task.

To distribute the files to the computers:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, from **Action**, select **Launch File Distribution Wizard** to start the wizard.
4. In the **What is this Wizard?** view, read the instruction, and then click the **Next** button.
5. In the **Select File** view, select **Create New Package**, specify the files to be registered in the package, and then click the **Next** button.
   If you have created a package already, you can select it in this step.
6. In the **Specify Package** view, set the package information, and then click the **Next** button.
7. In the **Create Package Distribution Task** view, set the schedule to perform distribution and so on, and then click the **Next** button.
   By clicking **Execute Option**, you can specify option settings such as the timing to distribute the files after the package distribution, email message to notify the users, and so on.
8. In the **Select Target Computers** view, click the **Change** button.
9. In the **Select Target Computers** dialog box, select the computers to which the files are distributed, and then click the **OK** button.
10. Click the **Next** button.
11. In the **Confirm Settings** view, check the settings, and then click the **Complete** button.
12. In the **Distribution Settings Configured** view, click the **Close** button.

The files are distributed to the specified target computers according to the schedule specified in the task. You can view the execution status of the task in the **Task List** view of the Distribution module.

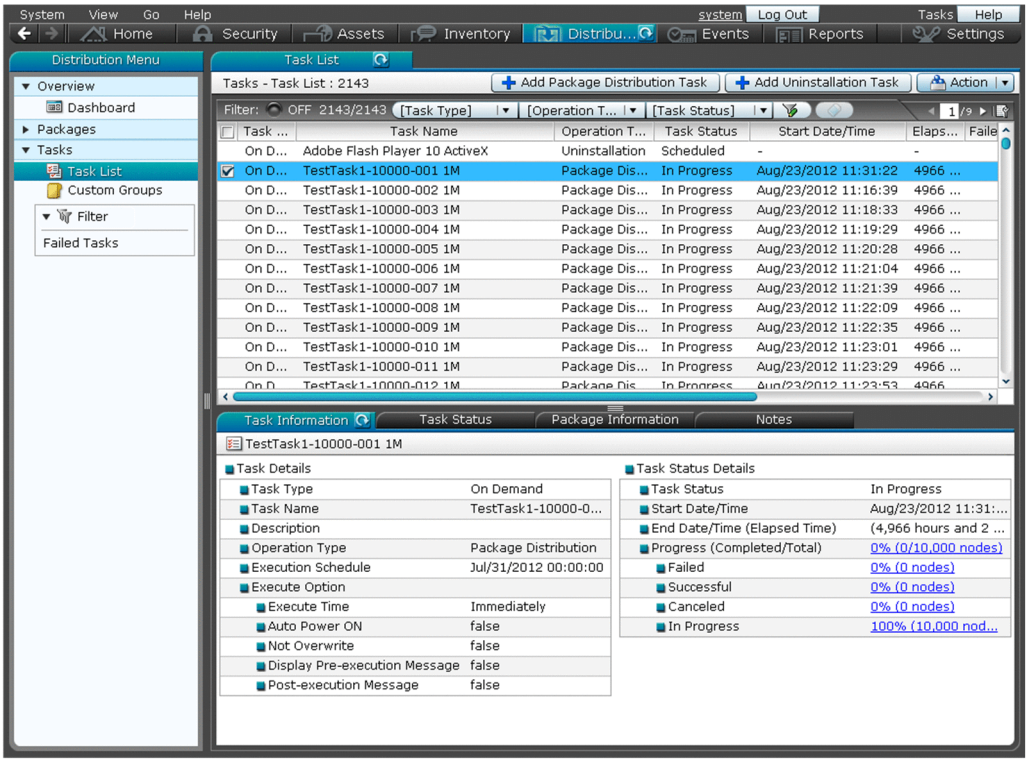
> **Tip**
>
> The users can change the schedule to execute the file distribution later if more urgent or important operation is in progress on their computers.

Related Topics:

- 12.6 Postponing downloads and installation as a user
- 12.5.5 Stopping tasks

(3) Reviewing the results of the task execution

You can review the task execution status in the **Tasks** view of the Distribution module.



We recommend that you check the task execution status on regular basis until the task is complete. If a failure occurs on the computer during the task execution, find the cause of the failure to solve the problem, and then re-execute the task.

Tip

You can also configure JP1/IT Desktop Management to automatically send an email when a distribution management event occurs (such as task completion and task failure).

1. Review the execution status of the task.

   In the **Tasks** view of the Distribution module, select a task to view its execution status. After you select a task, the detailed information of the task is displayed in the tab at the bottom of the information area. In the **Task Information** tab, select **Task Status Details** and then **Progress (Completed/Total)** to check whether the task has been completed successfully.

2. Find the cause of the task failure, and then solve the problem.

   If a failure occurred on the computer during the task execution, click the **Failed** link in the **Task Information** tab. The **Task Status** tab opens with a list of computers on which the task has failed.

   Click the link in **Task Status** to display a dialog box showing the details of the task status. Find the cause of the task failure, and then solve the problem.

3. Re-execute the task.

   When the problem has been resolved, re-execute the task.

   If you re-execute the task with the same settings:

   You can just re-execute the task with the same settings as the previous execution.

If you re-execute the task with different settings:

If you need to change the settings such as execution schedule or target computer, edit or copy the settings, and then re-execute the task.

Now the task will be re-executed on the target computers.

Related Topics:

- 15.8.1 Specifying settings for event notification
- 12.5.6 Re-executing tasks
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.5 Stopping tasks

1.13.3 General procedure for uninstalling software

If the software that is not necessary for the business operation or prohibited from being used has been installed on the computers in your organization, you can use the distribution function to uninstall the software from these computers.

To uninstall software from the computers in your organization:

1. Check the installation status of the software that needs to be uninstalled.

   Check the installation status of the software that needs to be uninstalled, such as software unnecessary for business operation and software prohibited from being used in your organization.

2. Create a software uninstallation plan.

   Create a software uninstallation plan before you begin the procedure. Also notify the users in advance of the details of the uninstallation plan.

3. Uninstall software from the computers.

   To uninstall software, you need to create a task to uninstall the software. The software is uninstalled according to the schedule specified in the task.

4. Review the results of the task execution.

   Review the execution status of the uninstallation task. If a failure occurs on the computer during the uninstallation, find the cause of the failure to solve the problem, and then re-execute the task.

Now the software has been uninstalled from all the target computers.

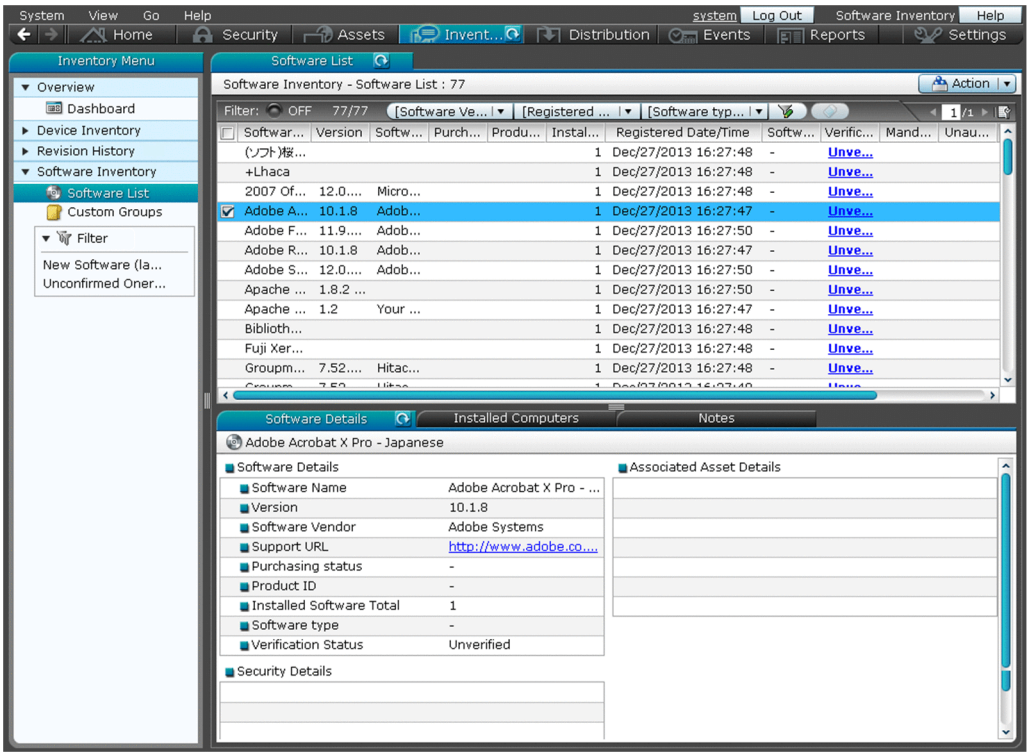
Related Topics:

- 1.13 Distributing software and files

(1) Checking the installation status of the software that needs to be uninstalled

Check the installation status of the software that needs to be uninstalled, such as software unnecessary for business operation and software prohibited from being used in your organization.

To check the software installation status, display the **Software Inventory** view of the Device module. By selecting the software in this view, you can check the computers on which the selected software has been installed in the **Installed Computers** tab at the bottom of the information area.



To check whether any software that is unnecessary for the business operation has been installed on the computers, review the software list. To check whether any software that is prohibited from being used has been installed on the computers, in the software list of the **Software Inventory** view, find the software with a checkmark in the corresponding **Unauthorized** column.

Tip

By using the **Installed Computers** tab, you can uninstall the software from the computers listed in that tab.

Tip

You can also set automatic enforcement in such a way as to automatically uninstall any unauthorized software when it is detected on a computer to which a security policy is applied.

When you find a computer with any unnecessary or unauthorized software installed, check with the user of that computer about the usage status and intended use, and then uninstall it as appropriate.

Related Topics:

- 1.7.1 Setting a security policy

(2) General procedure for creating a software uninstallation plan

Create a software uninstallation plan before you begin the procedure. Also notify the users in advance of the details of the uninstallation plan.

1. Create a software uninstallation plan.

   Consider the following items included in the software uninstallation plan:

   - Computers from which the software is to be uninstalled

- Date and time on which the software is to be uninstalled

  When you set the date and time on which the software is to be uninstalled, you need to consider the impact on the business operation. For example, you can schedule the uninstallation during night to avoid business hours, or divide the target computers into groups to perform uninstallation over several days.

Also, you need to do some preparation before you use the distribution function.

> **Tip**
>
> Before you start the uninstallation procedure, we recommend that you make sure that the software is successfully uninstalled by using the computer for testing.

2. Notify the users of the details of the software uninstallation plan.

   Notify the users in advance of the details of the uninstallation plan to successfully uninstall the software as scheduled and to avoid confusion among the users. For example, notify the users of the following information:

   - Software name
   - Software version
   - Reason of uninstallation
   - Date and time of the uninstallation
   - Cautions

Now the preparation for the software uninstallation is complete.

Related Topics:

- 12.3 Uninstalling software from a computer

(3) Uninstalling software from the computers

If the software that is not necessary for the business operation or prohibited from being used has been installed on the computers in your organization, you can uninstall the software from these computers.

Note that you can uninstall software only from the computers managed online.

To uninstall the software from the computers:

1. Display the Device module.
2. In the menu area, select **Software Inventory** and then **Software List**.
3. In the information area, select the software that you want to uninstall from the computers, and then display the **Installed Computers** tab.
4. In the tab, select the computer from which you want to uninstall the software, and then click the **Uninstall** button.

   You can select more than one computer in the tab to perform the uninstallation procedure in a batch.
5. In the displayed dialog box, create an uninstallation task, and then click the **OK** button.

The software is uninstalled according to the schedule specified in the uninstallation task. You can view the execution status of the task in the **Task List** view of the Distribution module.

Tip

You can also create and execute an uninstallation task from the Distribution module.

Tip

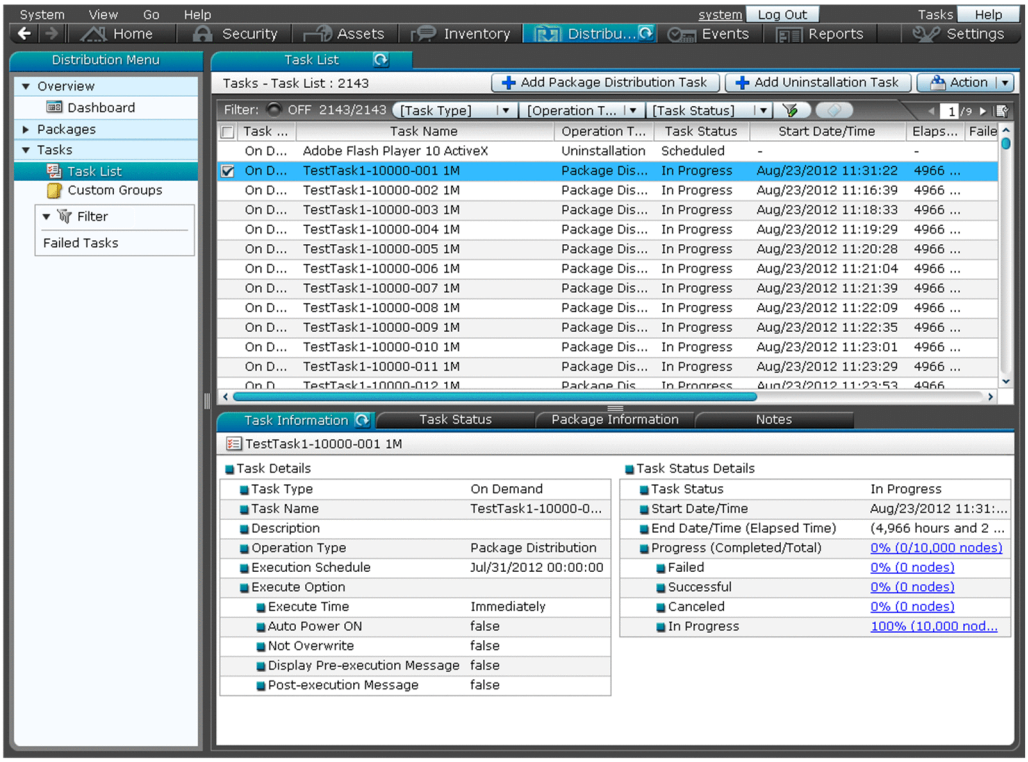
When you specify unauthorized software in a security policy, you can also set automatic enforcement to the security policy in such a way as to automatically uninstall any unauthorized software when it is detected.

Related Topics:

- 1.7.1 Setting a security policy

(4) Reviewing the results of the task execution

You can review the task execution status in the **Tasks** view of the Distribution module.



We recommend that you check the task execution status on regular basis until the task is complete. If a failure occurs on the computer during the task execution, find the cause of the failure to solve the problem, and then re-execute the task.

Tip

You can also configure JP1/IT Desktop Management to automatically send an email when a distribution management event occurs (such as task completion and task failure).

1. Review the execution status of the task.

   In the **Tasks** view of the Distribution module, select a task to view its execution status. After you select a task, the detailed information of the task is displayed in the tab at the bottom of the information area. In the **Task Information** tab, select **Task Status Details** and then **Progress (Completed/Total)** to check whether the task has been completed successfully.

2. Find the cause of the task failure, and then solve the problem.

   If a failure occurred on the computer during the task execution, click the **Failed** link in the **Task Information** tab. The **Task Status** tab opens with a list of computers on which the task has failed.

   Click the link in **Task Status** to display a dialog box showing the details of the task status. Find the cause of the task failure, and then solve the problem.

3. Re-execute the task.

   When the problem has been resolved, re-execute the task.

   If you re-execute the task with the same settings:

   You can just re-execute the task with the same settings as the previous execution.

   If you re-execute the task with different settings:

   If you need to change the settings such as execution schedule or target computer, edit or copy the settings, and then re-execute the task.

Now the task will be re-executed on the target computers.

Related Topics:

- 15.8.1 Specifying settings for event notification
- 12.5.6 Re-executing tasks
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.5 Stopping tasks

1.14 Updating department definitions upon an organizational change

If an organizational change occurs at the beginning of a fiscal year or term, according to the changes, you need to update the department definitions in JP1/IT Desktop Management.

To update department definitions upon an organizational change:

1. Determine department rules for the new organizational system.

   Before the organizational change takes place, determine the security policies and agent settings to be assigned to the departments of the new organizational system.

2. Update department definitions according to the new organizational system.

   Use the `ioassetsfieldutil export` command and the `ioassetsfieldutil import` command to update the department definitions. Also, assign security policies and agent settings to the departments of the new organizational system.

3. Update asset information according to the new organizational system.

   During the data migration period, ask each user to select his/her department in the **End User Form** dialog box. In addition, in accordance with the new organizational system, departmental administrators are to update department-related asset information that was used only in the old organizational system.

4. Delete information that was used only in the old organizational system.

   When updating of asset information is complete, delete the hierarchies of the departments that existed only in the old organizational system, because they are no longer necessary. In addition, if a departmental hierarchy that existed only in the old organizational system is contained in the administration scope of a department administrator, delete the hierarchy from the administration scope.

1.14.1 Determining rules for a new organizational system

Before an organizational change, you need to determine the rules for the new organizational system. The items to be determined are as follows:

- Security policies to be assigned to the departments of the new organizational system
- Agent settings to be assigned to the departments of the new organizational system
- Department administrators of the new organizational system
- The following asset information needs to be migrated from the departments of the old organizational system to the departments of the new organizational system:
  - Hardware asset information
  - Software license information
  - Contract information

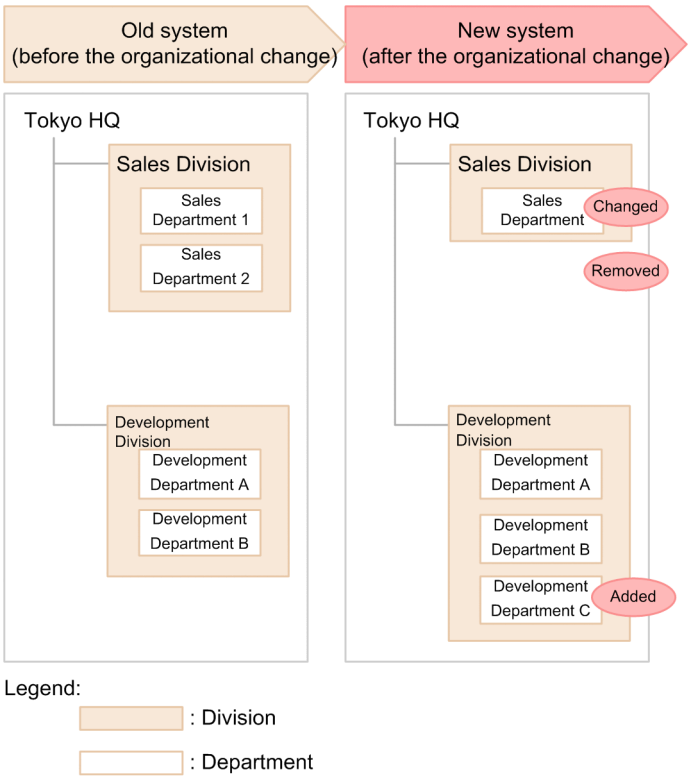
Related Topics:

- 1.7.1 Setting a security policy
- 15.3.1 Managing agent configurations
- 1.3.1 General procedure for determining the settings to be specified for each user account

1.14.2 General procedure for updating department definitions in accordance with the new organizational system

When you update department definitions in accordance with the new organizational system, use the `ioassetsfieldutil export` command and the `ioassetsfieldutil import` command to edit the definitions, and then assign security policies and agent settings to the departments of the new organizational system.

The example below explains how to update department definitions when the organizational change shown in the following diagram occurs:



For example, upon the organizational change on April 1, you need to make the following changes to the department definitions: changing the name of Sales Department 1 to Sales Department, deleting Sales Department 2, and adding Development Department C.

To update department definitions in accordance with the new organizational system:

1. Decide on a period for updating department definitions and a period for migrating asset information.

   You need to update department definitions and then migrate asset information in accordance with the new organizational system. Set periods for updating department definitions and for migrating asset information. The following are examples of such periods:

   - Period for updating department definitions: From March 15 to March 31
   - Period for migrating asset information: From April 1 to April 15

   The organizational change takes place on April 1, so during the migration period, the asset information contains information of both the old and new organizational systems. Therefore, the actual status appears in JP1/IT Desktop Management from April 16.

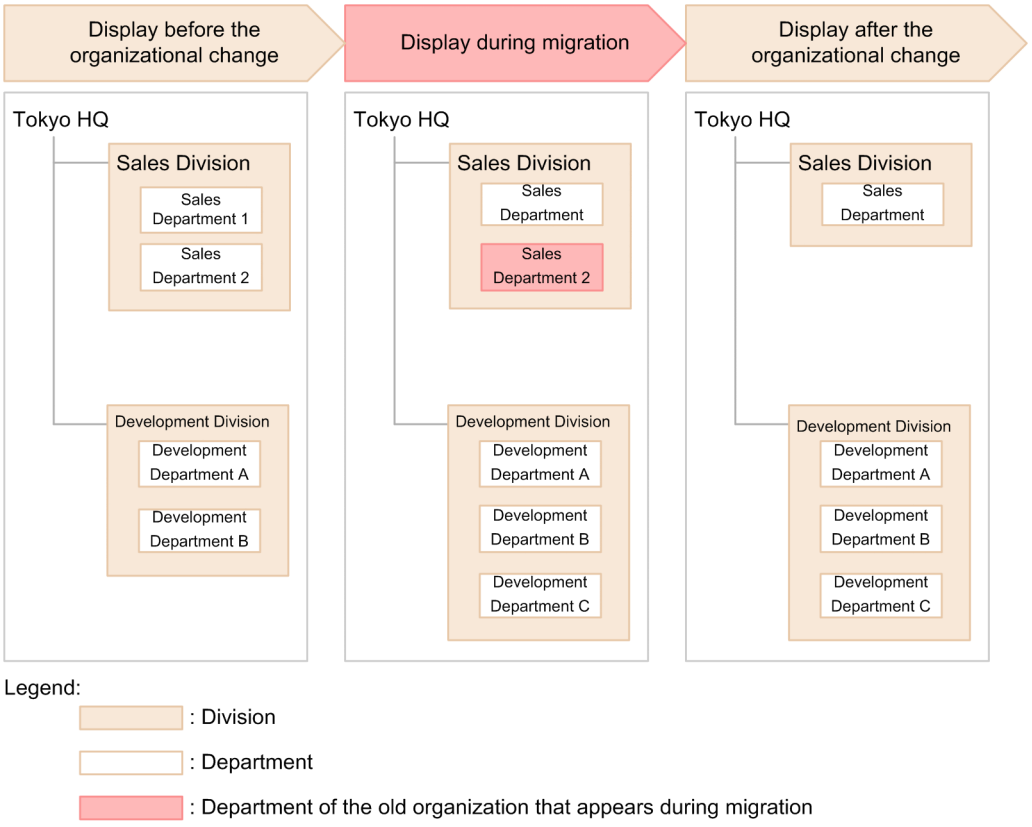
2. Inform the system administrators and departmental administrators of restrictions on the use of JP1/IT Desktop Management.

Inform the system administrators that updating of department definitions and of the hierarchies that appear in the menu area of the Assets module and the Device module is forbidden until the date of the organizational change has passed.

Also, inform the system administrators and departmental administrators that the menu area will appear as follows:

- During the period for updating department definitions: Departments of the new organizational system are displayed in addition to departments of the current organizational system.
- During the period for migrating asset information: Departments of the old organizational system are displayed in addition to departments of the new organizational system.

The following diagram shows how the menu area appears during the migration period:



3. Export department definitions in CSV format.

Use the `ioassetsfieldutil export` command to export department definitions in CSV format.

4. Edit the exported CSV file.

Edit department definitions as follows:

- Change the name of "Sales Department 1" to "Sales Department".
- Delete "Sales Department 2".
- Add "Development Department C".

5. Back up the database.

In case a failure occurs while you are importing the CSV file in step 7, use the database manager to back up the database.

6. Specify the start date and time for entering of user information.

   In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the Asset Field Definitions view that appears, specify the date of the organizational change to be the start date for entering of user information. In this example, specify April 1.

7. Import the CSV file.

   Use the `ioassetsfieldutil import` command to import the department definitions to JP1/IT Desktop Management.

   If the import fails, use the database manager to restore the database that you backed up in step 5.

8. Assign security policies and agent settings to the departments of the new organizational system.

   Assign security policies and agent settings to the departments of the new organizational system in accordance with the assignment rules.

   After assignment is finished, you can create an agent setting installation set for offline management.

9. Add the departments of the new organizational system to the administration scopes of the departmental administrators.

   In the Settings module, in the **Account Management** view, add the departments of the new organizational system to the administration scopes of the departmental administrators.

The department definitions are updated in accordance with the new organizational system.

Related Topics:

- 17.33 ioassetsfieldutil export (exporting the definitions of common management fields and additional management fields)
- A.7 Setting fields in the import file for the definitions of common management fields and additional management fields
- 16.2 Backing up databases
- 17.34 ioassetsfieldutil import (importing the definitions of common management fields and additional management fields)
- 16.3 Restoring databases
- 9.3.5 Assigning security policies
- 15.3.6 Assigning agent configurations
- 4.7 Adding a jurisdiction range

1.14.3 Updating asset information in accordance with the new organizational system

After you finish updating department definitions, ask each user to select his/her department in the **End User Form** view during the migration period.

In accordance with the new organizational system, departmental administrators update department-related asset information that was used only in the old organizational system. The information to be updated is as follows:

- Hardware asset information
- Software license information
- Contract information

Related Topics:

- 11.1.2 Editing hardware asset information
- 11.2.5 Editing software license information
- 11.3.2 Editing contract information
- 11.4 Importing asset information
- 11.5 Exporting asset information

1.14.4 General procedure for deleting information used only in the old organizational system

After you finish updating asset information, delete the hierarchies of the departments that exist only in the old organizational system because they are no longer necessary. Also, delete the hierarchies of the departments that exist only in the old organizational system from the administration scopes of department administrators. To delete the information that is used only in the old organizational system:

1. From the administration scopes of the department administrators, delete the departments that have been deleted from the department definitions.

   If departments that have been deleted from the department definitions are still included in the administration scopes of department administrators, do the following: In the Settings module, select **User Management** and then **Account Management**. In the Account Management view that appears, delete the departments from the administration scope.

2. Delete the hierarchies of the departments of the old organizational system that have already been deleted from the department definitions.

   From the menu area of the Assets module or Device module, display the **Delete Hierarchies Used in Old Organization** dialog box. In this dialog box, batch-delete the hierarchies of departments that have already been deleted from the department definitions. Deleting the hierarchies of the departments of the old organizational system ensures that the hierarchies in the department definitions are consistent with those displayed in the menu area.

   Note that if you delete the hierarchy of a department to which asset information is assigned, the department of the assigned asset information changes to `Unknown`.

   Important note

   If the security policies assigned to the deleted department differ from the security policies assigned to the `Unknown` department, the security policies assigned to the `Unknown` department are applied to the device. If you do not want to change which security policies are assigned, make sure that you migrate asset information to the departments of the new organizational system before deleting the departments of the old organizational system.

Information used only in the old organizational system is now deleted.

Related Topics:

- 4.8 Removing a jurisdiction range
- 6.31 Removing only hierarchies that were used in the old organizational system

2 Registering a Product License

This chapter describes how to register a product license.

2.1 Registering a product license

By registering product licenses in JP1/IT Desktop Management, you can manage as many devices as the number of licenses you have registered.

To register a product license:

1. Display the Login window.
2. Click the **License** button.
3. In the displayed dialog box, click the **Register License** button.
4. In the displayed dialog box, select a license key file, and then click the **Open** button.

License registration is complete.

> **Tip**
>
> If you are not registering a license for the first time, you can also register a license from the **License Details** view, which is displayed by selecting **Product Licenses** in the Settings module and then **License Details**. Click the **Register License** button. In the displayed dialog box, select a license key file, and then click the **Open** button to complete license registration.

> **Tip**
>
> If you are not registering a license for the first time, you can also register a license from the **About** dialog box, which is displayed by selecting **Help** in the top left corner of the view and then selecting **About**. Click the **Register License** button. In the displayed dialog box, select a license key file, and then click the **Open** button to complete license registration.

Related Topics:

- 2.3 Adding a product license

2.2 Checking product license information

You can check the information for registered product licenses in one of the following three ways:

- In the Login window, click the **License** button to display the **License Details** dialog box.
- In the Settings module, select **Product Licenses** and then **License Details** to display the **License Details** view.
- In the top left corner of the view, select **Help** and then **About** to display the **About** dialog box.

If you do not have enough product licenses, purchase additional product licenses. To register a purchased product license, display one of the dialog boxes and view mentioned above, and then click the **Register License** button. In the displayed dialog box, select a license key file.

Related Topics:

- 2.1 Registering a product license

2.3 Adding a product license

Product licenses are required to use JP1/IT Desktop Management to manage the devices in your organization.

If you do not have enough product licenses, purchase additional product licenses. You can then add the product licenses you have purchased by registering them.

Related Topics:

- 2.1 Registering a product license

3 Logging in to the Operation Window

This section describes how to log in to the Operation window of JP1/IT Desktop Management.

3.1 Logging in

Perform user authentication in the Login window. If successfully authenticated, you can then log in to JP1/IT Desktop Management.

You need to register a license for JP1/IT Desktop Management when logging in for the first time. To register the license, click the **License** button.

To log in:

1. Enter the following URL into the address bar of your Web browser:

   http://*management-server-IP-address-or-host-name*:*port-number-for-connection-from-administrator-computer*#/jp1itdm/

   #: This is the port number that was specified in the **Port Number Settings** view during setup. The default value of 31080 is specified for a simple installation.

2. Enter the user ID and password.

3. Click the **Log In** button.

The Home module is displayed if the user account is successfully authenticated.

The default user ID is `system`. The default password is `manager`. When you use the default user ID and password to log in, the **Change Password** dialog box is displayed. Change the password in the dialog box. Note that the **Change Password** dialog box is also displayed if you use a newly created user account to log in for the first time.

Tip

The password is valid for 180 days from the setup date. Beginning seven days prior to expiration, you will be prompted to change the password when logging in. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Important note

If login fails three times consecutively, the user account is locked. You must unlock the user account before you can use it to log in.

Related Topics:

- 4.9 Unlocking a user account

3.2 Setting user account information

After logging in to JP1/IT Desktop Management, set user account information.

Click the link of the user ID to the left of the **Log Out** button, and then edit the user account information in the displayed dialog box.

Specify the following information for the user account:

- Name of the account user
- Email address of the account user

After you specify an email address for a user account, digest reports and notifications of search completion or event occurrences can be sent to that email address. We recommend that you specify an email address, so that the user can be made aware of the operating status without having to frequently check the operation window. Note that to receive such notifications, you also need to specify the recipients of digest reports, the search conditions, and the event notification settings, in addition to the email address.

Tip

You can also set user account information in the **Account Management** view by selecting **User Management** in the Settings module and then **Account Management**. In addition, you can also add a new user account in the **Account Management** view.

3.3 Changing the default password

When you log in to JP1/IT Desktop Management for the first time by using the built-in account or a newly created account, you are required to change the password. If an administrator who has user account management permissions has changed the user account password, you are required to change the password the next time you log in. Make sure to change the default password to enhance security. After the password is changed, you must use the new password from the next login.

Tip

The password is valid for 180 days from the setup date. Beginning seven days prior to expiration, you will be prompted to change the password when logging in. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Tip

If the password you specified is easy to guess, your user account might be used illegally. We recommend that you specify a strong password by following the password policies described below:

- Use a combination of uppercase letters, lowercase letters, numbers, and symbols.
- Do not use an obvious sequence of characters, such as 12345.
- Do not use your name or birthday, the name or birthday of a friend or relative, or a word taken from a dictionary.

To change the password for the user account that is currently logged in, click the link of the user ID to the left of the **Log Out** button, and then change the password in the displayed dialog box.

An administrator who has user account management permissions can change the password for each user account in the **Account Management** view by selecting **User Management** in the Settings module and then **Account Management**.

3.4 Logging out

After you have finished performing operations in JP1/IT Desktop Management, log out from the operation window.

To log out:

1. Click the **Log Out** button at the top of the window.
2. In the displayed dialog box, click **OK**.

You are logged out from the operation window, and the Login window is displayed.

> **Tip**
>
> You can also log out by selecting **Log Out** from the **System** menu at the top of the window.

4 Managing User Accounts

This section describes how to manage user accounts.

4.1 Adding a user account

You can add a user account by selecting **User Management** in the Settings module, and then **Account Management**. The functions a user can use vary depending on his or her permissions, so assign adequate permissions to users.

Note that to add user accounts, you must have user account management authority.

To add a user account:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Add** button.
4. In the dialog box that appears, enter the user account information, and then click **OK**.

The user account is added and listed in **User Account List**.

Related Topics:

- 4.2 Editing a user account
- 4.3 Removing a user account

4.2 Editing a user account

You can edit a user account if you want to change the password or access permissions for the account.

The range of user accounts you can edit depends on the permissions assigned to you. If you do not have user account management authority, you can edit only your own user account. If you have user account management authority, you can edit all user accounts.

To edit your own user account:

1. Click the **user-account-name** link on the top of the operation window.

2. In the dialog box that appears, edit the user account information, and then click **OK**.

Your user account is updated.

To edit another administrator's user account:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Edit** button for the account you want to edit.
4. In the dialog box that appears, edit the user account information, and then click **OK**.

The selected user account is updated.

> **Tip**
>
> If the administrator user account that you want to edit is locked, unlock the account in the **Edit User Profile** dialog box.

Related Topics:

- 4.1 Adding a user account
- 4.3 Removing a user account

4.3 Removing a user account

You can remove a user account that is no longer used. However, you cannot remove the built-in account or your own account. Note that you must have user account management authority to remove a user account.

To remove a user account:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, select the user account you want to remove, and then click the **Remove** button.
   You can select multiple user accounts and remove them simultaneously.
4. In the dialog box that appears, click **OK**.

The selected user account or accounts are removed.

Related Topics:

- 4.1 Adding a user account
- 4.2 Editing a user account

4.4 Changing your own password

We recommend that you periodically change your user account password to improve security.

> **Tip**
>
> Passwords are valid for 180 days from the date they are set. From the 7th day prior to expiration, you will be prompted to change your password when you log in. If you are prompted, change your password. If 180 days have passed since the date your password was set, the **Change Password** dialog box appears when you log in.

To change your own password:

1. Click the **user-account-name** link on the top of the operation window.

2. In the dialog box that appears, click the **Change Password** button.
3. In the dialog box that appears, change the password, and then click **OK**.
4. Click **OK**.

The password for your user account is updated.

> **Tip**
>
> If the password you specified is easy to guess, your user account might be compromised. We recommend that you specify a strong password according to the following guidelines:
>
> - Use a combination of upper-case characters, lower-case characters, numbers, and symbols.
> - Do not use consecutive characters, such as 12345.
> - Do not use the name or birthday of yourself, a friend, or a relative, or a word taken from a dictionary.

Related Topics:

- 4.5 Changing another administrator's password
- 4.6 Resetting a password

4.5 Changing another administrator's password

We recommend that you periodically change user account passwords to improve security.

Tip

Passwords are valid for 180 days from the date they are set. From the 7th day prior to expiration, you will be prompted to change passwords when you log in. If you are prompted, change the password. If 180 days have passed since a password was set, the **Change Password** dialog box appears when you log in.

The range of passwords that you can change depends on the authority assigned to you. If you do not have user account management authority, you can change only your own password. If you have user account management authority, you can change the passwords of all user accounts.

To change another administrator's password:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Edit** button of the user account whose password you want to change.
4. In the dialog box that appears, change the password, and then click **OK**.

The password for the selected user account is updated.

When you change another administrator's password, the password is reset to the default. After the administrator logs in with the new password, the administrator is prompted to change the password.

Tip

If the password you specified is easy to guess, the user account might be compromised. We recommend that you specify a strong password according to the following guidelines:

- Use a combination of upper-case characters, lower-case characters, numbers, and symbols.
- Do not use consecutive characters, such as 12345.
- Do not use the name or birthday of yourself, a friend, or a relative, or a word taken from a dictionary.

Related Topics:

- 4.4 Changing your own password
- 4.6 Resetting a password

4.6 Resetting a password

If an administrator forgets his or her password, another administrator can reset the password to the default.

Note that you must have user account management authority to reset a password.

To reset a password:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Edit** button for the user account whose password you want to reset.
4. In the dialog box that appears, enter a password, and then click **OK**.
   The password is set for the selected user account.
5. Inform the administrator whose password has been reset, of the new password.
   Also inform the administrator that the password needs to be changed after the administrator logs in JP1/IT Desktop Management using the reset password.

The administrator logs in JP1/IT Desktop Management using the reset password. After login, the administrator is prompted to change the password.

Related Topics:

- 4.4 Changing your own password

4.7 Adding a jurisdiction range

You can add a jurisdiction range for a user account. After adding a jurisdiction range, you can manage devices and other hardware assets within the jurisdiction range. The functions a user can use vary depending on his or her permissions for assigning jurisdiction ranges, so assign adequate permissions to users.

Note that you must have user account management authority to add a jurisdiction range.

To add a jurisdiction range:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Add** button or the **Edit** button.
4. In the dialog box that appears, select **Set the administration scope for this user account**.
5. In **Jurisdiction Range**, click the **Add** button.
   In the dialog box that appears, select the jurisdiction range you want to add, and then click **OK**.

The jurisdiction range is added to the user account.

Related Topics:

- 4.8 Removing a jurisdiction range

4.8 Removing a jurisdiction range

You can remove a jurisdiction range from a user account.

Note that you must have user account management authority to remove a jurisdiction range.

To remove a jurisdiction range:

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Edit** button.
4. In the dialog box that appears, select the jurisdiction range that you want to remove from **Jurisdiction Range**, and then click the **Remove** button.
5. Click **OK**.

The selected jurisdiction range for the user account is removed.

Related Topics:

- 4.7 Adding a jurisdiction range

4.9 Unlocking a user account

A user account is locked if the user fails to log in three consecutive times. You must unlock the account before it can be used.

To unlock a user account:

1. Log in as a user who has user account management authority.
2. In the Settings module, select **User Management**, and then **Account Management** to display the **Account Management** view.
3. Click the **Edit** button of the locked user account.
4. In the dialog box that appears, select **Enabled** from **Status**.

The user account is unlocked.

> **Tip**
>
> If no other administrator has user account management authority, restart the management server. The user account is unlocked.

5 Window Operations

This chapter describes common operations that you can perform in operation windows in JP1/IT Desktop Management.

5.1 Setting the panels to be displayed and their layout

You can change the types of panels that are displayed in the Home module and other modules when you select **Overview** and then **Dashboard**, and you can change the layout of those panels.

To set the panels to be displayed and their layout:

1. Display the Home module or another module.
2. From the **View** menu in the upper left area of the window, select **Panel Layout**.
3. In the dialog box that appears, select the panels that you want to display and the layout in which they are to be displayed.
4. Click **OK**.

The panels that are displayed in the view and their layout change according to your settings.

Tip

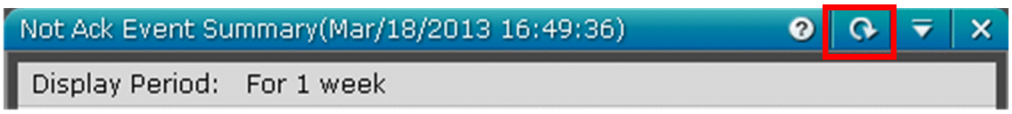
To restore the default view, from the **View** menu, select **Change View Default**.

5.2 Refreshing information in a view

You can refresh the information in the view or panel that is currently being displayed, by clicking the update icon ( ). Views refresh periodically; however, to check the latest information at a time of your choosing, manually refresh the view.

The refresh icon appears in buttons that are displayed at the top of a view, in the menu area, and in the headline of the information area.

The refresh icon also appears in the title bar of a panel that is displayed in a view.



Tip

To set a panel to automatically refresh, from the panel menu ( ), select **Specify Automatic Update Interval**, and then specify the refresh interval in the dialog box that appears. You can apply the interval that you specify to all panels.

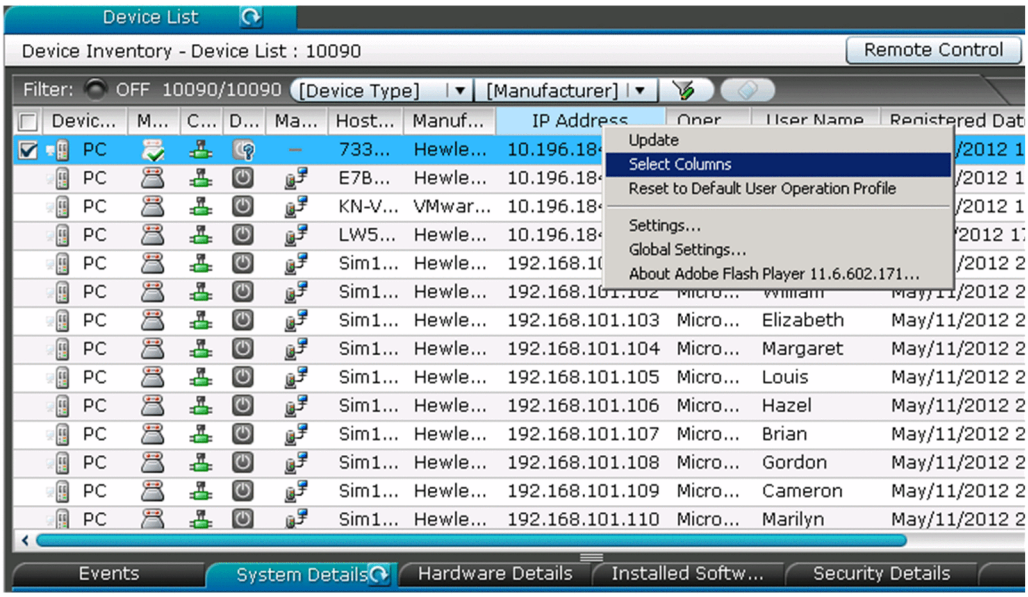
5.3 Changing items displayed in a list

You can change the management items that are displayed in the information area.

We recommend that you display the management items that you often refer to in your work.

To change the items that are displayed:

1. Display the information area that contains the items that need to be changed.
2. Right-click the title of a list item, and then select **Select Columns**.



3. In the dialog box that appears, select the management items that you want to display in the list.
4. Click **OK**.

The management items that are displayed in the information area are changed.

> **Tip**
>
> To restore the default items, right-click the title of an item in the list, and then select **Reset to Default User Operation Profile**.

> **Tip**
>
> In the Assets module, you can freely create management items that you want to display in the information area. To create a management item, from the Settings module, select **Asset Management**, select **Asset Field Definitions**, and then add the management item in the **Asset Field Definitions** view that appears.

Related Topics:

- 15.5.1 Adding asset management items

5.4 Common view operations

This section describes operations that are common to all views in JP1/IT Desktop Management.

Changing the displayed view according to your operation history

You can move backward and forward through your operation history to show previously-displayed views by clicking the  buttons that are located at the top of the operation window. To show or hide these buttons, select **Option** from the **View** menu.

Refreshing the information in a view

You can refresh the information in the view or panel that is currently being displayed.

Changing the items that are displayed in a list

You can change the management items that are displayed in the information area.

Filtering listed information

You can limit the information that is displayed in a list by using filters to specify display conditions.

Selecting multiple items in a list

You can select multiple items from a list that is being displayed in the information area.

You can select all items by selecting the check box in the left upper corner of the list. You can select multiple items by selecting the check box to the left of each item that you want to select, or by holding the **Ctrl** key while you click each item that you want to select. Alternatively, you can click one item, and then hold down the **Shift** key while you click another item to select all items between and including those two. When you use the **Ctrl** key or the **Shift** key to select items, click a place outside that item's check box.

When multiple items are selected, you can cancel the selection of an individual item by holding down the **Ctrl** key while clicking a selected item, or by clearing the check box of an item.

Using the menu that appears when you right-click the mouse

If you right-click inside a view, the currently-executable operations appear.

For example, if you right-click a group in the menu area, you can add a new tab to the information area. You can also perform actions such as editing a group, editing a filter, editing a custom group, and refreshing the information that is being displayed.

Additionally, by right-clicking the list in the information area, you can perform the same operations that are available as buttons or in the **Action**. You can also perform actions such as copying the information in the list to the clipboard, or changing the items that are displayed in the list.

Using a custom group

You can freely arrange device information or asset information into groups. By creating a group, you can register and manage information according to your needs. Such a group is called a custom group.

Switching list pages

If there are many items that need to be displayed in the list, the list is displayed across multiple pages. Move to the next page by clicking the  button in the upper right corner of the list. Return to the previous page by clicking the  button. You can also jump to a specific page by specifying a page number in the  area.

To change the number of items to be displayed on one page, click  , and then select from 100, 250, 500, or 1,000 items per page. The default setting is 250 items per page.

Related Topics:

- 5.2 Refreshing information in a view
- 5.3 Changing items displayed in a list

5.5 Managing user-defined groups

5.5.1 Adding a user-defined group

You can add a user-defined group by using **Device List (User-Defined)** in the menu area.

To add a user-defined group:

1. In the menu area, point to **Device List (User-Defined)**.
2. Click the  icon that appears to the right of the item.
3. From the menu that appears, click  .
4. In the dialog box that appears, click **Add**.
5. In the dialog box that appears, specify the User-defined group name and User-defined group conditions, and then click **OK**.
6. Click **OK**.

The user-defined group is added to the menu area.

Related Topics:

- 5.5.2 Changing the name of a user-defined group
- 5.5.3 Removing a user-defined group
- 5.5.4 Changing the user-defined group conditions

5.5.2 Changing the name of a user-defined group

You can change the name of a user-defined group in the menu area.

To change the name of a user-defined group:

1. In the menu area, in **Device List (User-Defined)**, point to the group whose name you want to change.
2. Click the  icon that appears to the right of the item.
3. From the menu that appears, click  .
4. In the text area that appears, enter the name of the user-defined group.

The name of the user-defined group is changed.

Tip

You can also change the name of a user-defined group by using the dialog box that appears by clicking **Device List (User-Defined)** in the menu area to edit the user-defined group.

Related Topics:

- 5.5.1 Adding a user-defined group
- 5.5.3 Removing a user-defined group
- 5.5.4 Changing the user-defined group conditions

5.5.3 Removing a user-defined group

In the menu area, you can remove a user-defined group that is no longer necessary.

To remove a user-defined group:

1. In the menu area, in **Device List (User-Defined)**, point to the group that you want to delete.
2. Click the  icon that appears to the right of the item.
3. From the menu that appears, click  .
4. In the dialog box that appears, click **OK**.

The user-defined group is removed.

Tip

You can also delete a user-defined group as follows: In the menu area, click **Device List (User-Defined)**, and then use the dialog box that appears.

Related Topics:

- 5.5.1 Adding a user-defined group
- 5.5.2 Changing the name of a user-defined group
- 5.5.4 Changing the user-defined group conditions

5.5.4 Changing the user-defined group conditions

You can change the user-defined group conditions in the dialog box that appears by clicking **Device List (User-Defined)** in the menu area.

To change the user-defined group conditions:

1. In the menu area, point to **Device List (User-Defined)**.

2. Click the  icon that appears to the right of the item.

3. From the menu that appears, click  .

4. In the dialog box that appears, click the **Edit** button for the user-defined group whose conditions you want to change.

5. In the dialog box that appears, edit the user-defined group conditions, and then click **OK**.

6. Click **OK**.

The user-defined group conditions are changed.

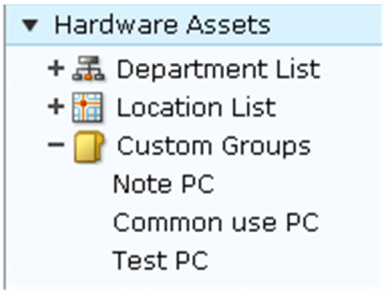
Related Topics:

- 5.5.1 Adding a user-defined group
- 5.5.2 Changing the name of a user-defined group
- 5.5.3 Removing a user-defined group

5.6 Managing custom groups

5.6.1 Adding a custom group

In the menu area, you can assign information, such as hardware asset information and device information, to any group. Such a group is called a custom group. If you want a group that contains only certain information, add a custom group.



For example, you can make use of custom groups in the following ways:

- In the Assets module, within the Hardware Assets custom group, add a custom group called **Under Repair** to manage information about devices that are being repaired.
- In the Device module, within the Software Information custom group, add a custom group called **Internal Software** to manage information about software created by your company.

To add a custom group:

1. In the menu area, point to **Custom Group**.
2. Click the  icon that appears to the right of **Custom Group**.
3. From the menu that appears, click  .
4. In the text area that appears, enter the name for the custom group.

The custom group is added to the menu area.

> **Tip**
>
> You can also add a custom group as follows: In the menu area, right-click **Custom Group**, and then use the menu that appears.

Related Topics:

- 5.6.2 Changing the name of a custom group
- 5.6.3 Removing a custom group
- 5.6.4 Adding information to a custom group
- 5.6.5 Removing information from a custom group

5.6.2 Changing the name of a custom group

You can change the name of a custom group if the purpose of the information that it contains has changed.

To change the name of a custom group:

1. In the menu area, inside **Custom Group**, point to the group whose name you want to change.
2. Click the  icon that appears to the right of the item.
3. From the menu that appears, click  .
4. In the text area that appears, enter the new name for the custom group.

The name of the custom group is changed.

> **Tip**
>
> You can also change the name of a custom group by right-clicking the custom group in the menu area, and then using the menu that appears.

Related Topics:

- 5.6.1 Adding a custom group
- 5.6.3 Removing a custom group
- 5.6.4 Adding information to a custom group
- 5.6.5 Removing information from a custom group

5.6.3 Removing a custom group

You can remove a custom group that is no longer needed.

To remove a custom group:

1. In the menu area, within **Custom Group**, point to the group that you want to remove.
2. Click the  icon that appears to the right of the item.
3. From the menu that appears, click  .
4. In the dialog box that appears, click **OK**.

The custom group is removed.

> **Tip**
>
> You can also remove the custom group by right-clicking the custom group in the menu area, and then using the menu that appears.

Related Topics:

- 5.6.1 Adding a custom group
- 5.6.2 Changing the name of a custom group
- 5.6.4 Adding information to a custom group
- 5.6.5 Removing information from a custom group

5.6.4 Adding information to a custom group

To group information according to purpose, add the information to a custom group you created.

To add information to a custom group:

1. In the information area, display the information that you want to add to the custom group.
2. Select the information that you want to add to the custom group, and then from **Action**, select **Add to Custom Groups**.
3. In the dialog box that appears, select the custom group to which you want to add the information, and then click **OK**.

The information is added to the custom group that you selected.

Tip

You can also add information to a custom group by right-clicking the information in the information area, and then selecting **Add to Custom Groups**.

Tip

You can also add information to a custom group by dragging the information from the information area and dropping it into a custom group in the menu area.

Related Topics:

- 5.6.1 Adding a custom group
- 5.6.2 Changing the name of a custom group
- 5.6.3 Removing a custom group
- 5.6.5 Removing information from a custom group

5.6.5 Removing information from a custom group

If you want to change the grouping of information that you added to a custom group, you can remove that information from the custom group.

To remove information from a custom group:

1. Select the custom group from which you want to remove information.

2. In the information area, select the information that you want to remove, and then from the **Action** menu, select **Remove from Custom Group**.

3. In the dialog box that appears, click **OK**.

The information is removed from the selected custom group.

> **Tip**
>
> You can also remove the information by right-clicking the information to be removed in the information area, and then selecting **Remove from Custom Group**.

Related Topics:

- 5.6.1 Adding a custom group
- 5.6.2 Changing the name of a custom group
- 5.6.3 Removing a custom group
- 5.6.4 Adding information to a custom group

5.7 Managing filters

5.7.1 Saving a filter

You can save a filter (a set of filtering conditions) in order to reuse it. If you save the filtering conditions that you frequently use in your work, you can quickly narrow down the desired information.

To save a filter:

1. In the menu area, point to **Filter**, and then click  .
2. Enter a name for the filter that was added to the **Filter** list.
3. In the **Edit Filter Conditions** dialog box that appears, set the filter conditions.
4. Click **Save As**.
   Before saving the filter, you can click **Apply** button and view the filter results to check whether the specified conditions meet your needs.

The filter is saved and added to **Filter** in the menu area.

Note that you can also display the **Edit Filter Conditions** dialog box by clicking the  button.

Tip

You can also save a filter by right-clicking **Filter** in the menu area, and then selecting **Add New Filter**.

Tip

You can export or import filters by executing commands.

Related Topics:

- 17.20 ioutils exportfilter (exporting filter settings)
- 17.21 ioutils importfilter, importing filter settings
- 5.7.2 Deleting a filter

5.7.2 Deleting a filter

You can delete a filter that is no longer needed.

To delete a filter:

1. In the menu area, point to the filter that you want to delete.
2. Click the  icon that appears to the right of the item.

3. In the menu that appears, click the  icon.

4. In the dialog box that appears, click **OK**.

The filter is deleted.

> **Tip**
>
> You can also delete a filter by right-clicking the filter in the menu area and then selecting **Remove Custom Filter**.

Related Topics:

- 5.7.1 Saving a filter

5.8 Precautions to observe when using the operations window

- If you are using the Windows magnifying glass function, close that function before logging out of JP1/IT Desktop Management.
- The operation window might be displayed incorrectly if the web browser is set to block cookies. If this is the case, take the following steps to add the management server to the set of sites that the web browser trusts:

  For Internet Explorer

  1. From the **Tools** menu, select **Internet Options**.
  2. In the **Internet Options** dialog box, within the **Security** tab, click **Trusted sites**.
  3. Click **Sites**.
  4. In the **Trusted sites** dialog box, specify the following settings, and then click the **Add** button:
     - Clear the **Require server verification (https:) for all sites in this zone** check box.
     - In **Add this website to the zone**, enter the address of the management server.
  5. Click the **Close** button.
  6. Click the **Custom level** button, and then make sure that **Active scripting** is set to **Enable**.

     If it is not set to **Enable**, select **Enable**. This prevents the following problems: If JavaScript is disabled in the web browser settings, Help links might not be displayed correctly or the Help might not work.
  7. Click the **OK** buttons until the **Internet Options** dialog box is closed.
  8. Restart the web browser.

  The management server is added to the set of sites that the web browser trusts.

  For Firefox

  1. From the **Tools** menu, select **Options**.
  2. In the **Options** dialog box, click **Privacy**.
  3. Select **Use custom settings for history**, and then click **Exceptions**.
  4. In the **Exceptions - Cookies** dialog box, within the **Address of website** box, enter the address of the management server, and then click **Allow**.
  5. Click **Close**.
  6. Restart the web browser.

  The management server is added to the set of sites that the web browser trusts.
- If a dialog box is displayed, but the **OK** button is not clicked for more than 60 minutes, a timeout occurs. Note that in such a case, operations that had been performed up to that point are not saved.
- In Internet Explorer 9 or 10, if you click the **Browse** button in the views below, and if you perform an operation in the JP1/IT Desktop Management operations window while the file selection view is displayed, an internal error might occur, or the operation might be interrupted. Make sure that you close the file selection view before performing operations in the JP1/IT Desktop Management operations window.
  - The **Import Assets** view
  - The **Install Software** view
  - The **File Distribution** view
- If the **malformed request** dialog box or the **unexpected error** dialog box appears when you open the operation window or when you log in, delete the temporary Internet files in the web browser. Note carefully that this is likely to happen especially when JP1/IT Desktop Management is installed. The procedure for deleting the temporary Internet files in each web browser is explained below:

For Internet Explorer 6

1. From the **Tools** menu, select **Internet Options**.
2. In the **Internet Options** view, select the **General** tab, and then in the **Temporary Internet files**area, click **Delete Files**.
3. In the **Delete Files** view, select **Delete all offline content**, and then click **OK**.
4. In the **Internet Options** view, click **OK**.

For Internet Explorer 7

1. From the **Tools** menu, select **Internet Options**.
2. In the **Internet Options** view, select the **General** tab, and then in the **Browsing history** area, click **Delete**.
3. In the **Delete Browsing History** view, within the **Temporary Internet files** area, click **Delete Files**.
4. In the **Delete Files** view, click **Yes**.

For Internet Explorer 8, 9, or 10

1. From the **Safety** menu, select **Delete Browsing History**.
2. In the **Delete Browsing History** view, select **Temporary Internet files**, and then click **Delete**.

For Firefox

1. From the **Tools** menu, select **Clear Recent History**.
2. In the **Clear Recent History** view, click the expand button to the left of **Details**.
3. Select **Cache** from the list that appears, and then click **Clear Now**.

- If the web browser is Internet Explorer and the pop-up blocker is enabled, pop-up windows might not appear even if you actively try to display them. In this case, perform the following procedure to add the address of the management server to the list of allowed sites:

  1. From the **Tools** menu, select **Internet Options**.
  2. In the **Internet Options** view, select the **Privacy** tab, and then click the **Settings** button.
  3. In the **Pop-up Blocker Settings** window, for **Address of Web site to allow**, enter the address of the management server, and then click **Add**.

6

Device Management

This chapter describes how to understand the current device status by collecting information from internal devices.

6.1 Starting to manage devices

Before managing devices, you need to set which devices are management targets. After management targets are set, you can know the current device status from the automatically collected information, and perform security management, asset management, and distribution management.

You can use the following methods to set a device as a management target.

How to search for devices:

This method searches for devices and sets the detected devices as management targets.

If you do not know the current device status, you can perform a search on the devices that are connected to the network, and then set detected devices as management targets. Also, you can search Active Directory, and set a device managed in Active Directory as a management target of JP1/IT Desktop Management.

How to install an agent on a computer:

Install an agent on a computer you want to manage, and then connect the computer to the network. When the computer that has the agent installed is connected with the management server, the computer is automatically set as a management target.

How to detect a device by using the network monitoring function:

This method uses the network monitoring function to detect a device that is trying to connect to the network. You can set the detected device as a management target of JP1/IT Desktop Management.

How to link with the MDM system:

By linking a smart device with the MDM system, you can set a smart device managed by the MDM system as a management target of JP1/IT Desktop Management.

We recommend that you install an agent on all computers to manage all devices within the organization.

There are two ways to install an agent on a computer. You can manually install the agent by creating an installer of the agent (agent installer) which can complete the installation and setup in one step. Alternatively, you can automatically install the agent by distributing the agent at the same time when searching for devices.

To manage a device other than a computer, search for the device and set the detected device as a management target.

To manage the device, click the **Getting Started** button. The **Getting Started** wizard starts when the button is clicked. You can use this wizard to search for a device or create an agent installer.

Tip

You can also start the **Getting Started** wizard by selecting **Getting Started** in the **Go** menu.

Registering a detected device

Based on the following information, you can know whether a device, detected either by performing a search or using network detection, has already been set as a management target:

- Host ID[#1]
- IMEI[#2]
- Host name
- MAC address
- IP address

#1: The host ID is a unique ID generated by the agent to identify a device.

#2: IMEI is used when a smart device is managed by linking it with the MDM system.

If the detected device is determined not to be a management target based on the above information, the device is handled as a newly detected device.

6.2 Creating an installation set

To manage computers in your organization by installing agents on the computers, you need to create an installation set. You can upload the created installation set to a Web portal so that users can download it to their computers. You can also record the installation set on CDs or DVDs and distribute them to users. In this way, the users can install agents on their computers by simply running the installation set on their computers.

Create an installation set as described below.

To create an installation set:

1. In the top of the view, select the **Go** menu, and then **Getting Started Wizard**.
2. In the displayed dialog box, click the **Next** button.
3. Select **Create Agent Installer**, and then click the **Next** button.
4. Select an agent configuration you want to apply to each computer, and then click the **Create** button.
   A dialog box for downloading an installation set appears. The default file name displayed in the dialog box is `ITDMAgt.exe`.
   An agent configuration defines the actions of each agent. You can add a new agent configuration in the Agent Configurations view. To display the Agent Configurations view, in the Settings module, select **Agent** and then **Agent Configurations**.
   To change the installation folder or to specify an account with Administrator privileges to allow general users to install agents on their computers, select the following check boxes and enter necessary information:

   Change Installation Folder

   Allows you to change the folder to which to install an agent.

   To change the installation folder, select this check box, and then enter the new installation destination for an agent under **Installation Folder**.

   Set the account to install Agent.

   Allows you to select whether to specify an account with Administrator privileges to allow users to install agents on their computers. This setting is enabled only for the task of installing agents on the computers running the following OSs: Windows 2000, Windows XP, and Windows Server 2003.

   The users need to have Administrator privileges on their computers in order to install agents on the computers.

   If you select this check box, users who do not have Administrator privileges can install agents by using the specified account. The use of the Administrator privileges is restricted to the task of installing an agent. This setting is therefore useful when you want to allow users with restricted privileges to install agents on their computers.

Downloading of the installation set begins.

> **Tip**
>
> You can also create an installation set in the Agent Configurations view. To display the Agent Configurations view, in the Settings module, select **Agent** and then **Agent Configurations**. Click the **Create Agent Installer** button for the agent configuration you want to apply to computers. In the displayed dialog box, enter the necessary information, and then click the **OK** button. Downloading of the installation set begins.

Related Topics:

- 15.3.2 Adding agent configurations

- (2) Installing agents on computers

6.3 Searching for devices registered in Active Directory

This approach is one way of searching for devices used in your organization. Using the **Getting Started** wizard, you can search for devices registered in Active Directory.

The **Getting Started** wizard allows you to set the domain information and search schedule for the Active Directory you want to search. When the wizard is complete, the search begins according to the set schedule.

To search for devices registered in Active Directory:

1. In the top of the view, select the **Go** menu, and then **Getting Started Wizard**.
2. In the **What is this Wizard?** view, check the settings for managing devices, and then click the **Next** button.
3. Select **Discover Nodes**, and then click the **Next** button.
4. Select **Discovery from Active Directory**, and then click the **Next** button.
5. Set the domain information of the Active Directory you want to access, and then click the **Next** button.
   To make sure that you can access the set Active Directory, click the **Test** button.
6. Set the search schedule, and then click the **Next** button.
7. Set whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them, and then click the **Next** button.
8. If you want to inform yourself (administrator) of completion of the search by email, specify the notification destination and the mail server information, and then click the **Next** button.
9. In the **Confirm Content and Finish Settings** view, check the settings, and then click the **Complete** button.
10. In the displayed **Discovery Settings Configured** view, click the **Close** button.

The search is performed according to the set search schedule.

To view the search results, in the Settings module, select **Discovery**, **Last Discovery Log**, and then **Active Directory** to display the Active Directory view.

> **Tip**
>
> The settings specified in the wizard are applied to the Active Directory view. To display the Active Directory view, in the Settings module, select **Discovery**, **Configurations**, and then **Active Directory**. You can also start a search by specifying search conditions in this view.

Related Topics:

- 15.2.2 Specifying search conditions (searching Active Directory)
- 15.2.4 Checking the device discovery status

6.4 Searching for devices connected to the network

This approach is one way of searching for devices used in your organization. Using the **Getting Started** wizard, you can search for devices connected to the network.

The **Getting Started** wizard allows you to set the range of IP addresses to be searched and the authentication information to be used during the search. When the wizard is complete, the search begins according to the set schedule.

To search for devices connected to the network:

1. In the top of the view, select the **Go** menu, and then **Getting Started Wizard**.
2. In the **What is this Wizard?** view, check the method used to specify the settings for managing devices, and then click the **Next** button.
3. Select **Discover Nodes**, and then click the **Next** button.
4. Select **Discovery from IP Address Range**, and then click the **Next** button.
5. Set the range of IP addresses to be searched, and then click the **Next** button.
   By default, **Management Server** is set as the IP address range. **Management Server** is a network segment that contains a management server.

   Important note

   If you want to specify a period of time to intensively search, specify settings so that the number of IP addresses that are contained in the IP address range is 50,000 or lower. If the number of IP addresses exceeds 50,000, the network search might stop.
6. Set the authentication information to be used during the search, and then click the **Next** button.
7. Set the authentication information to be used for each IP address range, and then click the **Next** button.

   Important note

   If an IP address range includes devices that are configured to lock the account after a specific number of failed logon attempts, assign specific authentication information for each IP address range. If you select **Any**, all authentication information items are used in an attempt to access devices, which can lead to some users unexpectedly getting locked out of their accounts.

   Important note

   If you select **Any**, each authentication information item is used in an attempt to access devices. The high network access frequency imposes a heavy load on the network. Select this option only after carefully considering the possible network load.
8. Set the search schedule, and then click the **Next** button.

Important note

If you select the **Intensive Discovery** check box, the search is repeated one after another during the specified period of time. During this time, the network is placed under heavy load. Select this option only after carefully considering the possible network load.

9. Set whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them, and then click the **Next** button.
10. If you want to inform yourself (administrator) of completion of the search by email, specify the notification destination and the mail server information, and then click the **Next** button.
11. In the **Confirm Content and Finish Settings** view, check the settings, and then click the **Complete** button.
12. In the displayed **Discovery Settings Configured** view, click the **Close** button.

The search is performed according to the set search schedule.

To view the search results, in the Settings module, select **Discovery**, **Last Discovery Log**, and then **IP Address Range** to display the IP Address Range view.

Tip

The settings specified in the wizard are applied to the IP Address Range view. To display the IP Address Range view, in the Settings module, select **Discovery**, **Configurations**, and then **IP Address Range**. You can also start a search by specifying search conditions in this view.

Related Topics:

- 15.2.1 Specifying search conditions (discovery from IP address)
- 15.2.4 Checking the device discovery status

6.5 Setting a device as a management target

Set a managed device detected in a search or excluded from the management targets, as a management target.

After you set the device as a management target, you can collect the device information and learn its security status.

To specify a device as a management target:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Discovered Nodes**.
3. Select the device you want to manage.
4. Click the **Manage** button.

The selected device is set as a management target.

You can view the collected device information of the management target in the Device module.

Tip

When the network monitor function is installed on a device, the device network connection is controlled at the time it is detected, based on the settings for the network monitor and the network control list. When a device is set as a management target, its network connection is automatically allowed.

Important note

One license is assigned to a device when it is set as a management target. If the number of licenses is insufficient, the devices without a license cannot be set as management targets. If this is the case, you need to purchase additional licenses.

6.6 Excluding a device from the management targets

Exclude a device detected in a search or a managed device that no longer needs to be managed from the management targets.

When a device is excluded from the management targets, it cannot be detected in a device search. Therefore, you can only view the newly detected devices in periodical device searches.

To exclude a device from the management targets:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Discovered Nodes** or **Managed Nodes**.
3. Select the device to be excluded.
4. Click the **Ignore** button.

The selected device is excluded from the management targets.

After you excluded a device from the management targets, the device is no longer displayed in the Device module. The device information associated with the hardware asset information is also removed.

Tip

When the network monitor function is installed on a device, the device network connection is controlled at the time it is detected, based on the settings for the network monitor and the network control list. When a device is excluded from the management targets, its network connection is automatically allowed.

Tip

When you set an exclusion device as a management target, its device information is automatically associated with the hardware asset information if the hardware asset information has the same IP address, host name, serial number, or MAC address exists.

Important note

You cannot exclude a computer for which the site server or network monitor is enabled from the management targets.

6.7 Switching from offline management to online management

To switch a user computer from offline management to online management, you need to change the agent configuration and then set up the user computer. The procedure for switching to online management is described below.

To switch to online management (changing the agent configuration):

1. In the **Agent Basic Settings** view for the agent configuration, select **Connect to the management server**, and then click **OK**.

After you have changed the agent configuration, perform a setup on the user computer.

To switch to online management (setting up on the user computer):

1. Log in to a computer that has the agent installed.
2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Administrator Tool**, and then **Setup**.
3. In the **Setup** dialog box, select **Connect to the management server**, and then click **OK**.
4. In the displayed confirmation dialog box, click **OK**.

The configuration is complete, and the user computer is now switched to online management.

6.8 Switching from online management to offline management

To switch a user computer from online management to offline management, you need to change the agent configuration. The procedure for switching to offline management is described below.

Important note

When switching to offline management, you need to consider the operations for switching back to online management again. When switching a computer that is disconnected from the network from offline management to online management, you also need to change the agent configuration in the **Setup** dialog box on all computers that are switched.

To switch to offline management (changing the agent configuration):

Important note

If the security policy assigned to the target computer has operation log acquisition enabled, change the security policy to disable the operation log acquisition first, and then switch to online management. If you leave the security policy with operation log acquisition enabled, the user computer will keep acquiring operation log files.

1. In the **Agent Basic Settings** view for the agent configuration, clear the **Connect to the management server** check box, and then click **OK**.
2. In the displayed dialog box, click **OK**.

The configuration is complete, and the user computer is now switched to offline management.

6.9 Removing a device

If a device was removed without uninstalling the agent or communication with the management server was disabled when uninstalling the agent, the device information might be left in the management server. In such a case, you need to remove the unnecessary device to obtain the correct information about the device status.

To remove a device:

1. Display the Settings module.
2. In the menu area, select **Discovery**, **Discovered Nodes**, and **Managed Nodes** or **Ignored Nodes**.
3. Select the device you want to remove.
4. From **Action**, select **Remove**.

The selected device is removed. When a device is removed, the device information is also removed from the database.

You can rediscover a removed device by performing a search. A rediscovered device is handled as a new device, and the previous device settings are not inherited.

> **Important note**
>
> You cannot remove a computer whose network monitor is enabled.

6.10 Editing device information

You need various device information to manage the devices. However, depending on the device environment, you might sometimes be unable to collect device information. For a device whose information cannot be collected, you can manually edit the device information. You can edit not only the uncollected information, but also the information that has already been collected.

For example, when the OS information is not collected or the OS information of an unsupported OS is collected from another computer, the device is handled as an unknown device, instead of being registered in the OS group. As a result, the group configuration differs from the actual computer group. In such a case, you can manually edit the OS information to ensure that the computer is correctly managed.

To edit device information:

1. Display the Device module.
2. In the menu area, select a group from **Device Inventory**.
3. In the information area, select the device whose information you want to edit.
   You can select multiple devices.
4. Select **Edit Device Details** from **Action**.
5. In the displayed dialog box, edit the device information.
6. Click **OK**.

The device information is updated.

Important note

The collected information has a higher priority than the device information that has been manually edited. Therefore, if information is collected after being manually edited, the information is updated with the collected information. However, as the only exemption, the **device type** information that was manually edited takes precedence over the collected information.

Important note

When you change the **host name** in the device information, the **device name** in the hardware asset information is not automatically changed, even if the device information and hardware asset information are associated with each other. If you change the **host name** in the device information, and if the **device name** in the hardware asset information is the same as the **host name** in the device information, manually change the **device name** in the hardware asset information.

6.11 Acquiring the latest device information

You can acquire the latest device information any time from a computer that has the online management agent installed.

When you are collecting user information entered by the user, when the device information is acquired, the **End User Form** view appears on the user's computer if the following condition is met: During agent setup, in **Agent Basic Settings**, you specified display of the End User Form view.

To acquire the latest device information:

1. Display the Device module.
2. In the menu area, select a group from **Device Inventory**.
3. In the information area, select the device you want to use to acquire the information.
   You can select multiple devices.
4. From **Action**, select **Update Device Details**.
5. If you want to simultaneously turn on the device that has the agent installed when the information is acquired, select **Start the selected computer if it is not running**.
6. Click **OK**.

The latest device information is obtained. The user information that was last entered is obtained.

When **Start the selected computer if it is not running** is selected, the device is automatically turned on before the device information is acquired, if the power has been turned off. After the device information is obtained, the device is automatically turned off. However, if the device has already been turned on when the information is acquired, the power is not turned off.

Important note

The Wake on LAN function can only turn on the computers in the same network segment as the management server.

In the following cases, the device might be automatically turned off after the device information is obtained:

- When the user manually turned on the computer right before the power is automatically turned on
- When it cannot be correctly determined whether the power on the computer is on or off due to the network status

Related Topics:

- 15.6.6 Setting AMT credentials

6.12 Creating the information collection tool

Use the information collection tool to collect the device information of an offline-managed computer.

To create the information collection tool:

1. Display the Device module.
2. In the menu area, select a device from **Device Inventory**.
3. From **Action**, select **Create the Information Collection Tool**.
   The dialog for downloading the information collection tool is displayed. The displayed file name is ITDMOffline.zip by default.

Starts to download the information collection tool.

Extract the information collection tool to the location where the tool is saved, and then store the tool on an external storage device. When you collect device information by using a logon script, save the information to a shared server that is connected with the offline-managed computer.

Related Topics:

- 6.13 Notification of the device information collected by using the information collection tool

6.13 Notification of the device information collected by using the information collection tool

The device information of an offline-managed computer collected by using the information collection tool is notified to the management server from an online-managed computer. By notifying the device information, the device information of the offline-managed computer is updated to the latest.

To notify the device information, the online-managed computer must be logged on by a user who has full control permissions over the folder that stores the information collected by using the information collection tool. Because the management server must be connected when notifying the device information, the device information cannot be notified from an offline computer.

Important note

When out-of-date device information is notified, the current device information registered with JP1/IT Desktop Management is overwritten with the out-of-date device information. In this case, you need to collect the latest device information from the applicable computer and then notify the latest information again.

Important note

If you have set acquisition of device revision history, notify the device information in the order that the device information was changed. If you do not notify the device information in this order, the date and time of revision history cannot be correctly obtained.

To notify the device information collected by using the information collection tool:

If you used the logon script when collecting the device information, step 1 can be omitted.

1. Connect the external storage media that stores the device information collected by using the information collection tool to an online-managed computer.

2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Administrator Tool**, and then **Send Inventory**.

   When the information notification that uses an external storage media is password-protected, a window for entering the password appears. Enter the password that was specified in **Settings for Sending Information Using External Storage Media** during agent setup. If the agent is newly created, the notification is not password-protected by default.

3. In the **Specify storage location** dialog box, specify the folder that stores the device information to be notified. Specify the path of the folder with a character string of no more than 133 characters that contains \Data and excludes the ASCII control characters.

4. Click **OK**.

   Notification of the device information starts. A dialog box indicating the progress appears until the notification is complete.

A dialog showing the notification results appears, and the notification of the device information is complete.

If a computer failed to notify the device information, recollect the device information based on the information provided in the failure notification list (result_failed.txt), and then send the notification again. For details, see 18.4 Actions to be taken when notification of device information that was collected with the Information Collection Tool fails.

To view the computers that have successfully notified the device information, check the success notification list (result_success.txt). The success notification list is generated when a computer successfully notified the device information. The host names of the computers that have successfully notified the device information are output to the success notification list.

Generation location

The Data folder specified in the **Specify storage location** dialog box

Output format

YYYY/*MM*/*DD hh*:*mm*:*ss host-name*#

YYYY: year; MM: month; DD: day; hh: hour; mm: minute; ss: second

Output example

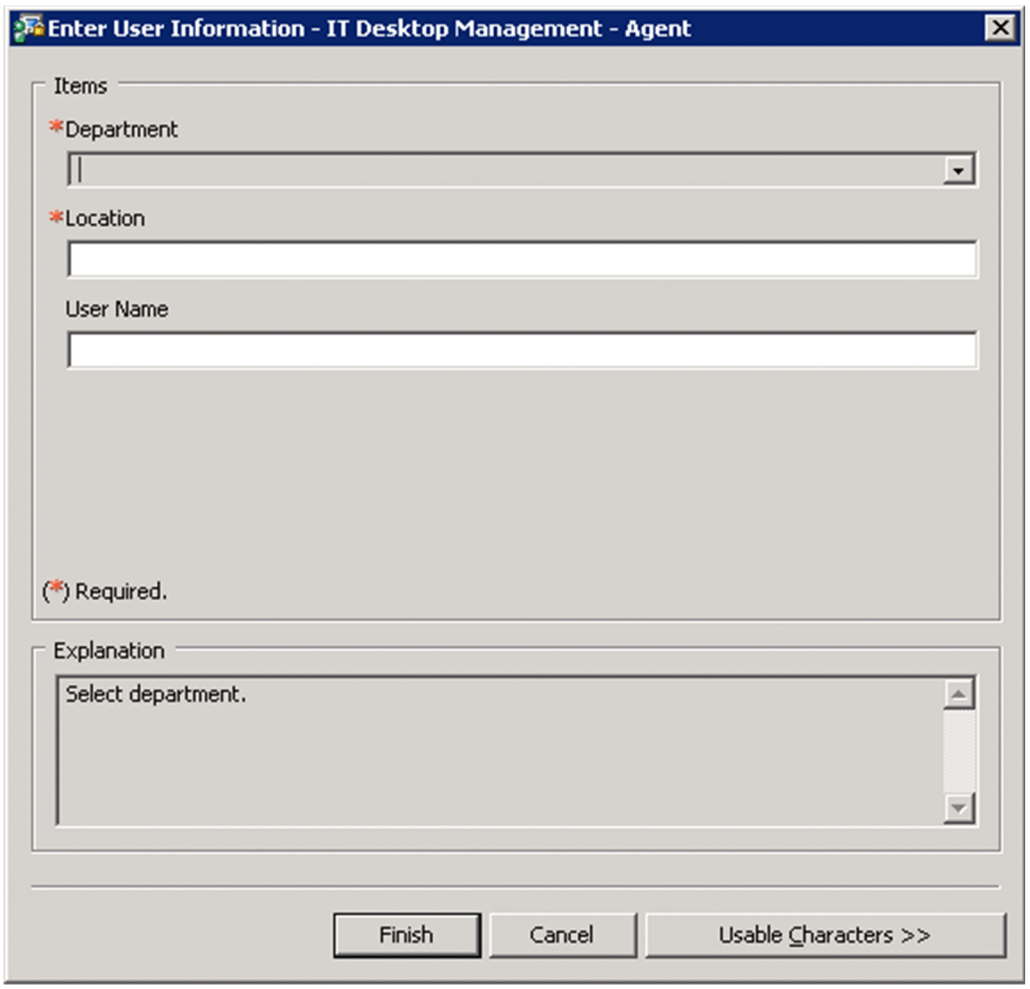
```
2012/10/11 14:15:16 Host1
2012/10/11 14:15:18 Host2
2012/10/11 14:15:19 Host3
```

Related Topics:

- 6.12 Creating the information collection tool

6.14 Obtaining user information

You can display the **End User Form** view on a user computer and obtain the information entered by the user. The management workload can be reduced by periodically requesting users to enter user information. An example of the **End User Form** window is shown below.



Note that to display the **End User Form** view, the agent must be installed on the user computer. Whether the End User Form view is displayed depends on the settings of **Agent Basic Settings** for agent setup.

The procedure for displaying the **End User Form** view at any time and the procedure for displaying the view from a specified time onwards are described below.

To obtain user information (at any time):

1. Display the Settings module.
2. In the menu area, select **Asset Management** and then **Asset Field Definitions**.
3. In **End User**, specify the **input method** for the user information you want to obtain.
   Note that you can specify **End User** in **Common Fields (Assets and Device Inventory)** and in **Common Fields (Hardware Assets)** only.

After the user enters the user information in the **End User Form** view and clicks **OK**, the user information is acquired.

To obtain user information (by specifying a date and time):

1. Display the Settings module.
2. In the menu area, select **Asset Management** and then **Asset Field Definitions**.
3. In the information area, in **Start Date for Entry of User Information**, click **Edit**.
4. In **Timing for starting user entry**, select **Specified (a specified date and time for starting entry, in the local time of the user computers)**, and then specify the start date and time for data entry.
5. Click **OK**.
6. In **End User**, specify **Data source** for the user information you want to obtain.
   Note that you can specify **End User** in **Common Fields (Assets and Device Inventory)** and in **Common Fields (Hardware Assets)** only.
   You can edit the start date and time for data entry by clicking the **Edit Entry Start Date** button in the dialog box used for setting the data source, and then using the dialog box that appears.

After the user enters the user information in the **End User Form** view and clicks **OK**, the user information is acquired.

Related Topics:

- 15.5.1 Adding asset management items

6.15 Setting the display interval for the End User Form view in the Device module

You can set the interval at which the **End User Form** view appears on online-managed computers. The management workload can be reduced by periodically requiring users to enter user information.

For example, if the department information is not frequently updated after being entered by a user, the information displayed in the operation window might not match the actual situation after the user is transferred within the organization. Therefore, you need to set an appropriate schedule that matches the environment.

To set the interval at which user information appears:

1. Display the Device module.
2. In the menu area, select a group from **Device Information**.
3. From **Action**, select **Enable End User Form (Frequent Pop-up)**.
4. In the dialog box that appears, specify the display interval, and then click **OK**.

The interval at which the **End User Form** view appears is set.

When the interval at which the **End User Form** view appears is set, a green check mark appears in the item in the operation menu. When you select the item again, the setting is cleared.

Related Topics:

- 6.14 Obtaining user information

6.16 Setting the information acquired from Active Directory as an additional management item

You can obtain the detailed device information that is managed in Active Directory as an additional management item by specifying **Active Directory** as the data source of the additional management item. Also, set the management item for the Active Directory from which information is obtained.

To set the information obtained from Active Directory as an additional item:

1. Display the Settings module.
2. Select **Asset Management** and then **Asset Field Definitions**.
3. Create an item for obtaining the information from the Active Directory, or edit an existing item.
   To create a new item, click the **Add Fields** button. To edit an existing item, select the item and then click the **Edit** button.
4. In the displayed dialog box, specify **Data Source** for **Active Directory**.
5. Specify the Active Directory management item from which information is obtained.

The information managed in Active Directory can now be obtained as an additional management item of each device.

6.17 Exporting device information

Select **Device Information** in the Device module, then you can export (in a batch) the information displayed in the information area of the **Device Information** view into a CSV file.

To export the specific device information only, use the filter to limit the information.

For example, if you only want to export the device information whose **device type** is PC, filter out and display the device information whose **device type** has been specified as **PC**.

To export device information:

1. Display the Device module.
2. Select a group from **Device Information**.
3. In the information area, display the device whose information you want to export.
4. From **Action**, select **Export Device List** or **Export Device Details**.
5. In the **Export Item Selection** dialog box, select the items you want to export, and then click **OK**.
   To specify the character code for the exported CSV file, select a character code in **Encoding**. The default character code is UTF-8.
6. In the displayed window, click the **Save** button.

The CSV file is saved with the specified name in the location where the file is downloaded.

> **Tip**
>
> In the **Export Device Details** view, you can also export the information displayed on the tab at the bottom of the window. To create a list of the main information only, use **Export Device List**. To create a detailed information list, use **Export Device Details**.

6.18 Exporting software inventory

Select **Software Inventory** in the Device module, then you can export (in a batch) the software inventory displayed in the information area of the **Software Inventory** view into a CSV file.

To export a specific software inventory only, use the filter to limit the information.

For example, if you only want to export a software inventory that has been specified as mandatory information, filter out and display the software inventorys whose **Mandatory Software** has been specified as **Mandatory**.

To export device information:

1. Display the Device module.
2. Select **Software Inventory** and then **Software List**.
3. In the information area, display the software whose inventory information you want to export.
4. From **Action**, select **Export Software List**.
5. In the **Export Item Selection** dialog box, select the items you want to export, and then click **OK**.
   To specify the character code for the exported CSV file, select a character code in **Encoding**. The default character code is UTF-8.
6. In the displayed window, click the **Save** button.

The CSV file is saved with the specified name in the location where the file is downloaded.

6.19 Removing software inventory

Select **Software Inventory** in the Device module, then you can remove the software inventory displayed in the Software Inventory view.

We recommend that you remove software inventorys whose used license count is 0 and that do not need to be managed.

To remove software inventory:

1. Display the **Software Inventory** view from the Device module.
2. In the information area, select the software inventory that you want to remove.
3. From **Action**, select **Remove Software Inventory**.
4. In the **Remove Software Inventory** dialog box, check whether the software inventory can be removed.
   If the software inventory can be removed, select **Continue Operation**.
5. Click **OK**.

The software inventory is removed.

If the removed software inventory was collected from a managed computer, the software inventory is displayed again.

Note that the settings for the unauthorized software, the mandatory software due to security policies, and managed software inventory are not affected by the removal of the software inventory. The installed software inventory of each device is not affected either.

6.20 Setting unauthorized software

You can set the software you checked in the software inventory list as unauthorized software.

You can know the installation status and control the use of software by registering the software that is no longer needed or that has security problems to security policies as unauthorized software.

To set unauthorized software:

1. Display the Device module.
2. In the menu area, select **Software Inventory** and then **Software List**.
3. In the information area, click the **Add as Unauthorized Software** button for the software that you want to register as unauthorized software.
4. In the displayed dialog box, specify the unauthorized software by selecting the security policy to which you want the software to be registered.
5. Click **OK**.

The selected software is registered to the security policy as unauthorized software.

In the information area, the unauthorized software you registered can be identified with a mark displayed in the **Unauthorized Software** field. You can also view the registration details in **Security Details** on the **Software Inventory** tab.

To change the information registered for the unauthorized software, edit the security policy.

Related Topics:

- 1.7.1 Setting a security policy

6.21 Uninstalling software from the computers

If the software that is not necessary for the business operation or prohibited from being used has been installed on the computers in your organization, you can uninstall the software from these computers.

Note that you can uninstall software only from the computers managed online.

To uninstall the software from the computers:

1. Display the Device module.
2. In the menu area, select **Software Inventory** and then **Software List**.
3. In the information area, select the software that you want to uninstall from the computers, and then display the **Installed Computers** tab.
4. In the tab, select the computer from which you want to uninstall the software, and then click the **Uninstall** button.
   You can select more than one computer in the tab to perform the uninstallation procedure in a batch.
5. In the displayed dialog box, create an uninstallation task, and then click the **OK** button.

The software is uninstalled according to the schedule specified in the uninstallation task. You can view the execution status of the task in the **Task List** view of the Distribution module.

Tip

You can also create and execute an uninstallation task from the Distribution module.

Tip

When you specify unauthorized software in a security policy, you can also set automatic enforcement to the security policy in such a way as to automatically uninstall any unauthorized software when it is detected.

Related Topics:

- 1.7.1 Setting a security policy

6.22 Sending a notification to a user

If you have a message to inform the computer users of, you can create a notification and send it to individual users.

Note that you can send notifications to online-managed computers only.

To send a notification to a user:

1. Display the Device module.
2. From **Device Information** in the menu area, select the group that contains the computer to which you want to send the notification.
3. In the information area, select the computer to which you want to send the notification, and then select **Send User Notification** from **Action**.

   You can also select multiple computers to send the same notification to more than one user simultaneously.
4. In the displayed dialog box, specify the notification to be sent, and then click **OK**.

   If you select **Start the selected computer if it is not running**, the notification can also be sent to the computers that are not running.

   If you select **Add Notes**, the notification history and reasons for sending the notifications can be recorded. The information entered here will be added to the **Notes** tab.

The notification is sent to the computer user.

6.23 Controlling the computer power

You can turn on or off the power of a computer, or restart a computer.

Note that to control the computer power, the target computer must satisfy certain conditions.

To control the computer power:

1. Display the Device module.
2. From **Device information** in the menu area, select the group that contains the computer whose power you want to control.
3. In the information area, select the computer whose power you want to control, and then select **Power ON**, **Power OFF**, or **Reboot** from **Action**.
   You can select multiple computers to simultaneously control the power of the selected computers.
4. In the displayed dialog box, select **Continue Operation**, and then click **OK**.

The power of the computer is turned on or off, or the computer restarts.

In the **Power Status** field, you can check the computer power status.

6.24 Obtaining smart device information

You can obtain the latest smart device information from the linked MDM system at any desired time.

To obtain smart device information:

1. Display the Settings module.
2. In the menu area, select **General** and then **MDM Linkage Settings**.
3. From **MDM Linkage Settings** in the information area, select the settings for the MDM system that manages the smart device from which you want to obtain information.
4. From **Action**, select **Collect Device Info. From MDM System**.
5. In the displayed dialog box, click **OK**.

The list is updated, and the smart information is obtained.

If you want to know the acquisition status of device information, select **Refresh List to Latest Info** from **Action**. The list in **MDM Linkage Settings** is updated with the most recent information, so that you can view the acquisition status.

Tip

If you have set the MDM linkage to periodically obtain smart device information, the device information of the managed smart devices is automatically updated according to the schedule.

Tip

The device information that JP1/IT Desktop Management obtains is the information that the MDM system obtained from smart devices. Therefore, the latest smart device information might differ from the device information managed by JP1/IT Desktop Management.

6.25 Locking a smart device

If a smart device is lost, the administrator can lock the smart device to prevent it from being used by the person who finds it.

To lock a smart device:

1. Display the Device module.
2. From **Device Information** in the menu area, select the group that contains the smart device to be locked.
3. In the information area, select the smart device to be locked, and then select **Lock Smart Device** from **Action**.
   You can also select multiple smart devices to simultaneously lock more than one device.
4. In the displayed dialog box, click **OK**.

The selected smart device is locked.

Important note

If no passcode is specified for the smart device, the smart device can still be used even after it is locked. If you do not want the smart device to be used, be sure to specify a passcode for it.

Tip

A smart device is locked by the MDM system according to a request issued by JP1/IT Desktop Management. Therefore, locking of the smart device is complete at the time the MDM system receives the execution request from JP1/IT Desktop Management.

6.26 Resetting a smart device passcode

If the user forgets the passcode of a smart device, the administrator can reset the smart device passcode, so that the user can respecify the passcode.

Only one smart device passcode can be reset at a time. If you need to reset more than one smart device passcode, reset them one by one.

To reset a smart device passcode:

1. Display the Device module.
2. From **Device Information** in the menu area, select the group that contains the smart device for which you want to reset the passcode.
3. In the information area, select the smart device for which you want to reset the passcode, and then select **Reset Smart Device Passcode** from **Action**.
4. In the displayed dialog box, select **Continue Operation**.

   If you select **Add Notes**, the reset history and reasons for resetting the smart device passcode can be recorded. The information entered here will be added to the **Notes** tab.
5. Click **OK**.

The passcode for the selected smart device is reset.

Instruct the user to respecify the passcode after the smart device passcode is reset.

> **Tip**
>
> A smart device passcode is reset by the MDM system according to a request issued by JP1/IT Desktop Management. Therefore, the reset of the smart device passcode is complete at the time the MDM system receives the execution request from JP1/IT Desktop Management.

6.27 Resetting a smart device

You can reset a smart device to its factory settings.

You can only reset one smart device at a time. If you need to reset more than one smart device, reset them one by one.

To reset a smart device:

1. Display the Device module.
2. From **Device Information** in the menu area, select the group that contains the smart device you want to reset.
3. In the information area, select the smart device you want to reset, and then select **Initialize Smart Device** from **Action**.
4. In the displayed dialog box, select **Continue Operation**.
   If you select **Add Notes**, the reset history and reasons for resetting the smart device can be recorded. The information entered here will be added to the **Notes** tab.
5. Click **OK**.

The selected smart device is reset.

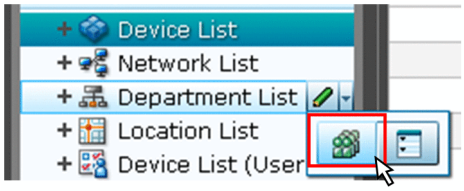
> **Tip**
>
> A smart device is reset by the MDM system according to a request issued by JP1/IT Desktop Management. Therefore, the reset of the smart device is complete at the time the MDM system receives the execution request from JP1/IT Desktop Management.

6.28 Adding the definition for a department or location

If the departments or locations to manage increase, you can add a definition for a new department or location. After the definition is added, the new department or location is displayed in the menu area of the Assets module and the Device module.

To add the definition for a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



> **Tip**
>
> Alternatively, you can perform the following: In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the window that appears, click either **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

3. In the displayed dialog box, click the **Edit** button in **Type**.
4. In the displayed dialog box, add the department or location.
5. Click **OK**.
6. Click **OK**.

The the definition for the department or location is added, and the added group is displayed in the menu area of the Assets module and Device module.

Related Topics:

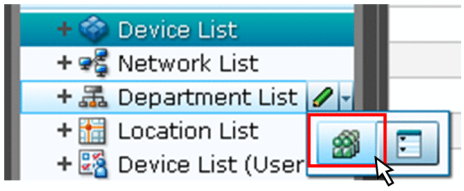
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location

6.29 Editing the definition for a department or location

If the organizational structure of the departments you are managing or the name of a location was changed, you can edit the definition for the department or location. After the definition is edited, the edited department or location is displayed in the menu area of the Assets module and the Device module.

To edit the definition of a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



> **Tip**
>
> Alternatively, you can perform the following: In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the window that appears, either click **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

3. In the displayed dialog box, click the **Edit** button in **Type**.
4. In the displayed dialog box, edit the name of the department or location, or hierarchical structure.
5. Click **OK**.
6. Click **OK**.

The definition for the department or location is edited, and the edited group is displayed in the menu area of the Assets module and Device module.

The user information (actual status) of each device is unchanged even if you changed a definition. Therefore, the definition that is different from the actual status is added to the menu area of the Assets module and Device module. To ensure the actual status is consistent with the definition, update the user information according to the definition after you edited the definition for a department or location. After you update the user information, delete only the hierarchies that exist in the old organizational system, so that the menu area display is consistent with the definition. For details about how to delete only the hierarchies that were used in the old system, see 6.31 Removing only hierarchies that were used in the old organizational system.

> **Tip**
>
> After you change the department definition, the department information displayed in the following views in the Assets module also changes: **Software License List** in **Software Licenses**, **Software License Status List** in **Software License Status**, and **Contract List** in **Contracts**.

Related Topics:

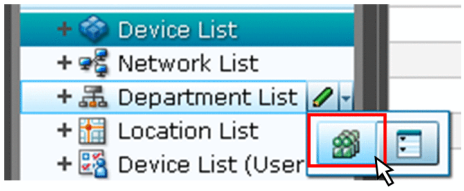
- 6.28 Adding the definition for a department or location

6.30 Removing the definition for a department or location

If you no longer manage a department or location, you can remove the definition for the department or location. After the definition is removed, the removed department or location no longer appears in the menu area of the Assets module and the Device module.

To remove the definition for a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



3. In the displayed dialog, click the **Edit** button in **Type**.
4. In the display the window, remove the definition for the department or location.
5. Click **OK**.
6. Click **OK**.

The definition for the department or location is removed.

The user information (actual status) of each device is unchanged even if you remove a definition. Therefore, the removed hierarchy is still displayed in the menu area of the Assets module and the Device module. To ensure the actual status is consistent with the definition, update the user information according to the definition after you edited the definition for a department or location. After you update the user information, delete only the hierarchies that exist in the old organizational system, so that the menu area display is consistent with the definition. For details about how to delete only the hierarchies that were used in the old system, see 6.31 Removing only hierarchies that were used in the old organizational system.

Tip

After you delete the department definition, in the following views of the Assets module, Unknown appears for the department:

- The **Software License List** view in **Software Licenses**
- The **Software License Status List** view in **Software License Status**
- The **Contract List** view in **Contracts**

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location

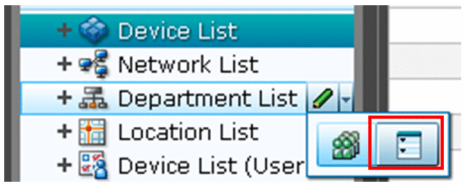
6.31 Removing only hierarchies that were used in the old organizational system

Even if you remove the hierarchies (definitions) for the departments or locations in the Settings module in association with an organizational change, the removed hierarchies will still appear in the menu area of the Assets or Device module. To ensure that the display in the menu area is consistent with the definitions, you need to remove only the hierarchies that were used in the old organizational system. You can do so in the dialog box that you display from the menu area of the Assets module, the Device module, or the Security module.

The example below explains how to remove such hierarchies from the Assets module.

To remove only hierarchies that were used in the old organizational system:

1. Display the Assets module.
2. In the menu area, select **Hardware Asset**, select **Department List** or **Location List**, and then click the icon that appears.



3. In the dialog box that appears, select the hierarchies that you want to remove.
4. Click the **Remove** button.
5. In the dialog box that appears, click **OK**.
6. Click the **Close** button.

Only the hierarchies that were used in the old organizational system are removed, and the display of the menu area in the Assets module or the Device module is now consistent with the definitions.

6.32 Changing the name of a department or location

If the organizational structure of the departments you are managing or the name of a location was changed, you can change the name of the department or location.

To change the names of a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then move the cursor over the group for which you want to change the name.
3. Click  that is displayed to the right of the item.
4. In the displayed menu, click  .
5. In the displayed text area, enter the name of the department or location.

The name of the department or location is changed. The group name in the device user information is also changed to the new name.

> **Tip**
>
> You can also right-click the department or location in the menu area, and then change the name from the displayed menu.

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location
- 6.33 Deleting a department or location

6.33 Deleting a department or location

You can remove an unnecessary department or location.

To remove a department or location:

1. Display the Assets module.
2. In the menu area, select **Hardware Assets** and then **Department List** or **Location List**, move the cursor over the group that you want to remove.
3. Click  displayed on the right side of the item.
4. In the displayed menu, click  .
5. In the displayed dialog box, click **OK**.

The group that contains the department or location is removed. The department or location is also removed from the device user information.

> **Tip**
>
> You can also right-click the department or location in the menu area, and then remove it from the displayed menu.

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location
- 6.32 Changing the name of a department or location

7

Remotely Controlling Devices

This chapter describes how to remotely control devices in your organization.

7.1 Installing the controller

The controller is not installed when you install JP1/IT Desktop Management. Install the controller by downloading it from the operation window.

Note that you need administrator permissions to install the controller.

To install the controller:

1. Display the Device module.
2. Select a computer from the device list, and then click the **Remote Control** button.
3. In the displayed dialog box, click the **Go** button.

The controller is installed on the computer displayed in the operation window.

The dialog box for starting remote control is displayed. Start remote control by following the dialog box.

Important note

If you are using Firefox as your web browser, the controller cannot be automatically installed. In step 3, click the **Save** button to save the controller, and then manually install the controller.

Important note

Pay attention to the following issues when installing the controller:

- When you install the controller, the driver signing options in Windows temporarily turns to a warning. In Windows Server 2003 and Windows XP, the driver signing options might not return to the original settings when the installation is complete. If this happens, manually reset the driver signing option.
- To upgrade the version of the OS, uninstall the controller first, and then upgrade the OS. For details about how to uninstall the controller, see 7.2 Uninstalling a controller.
- Do not install the controller to Windows XP Mode in Windows 7.

Tip

The remote control agent is automatically installed if you install the agent on a user computer.

Related Topics:

- 7.3 Changing the controller environment settings
- 7.4 Setting up an operational environment for the remote control agent

7.2 Uninstalling a controller

Uninstall the controllers from the computers that you no longer need to perform remote control with.

To uninstall a controller:

1. In Windows control panel, start **Programs and Features**.
2. Select JP1/IT Desktop Management - RC Manager, and then click the **Uninstall** button.
3. In the displayed dialog box, click the **Yes** button.

The controller is uninstalled.

Tip

The remote control agent is automatically uninstalled when the agent is uninstalled.

7.3 Changing the controller environment settings

To remotely control a computer, you can change the operation environment, such as the connection method, connection mode, and method for forwarding data received from the computer.

Change the environment settings in the **Options** dialog box. You can set up the items listed in the following table:

Tab	Item
Connection tab	• Port number • Whether power control is enabled • Settings for retrying a connection when the connection fails • Whether automatic disconnection is enabled • Connection mode
Session tab	• Items related to data transfers (whether data compression and encryption is enabled) • Items related to the Desktop (wallpaper, animation control) • Items related to drawing (tone reduction, bitmap cache) • Items related to the clipboard
Key Input tab	Special key registration and settings for data transfers
Logging tab	• Whether log output is enabled • Environment settings for log output • Settings for remote control recording
Advanced tab	• Saving and loading the settings • AMT settings (user ID and password) • Keyboard and mouse settings (mouse button settings) • Scroll (whether auto-scrolling is enabled)

To change the controller environment settings:

1. On the toolbar of the **Remote Control** window, click the **Options** button.
2. In the displayed dialog box, perform settings on each tab, and then click **OK**.

The specified values are saved, and the environment settings for the controller are changed.

Tip

The controller environment settings are applied to the controllers installed on individual computers. The controller environment settings do not have an effect on other computers.

7.4 Setting up an operational environment for the remote control agent

Set up an operational environment for the remote control agent in the **Remote Control Settings** view and the **Remote Control Security Settings** view that are used for agent setup.

For details about how to set up the agent, see 15.3.1 Managing agent configurations.

7.5 Performing remote control

7.5.1 Directly starting the controller

You can directly start the controller and connect it to a remote computer without logging in to JP1/IT Desktop Management. Because there is no need to log in to the operation window, you can start the operation immediately if you need to perform remote control only.

To directly start the controller:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Manager**, and then **Remote Controller**.

The controller starts.

At this moment, no computer is connected to. To start remote control, you must specify the connection destination. For how to specify a connection destination for the controller, see 7.5.2 Starting remote control by selecting a computer.

Tip

You can also directly start the controller by executing the following command:

```
jdngrcctr.exe /agent IP-address
```

Specify the host name and IP address of the connection destination. The controller starts, and the specified computer is connected to. If you do not specify this information, the computer is not connected to.

7.5.2 Starting remote control by selecting a computer

You can start remote control by selecting the computer to connect to from the controller.

To select and connect to a computer:

1. Start the controller.
2. On the toolbar of the **Remote Controller** window, click the **Connect** button.
3. Select the computer from the displayed menu.

Tip

If you click the **Connect** button, the computers registered in the connection list are shown in the displayed menu.

The selected computer is connected, and the view of the computer is displayed.

If authentication information is set on the computer, a dialog box for entering the authentication information is displayed when connecting the computer. In this case, enter the authentication information that was set by selecting **Remote Control Security Settings** and then **User Authentication** during agent configuration, or the authentication information

that was set on the VNC server to be connected to. The default agent configuration for authentication information is set as follows: user ID=system; password=manager.

In addition, when the settings on the computer are set to display connection requests, if the request is rejected, a message indicating that the connection has been rejected will be displayed on the controller.

Tip

If the request to connect to the computer is rejected or a timeout occurs, try to reconnect to the computer by using RFB. Also, when the computer being connected to has been set to turn on when connecting, if the RFB reconnection fails (times out) because the computer is turned off, restart the computer by using Wake on LAN or AMT, and try to connect to the computer again.

Related Topics:

- 7.5.1 Directly starting the controller

7.5.3 Starting remote control by directly specifying the host name or IP address

You can start remote control by directly specifying the IP address or host name of the computer to connect to from the controller.

To connect to a computer by directly specifying the host name or IP address:

1. Start the controller.
2. On the toolbar of the **Remote Controller** window, enter the host name or IP address of the computer you want to connect to for **Agent Specification**.

   Alternatively, you can also click the **Connect** button () and then **Connection**, and then directly specify the host name or IP address in the displayed dialog box.
3. Click the **Enter** button.

The computer with the specified host name or IP address is connected to, and the view of the computer is displayed.

If authentication information is set on the computer, a dialog box for entering the authentication information is displayed when connecting the computer. In this case, enter the authentication information that was set by selecting **Remote Control Security Settings** and then **User Authentication** during agent configuration, or the authentication information that was set on the VNC server to be connected to. The default agent configuration for authentication information is set as follows: user ID=system; password=manager.

In addition, when the settings on the computer are set to display connection requests, if the request is rejected, a message indicating that the connection has been rejected is displayed on the controller.

Tip

If the request to connect to the computer is rejected or a timeout occurs, try to reconnect to the computer by using RFB. Also, if the computer being connected to has been set to turn on when connected to, if the RFB

reconnection fails (times out) because the computer is turned off, restart the computer by using Wake on LAN or AMT, and try to connect to the computer again.

Related Topics:

- 7.5.1 Directly starting the controller

7.5.4 Starting remote control by using the connection history

For a computer that was previously connected, you can start remote control by using the connection history.

To connect to a computer by using the connection history:

1. Start the controller.
2. On the toolbar of the **Remote Controller** window, right-click **Agent Specification**.
3. From the pull-down menu, select the computer that you want to connect.

The selected computer is connected, and the view of the computer is displayed.

If authentication information is set on the computer, a dialog box for entering the authentication information is displayed when connecting the computer. In this case, enter the authentication information that was set by selecting **Remote Control Security Settings** and then **User Authentication** during agent configuration, or the authentication information that was set on the VNC server to be connected to. The default agent configuration for authentication information is set as follows: user ID=system; password=manager.

In addition, when the settings on the computer are set to display connection requests, if the request is rejected, a message indicating that the connection has been rejected will be displayed on the controller.

Tip

If the request to connect to the computer is rejected or a timeout occurs, try to reconnect the computer by using RFB. Also, when the computer being connected to has been set to turn on when connected to, if the RFB reconnection fails (times out) because the computer is turned off, restart the computer by using Wake on LAN or AMT, and try to connect to the computer again.

Related Topics:

- 7.5.1 Directly starting the controller

7.5.5 Starting remote control by searching for a computer

If you do not know which computers can be remotely controlled, you can find the computers that can be connected to within the network by performing a search. Then, you can connect to a computer found in the search and start remote control.

To connect to a computer by performing a search:

1. Start the controller.

2. Search for computers.

3. Connect to a computer displayed in the search results.

   If you used the connection list to search for computers, select a detected computer, and then click  .

   If you used the **Remote Controller** window to search for computers, select a detected computer that is waiting to be connected to, and then click the **Connect** button.

The selected computer is connected, and the view of the computer is displayed.

If authentication information is set on the computer, a dialog box for entering the authentication information is displayed when connecting to the computer. In this case, enter the authentication information that was set by selecting **Remote Control Security Settings** and then **User Authentication** during agent configuration, or the authentication information that was set on the VNC server to be connected to. The default agent configuration for authentication information is set as follows: user ID=system; password=manager.

In addition, when the settings on the computer are set to display connection requests, if the request is rejected, a message indicating that the connection has been rejected will be displayed on the controller.

Tip

If the request to connect to the computer is rejected or a timeout occurs, try to reconnect the computer by using RFB. Also, when the computer being connected to has been set to turn on when connected to, if the RFB reconnection fails (times out) because the computer is turned off, restart the computer by using Wake on LAN or AMT, and try to connect to the computer again.

Related Topics:

- 7.5.1 Directly starting the controller
- 7.5.26 Searching for connectable computers by using the **Remote Controller** window
- 7.5.27 Searching for connectable computers by using the connection list

7.5.6 Starting remote control from the operation window

You can start remote control by connecting to a computer selected in the operation window of JP1/IT Desktop Management.

To connect to a computer:

1. Display the Device module.

2. In the **Device Information** view, select the computer you want to connect to.
   You can select multiple computers.

   Tip

   You can use a filter to efficiently detect a target computer.

3. Click the **Remote Control** button.

The controller (the **Remote Controller** window) starts, and the screen of the computer being connected to is displayed. When more than one computer is connected to, the number of computers being connected to is the same as the number of views open.

If authentication information is set on the computer, a dialog box for entering the authentication information is displayed when connecting the computer. In this case, enter the authentication information that was set by selecting **Remote Control Security Settings** and then **User Authentication** during agent configuration, or the authentication information that was set on the VNC server to be connected to. In the default agent configuration, authentication information is set as follows: user ID=system; password=manager.

In addition, when the setting on the computer end is set to display connection requests, if the request is rejected, a message indicating that the connection has been rejected will be displayed on the controller.

Tip

If the controller is not installed on the computer that you are operating, the controller is automatically installed when remote control starts.

Tip

One computer can simultaneously connect to up to 255 controllers.

Tip

If the request to connect to the computer is rejected or a timeout occurs, try to reconnect to the computer by using RFB. Also, when the computer being connected to has been set to turn on when connected to, if the RFB reconnection fails (times out) because the computer is turned off, restart the computer by using Wake on LAN or AMT, and try to connect to the computer again.

7.5.7 Disconnecting a remotely controlled computer

You can disconnect a remotely controlled computer at any time.

To disconnect a computer:

1. On the toolbar of the **Remote Controller** window, click the **Disconnected** button.

The computer is disconnected from.

If multiple computers are connected to and multiple **Remote Controller** windows are open, only the computer that corresponds to the Remote Controller window on which you performed the disconnection operation is disconnected.

Tip

After the disconnection, if you select **File** and then **Reconnect** from the menu of a **Remote Controller** window, the computer that was disconnected from by using the Remote Controller window is reconnected.

However, depending on the settings on the computer, the remote control agent might automatically stop at the time of disconnection. In this case, restart the remote control agent, and then reconnect to the computer.

7.5.8 Setting automatic disconnection for a remotely controlled computer

You can monitor computers that are not being operated on or whose **Remote Controller** window is inactive, and automatically disconnect such a computer after the status continues for a set amount of time.

To set automatic disconnections for a computer:

1. On the toolbar of the **Remote Controller** window, click the **Options** button.
2. On the **Connection** tab of the displayed dialog box, select **Auto Disconnect when idle**, and then specify the wait time from the operating stops until the computer is disconnected.

Based on the above settings, the computer is automatically disconnected from when the specified time elapses since an operation was last performed on the computer (no data is transferred).

Tip

After the disconnection, if you select **File** and then **Reconnect** from the menu of a **Remote Controller** window, the computer that was disconnected from by using the Remote Controller window is reconnected.

However, depending on the settings on the computer, the remote control agent might automatically stop at the time of the disconnection. In this case, restart the remote control agent, and then reconnect to the computer.

7.5.9 Stopping the controller

To stop remote control, stop the controller.

To stop the controller:

1. From the menu of the **Remote Controller** window, select **File** and then **Close**.

The **Remote Controller** window is closed and remote control stops. If the controller is connected to a computer, the computer is disconnected.

When multiple computers are connected and multiple **Remote Controller** windows are open, only the Remote Controller window in which you performed the disconnection operation is closed.

Tip

When multiple windows are open, if you want to close all windows, select **File** and then **Close All** from the menu.

7.5.10 Changing the connection mode

Set the connection mode for the controller based on the remote control settings for the target remote computer. However, if the remote control mode specified for the agent has higher privileges than those specified for the controller, you might need to change the controller mode when connecting the computer.

To change the connection mode:

1. From the menu of the **Remote Controller** window, select **Tools** and then **Connection Mode**.
2. From the submenu, select **Monitoring Mode**, **Shared** or **Control Mode**.

The connection mode is changed.

You can check the current connection mode from the status bar or the toolbar of the **Remote Controller** window.

You can also change the connection mode by clicking the **Options** button and on the toolbar, and then making changes on the **Connection** tab of the displayed dialog box.

7.5.11 Remotely controlling a computer that has been turned off

You can use the controller to turn on a computer whose power has been turned off and connect to it. To turn on and connect to a computer, you need to set the environment for the controller.

Tip

The default setting enables computers to be turned on and connected to.

To turn on and connect to a computer:

1. In the toolbar of the **Remote Controller** window, click the **Options** button.
2. On the **Connection** tab of the displayed dialog box, select **If Offline, try to startup the Agent PC**.

If the computer is off, it is turned on and connected.

7.5.12 Turning off a remotely controlled computer

You can use the controller to turned off a remotely controlled computer.

Important note

Note that an RFB-connected computer cannot be turned off from the controller. Use the Device module to turn off such a computer. For details, see 6.23 Controlling the computer power.

To turn off a remote computer:

1. From the menu of the **Remote Controller** window, select **Tools** and then **Shutdown**.

The remote computer is turned off.

7.5.13 Rebooting a remotely controlled computer

A remote computer can be rebooted based on a request from the controller. When the controller issues a reboot request, the reboot processing of the computer is interrupted. Wait until the computer automatically restarts. If the agent starts automatically, remote control can be resumed when the computer is connected to from the controller.

Important note

Note that an RFB-connected computer cannot be rebooted from the controller. Use the Device module to reboot such a computer. For details, see 6.23 Controlling the computer power.

To reboot a remote computer:

1. From the menu of the **Remote Controller** window, select **Tools** and then **Reboot** from the menu.
2. In the displayed dialog box, set the actions after the computer is rebooted, and then click **OK**.

The remote computer rebooted.

Tip

If you select **Reboot** from the menu, and then set the computer to be connected to after rebooting in the displayed view, remote control can be automatically resumed after the computer is rebooted.

7.5.14 Using the Ctrl, Alt, and Delete keys in remote control

The **Ctrl**, **Alt**, and **Delete** keys cannot be used directly for a remote computer. To perform the operational equivalent of pressing the **Ctrl**, **Alt**, and **Delete** keys simultaneously, use the exclusive menu.

To perform the operational equivalent of pressing the Ctrl, Alt, and Delete keys simultaneously:

1. In the **Remote Controller** window, click the **Ctrl+Alt+Del** button ().

This operation is equivalent to simultaneously pressing the **Ctrl**, **Alt**, and **Delete** keys on the remote computer.

Alternatively, you can achieve the same results by selecting **Tools** and then **Send Ctrl+Alt+Del** from the menu of the **Remote Controller** window.

7.5.15 Registering a special key with the controller

To use a special key for a remotely controlled computer, you need to register the key in advance.

To register a special key:

1. From the menu of the **Remote Controller** window, select **View**, **Key Input Bar**, and then **Key Input**.
2. In the displayed dialog box, set the special key, and then click **OK**.

The special key is registered.

Tip

The following four key combinations can be set as special keys, so that they can be executed on a remote computer when you press them on the controller:

- **Windows**
- **Ctrl** + **Esc**
- **Alt** + **Esc**
- **Alt** + **Tab**

To enable these keys to be executed on a remote computer, perform the following: In the toolbar of the **Remote Controller** window, click the **Options** button, and then select **Emulate System key input on Agent PC** on the **Advanced** tab of the displayed dialog box.

7.5.16 Using a special key when performing remote control

To use a special key for a remotely controlled computer, use the keyboard input bar. Any registered special keys are displayed on the keyboard input bar.

To use a special key:

1. From the menu of the **Remote Control** window, select **View**, **Key Input Bar**, and then **Key Input Bar**.
   The keyboard input bar is displayed.
2. Click the button on the keyboard input bar.

Any special keys registered to the button you clicked are sent to the connected computer.

7.5.17 Encrypting transferred data when performing remote control

You can encrypt the data (including clipboard data) to be transferred to or received from a remotely controlled computer. The data between the controller and the remote control agent can be protected through data encryption.

To encrypt transferred data:

1. On the toolbar of the **Remote Controller** window, click the **Options** button.
2. On the **Session** tab of the displayed dialog box, select **Encrypt transfer data**, and then click **OK**.

The data to be transferred in remote control is encrypted.

When the transferred data is encrypted, a lock symbol is displayed for the data transfer icon on the status bar.

7.5.18 Enlarging or reducing the views of a computer to match the size of the controller window

The size of the controller window automatically changes based the view resolutions of the remote computers. To make the view of a computer easy to operate, you can enlarge or reduce the view of the computer to match the window size of the controller.

To enlarge or reduce the view of a computer to match the window size of the controller:

1. On the toolbar of the **Remote Controller** window, click the **Auto-zoom** button.

The view of the target computer is enlarged or reduced to match the controller window size. If you click the same button again, the view size is no longer enlarged or reduced.

To change the view of the computer back to normal, click the **Auto-zoom** button on the toolbar.

7.5.19 Remotely controlling a device by using the fullscreen display

By using the fullscreen display on the controller, you can perform remote control as if you were directly using the remote computer.

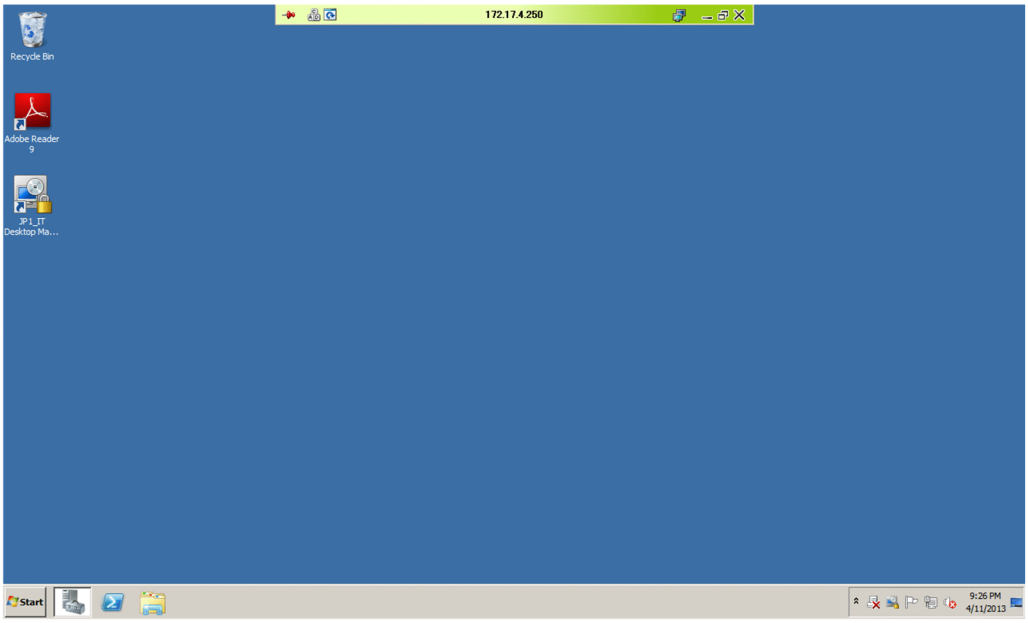
To remotely control a computer by using the fullscreen display:

1. On the toolbar of the **Remote Controller** window, select  .

The controller is switched to fullscreen display mode.

> **Tip**
>
> The controller might not be displayed in fullscreen if its window resolution cannot be changed.

If you move the cursor to the top of the screen while in fullscreen mode, the menu bar appears. You can use this menu bar to specify the screen display status or perform the operational equivalent of simultaneously pressing the **Ctrl**, **Alt**, and **Delete** keys on the remote computer. When you move the cursor away from the top of the screen, the menu bar disappears. Note that you can set the menu bar to be always displayed.



The color of the menu bar changes depending on the connection mode. Therefore, you can determine the current connection mode by the color of the menu bar.

- Green: Control mode
- Yellow: Common mode
- Orange: Monitoring mode

Use the menu bar to exit fullscreen mode.

7.5.20 Tiling multiple controller views

When multiple computers are under remote control, you can tile the controller views to make operations easier.

To tile multiple controller views:

1. From the menu of the **Remote Controller** window, select **Window**, and then **Arrange Vertically**, **Arrange Horizontally**, or **Arrange All**.

The controller views are tiled according to the selected menu. If you selected **Arrange All**, the computer views are equally tiled, both vertically and horizontally.

7.5.21 Showing or hiding controller bars

You can show or hide the toolbar, address bar, or keyboard input bar. By hiding the bars, you can enlarge the display area of the computer view, and operations can be easier to perform.

To show or hide a bar:

1. From the menu of the **Remote Controller** window, select **View**, **Toolbar**, and then **Toolbar**.
   For the status bar, select **View**, **Status Bar**, and then **Status Bar**. For the keyboard input bar, select **View**, **Key Input Bar**, and then **Key Input Bar**.

When the menu is selected, the corresponding bar is displayed.

Tip

You can also show or hide tool button labels. To show tool button labels, select **Toolbar** and then **Button Text Labels** from the **View** menu.

7.5.22 Using auto-scroll to perform remote control

When the computer view is larger than the controller window, a scrollbar is displayed on the controller. If you move the cursor close to an edge of the view when the scrollbar is displayed, you can use the auto-scroll function to automatically scroll the computer view.

To use the auto-scroll function:

1. On the toolbar of the **Remote Controller** window, click the **Options** button.
2. On the **Advanced** tab of the displayed dialog box, select **Scroll synchronized with the mouse pointer**.
3. Select the auto-scroll method, and then click **OK**.

The auto-scroll function is enabled.

You can choose from the following two auto-scroll methods:

- **Always**: When you move the cursor close to an edge of the view, the view automatically scrolls.
- **Only while dragging**: The view automatically scrolls only if you drag the view.

7.5.23 Using the mouse wheel to remotely control scrolling

You can use the mouse wheel to scroll the views displayed on a remote computer.

However, when a scroll bar is displayed on both the view of the controller and the view of the remote computer, the views scroll simultaneously when you use the mouse wheel, making it hard to achieve the desired result. To prevent this from happening, you can control the movement when scrolling with the mouse wheel.

To control scrolling when using the mouse wheel:

1. On the toolbar of the **Remote Controller** window, click the **Options** button.
2. On the **Advanced** tab of the displayed dialog box, select **Disable wheel scroll**, and then click **OK**.

The mouse wheel can no longer be used to scroll in the controller, and only the view of the connected computer can be scrolled by using the mouse wheel.

Tip

You can use the mouse wheel to scroll all views of the remote control functions. When you use the mouse wheel, the view moves vertically if it can be vertically scrolled, and the view moves horizontally if it can be

horizontally scrolled. When the **Remote Controller** window can be scrolled both horizontally and vertically, you can horizontally scroll the view by holding the **Shift** key while using the mouse wheel.

7.5.24 Saving a remote control view as an image

You can save a view on a remotely controlled computer as a BMP file. For example, if you save a remote control error message as it is displayed, you can later use the saved image to analyze the cause of the error or use it as a window image when creating the operation manual.

To save a computer view:

1. From the menu of the **Remote Controller** window, select **File** and then **Save Screen**.
2. In the displayed dialog box, specify the file name and the storage location.
   You can also specify the number of colors for the file to be saved. The default setting is the same as the number of colors of the computer view.

The view in operation is saved as a BMP file.

7.5.25 Using a remote CD-ROM

The CD/DVD drive on the controller computer can be used as a drive of a remote computer. Therefore, you can use the CD-ROM to install software without transferring files while performing remote control. Also, for an RFB-connected computer, you can also recover the OS by specifying the remote CD-ROM drive as the boot drive.

Important note

To use the remote CD-ROM function, the AMT IDE-R function must be available for the remote computer. You can use either the standard method or the RFB method to connect.

To use a remote CD-ROM:

1. From the menu of the **Remote Controller** window, select **Tools** and then **CMount CD/DVD**.

The CD/DVD drive on the controller can now be used as a drive of the connected controller. In this case, the drive name and the name of the remote computer are displayed, following the names of the menu items.

To disable the remote CD-ROM, select **Tools** and then **Unmount CD/DVD** from the menu.

Tip

Note that the remote CD-ROM remains mounted even when the remote control is disconnected. Therefore, you can use the remote CD-ROM drive as the boot drive when starting a remote computer.

7.5.26 Searching for connectable computers by using the Remote Controller window

You can use the **Remote Controller** window to search for computers that can be connected to within the network. Then, you can connect to and remotely control computers found in the search.

To search for computers by using the Remote Controller window:

1. In the **Remote Controller** window, click the **Connect** button, and then select **Connection**.
2. In the displayed dialog box, click the **Search** button.
3. In the displayed dialog box, specify the range of the IP addresses you want to search.
4. Click the **Search** button.

The computer search starts, and the search progress is displayed.

You can start remote control by selecting the computers that are waiting for a connection from the computers found in the search and then clicking the **Connect** button.

Note that when some of the computers found in the search are connected to, all information about the other computers found in the search is removed. If you want to save the search results, we recommend that you use the connection list to search for the computers.

Related Topics:

- 7.5.27 Searching for connectable computers by using the connection list

7.5.27 Searching for connectable computers by using the connection list

You can use the connection list to search for computers that can be connected to within the network. Then, you can connect to and remotely control the computers found in the search.

To search for computers by using the connection list:

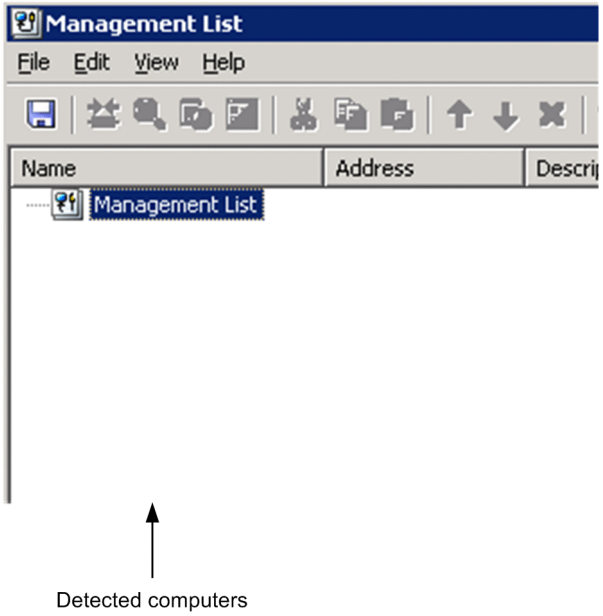
1. From the menu of the **Remote Controller** window, select **Connection List** and then **Change List**.
2. From the displayed connection list, select the location to create a **Network** icon.

> **Tip**
>
> A **Network** icon is an icon for which a range-of-agents search is set. For each **Network** icon, you can specify any range of addresses in the same subnetwork. You can repeatedly perform the searches of the same range by creating a **Network** icon in the connection list. You can also search for remotely controllable computers by using the **Search Agents** dialog box which is displayed by using the **Remote Controller** window.

3. From the menu of the connection list, select **File**, **New**, and then **Network**.
4. In the displayed dialog box, specify the network name and the range of the IP addresses, and then click **OK**.
5. Double-click the **Network** icon you created.

The computer search starts, and the search progress is displayed in the **Search Agents** dialog box.

If you close the **Search Agents** dialog box after the search is completed, the computers displayed in the **Computer** tab of the dialog box are added as subitems of the **Network** icon. Note that if you click the **Close** button during the search, only the computers that have been found so far are added.



Tip

Only the computers displayed on the **Computer** tab of the **Search Agents** dialog box are added to the connection list. Therefore, when the search is completed, click the icon before closing the dialog box, so that the computers to add to the connection list are displayed on the **Computer** tab. For example, if you want to manage the configuration of all computers on the network by using the connection list, regardless of whether the computers can be connected to, you need to select all computers that are in the statuses from waiting for a connection to no response. Conversely, if you only want to add the computers that can be currently connected to, select only the computers in the status of waiting for a connection.

Note that the computers found in a search are temporarily displayed as search results, so they are not saved as data. The computer information disappears when the connection list is closed. If you want to save the information of the computers found in a search, you need to drag and drop the computers to another group. The computers are treated as the computers on the connection list after being moved to a group, and the computer names and descriptions can be changed.

7.5.28 Customizing the search method for computers available for remote control connections

You can customize the method for searching for computers that can be connected to. For example, you can enable or disable name resolution or customize the connection verification method.

To customize the agent search method:

When using the **Remote Controller** window to search

In the **Search Agents** dialog box, click the **Settings** button. In the displayed **Agent Search Setting** dialog box, customize the search method.

When using the connection list to search:

You can customize the search method in the dialog boxes below. The items to specify are the same as those in the **Agent Search Setting** dialog box. However, in the connection list, you can also specify the connection options for the agents on the computers that are found in a search.

- The **Setup** tab of the **New Network** dialog box which is displayed for creating a new network
- The **Setup** tab of the **Properties** dialog box that displays network properties
- The **Setup** dialog box for the network that is displayed from the **Properties** dialog box of a folder or multiple items

7.6 Transferring files

7.6.1 Opening the File Transmission window

To open the **File Transmission** window, a remote computer must be connected.

To open the File Transmission window:

1. On the toolbar of the **Remote Controller** window, click the **File Transmission** button ().

The **File Transmission** window is opened. You can also open the **File Transmission** window by selecting **Tools** and then **File Transmission** from the menu.

> **Tip**
>
> You can also transfer files by dragging and dropping them onto the computer view displayed on the controller. In this case, files can be transferred immediately after the **File Transmission** window opens.

Related Topics:

- 7.6.3 Closing the **File Transmission** window

7.6.2 Terminating a file transfer connection

You can terminate a file transfer connection with a computer. The file transfer connection is also terminated when the computer is logged off from. Note that remote control remains connected even if the file transfer connection is terminated.

To terminate a file transfer connection:

1. From the menu of the **File Transmission** window, select **File**, **Disconnect**, and then the computer to be disconnected.

The file transfer connection is terminated.

Note that if a file is being transferred or deleted, the processing is also terminated.

> **Important note**
>
> When remote control is disconnected, the file transfer connection is automatically terminated.

> **Important note**
>
> When the connection mode is changed to monitoring mode, the file transfer connection with the remote computer is also terminated. In this case, if a file is being transferred or deleted, a dialog box is displayed to make sure that you really want to terminate processing.

7.6.3 Closing the File Transmission window

You can terminate a file transfer connection after file transfer is completed. To terminate the connection, close the **File Transmission** window.

To close the File Transmission window:

1. From the menu of the **File Transmission** window, select **File** and then **End**.

The **File Transmission** window is closed.

When the window is closed, all file transfer connections are automatically terminated. Note that if a file is being transferred or deleted at the moment the window is closed, that processing is also terminated.

7.6.4 Adding a computer as a file transfer destination

When you open the **File Transmission** window, the computers connected to the controller that you used to open the File Transmission window are displayed in the tree view. You can transfer files between multiple computers by adding computers to the tree view.

Note that only the computers being remotely controlled can be added to the **File Transmission** window. Also, the computers must be logged on to the OS.

To add a computer as a file transfer destination:

1. Start the **File Transmission** window by using the controller that is connected with a computer.

The computer is added to the File Transmission window. Note that you cannot simultaneously open multiple **File Transmission** windows.

7.6.5 Checking the file information to be transferred

You can check the detailed information and total size of the files being selected in the **File Transmission** window, or of the files to be copied or moved that are specified in the **Edit** menu. To check the file information, display the **File Confirmation** dialog box.

To check the information of a selected file:

1. Select the file or folder, and then from the menu of the **File Transmission** window, select **Edit**, **Confirm Files**, and then **Selected File**.

To check the information of a reserved file:

1. From the menu of the **File Transmission** window, select **Edit**, **Confirmation**, and then **Reserved File**.
   The **Reserved File** menu is activated when a file to be copied or transferred is reserved.
2. Click **OK** when you finished checking the file information.

If you used the **Remove** button to cancel the reservation, the cancellation takes effect when you click **OK**. If you click the **Cancel** button, the cancellation by clicking the **Remove** button is disabled.

You can change the type of file transfer in the **File Confirmation** dialog box. To reserve a file for copying or moving, select the file and then change its **Type** from **Select** to **Copy** or **Move**. Also, when you are checking the information of a reserved file, you can also change the reservation type (copying or moving).

7.6.6 Setting up secure file transfers

To safely transfer files, you must specify security settings. You can use the following two methods to secure file transfers:

- Transfer data encryption

  Data to be transferred via the network might be leaked to a third-party if it is transferred without protection. Data encryption protects the data to be transferred between the controller and remote control agent from a third-party.
- Setting file access permissions

  In the **File Transmission** window, you can set the same access permissions for the controller and remote computers. Therefore, to prevent files being used on the business server by mistake, you can set permissions for access from the controller.

To encrypt the data to be transferred:

1. On the toolbar of the **Remote Controller** window, click the **Options** button ().
2. On the **Session** tab of the displayed dialog box, select **Encrypt transfer data**, and then click **OK**.

The data to be transferred is encrypted.

When data is encrypted, a lock icon is displayed on the controller and the target computer.

To set file access permissions:

1. Specify **Access Permission to File** for **Remote Control Settings** during agent setup.

File access from the controller is limited according to the specified access permissions.

Access permissions include the read/write permission. Executable file operations differ depending on which access permissions are set. For example, when only the read permission is set, an error message is displayed if you try to transfer files to a remote computer.

7.6.7 Transferring files

You can use the **File Transmission** window to perform two-way file transfers between the controller and a remote computer. In addition, when more than one computer is connected, files can be transferred between the remote computers.

There are three main methods for transferring files by using the **File Transmission** window. Each method is described below:

To transfer by dragging and dropping files:

You can transfer files and folders displayed in the **File Transmission** window by dragging and dropping files. When you drag and drop files, the files are copied. To move files, drop the files while holding down the **Shift** key. In addition, if you drag the files with the right mouse button, a menu appears when you drop the files. You can select from the three options in the menu: **Move**, **Copy**, or **Cancel**.

You can also use this drag-and-drop method to transfer files between the system explorer and the **File Transmission** window. In this case, all files being transferred are copied even if you press down the **Shift** key.

To transfer by registering the files:

1. Select the files or folders you want to transfer, and then click the **Register for Copying** button () or the **Register for Moving** button () on the toolbar of the **File Transmission** window.
2. Select the drive or folder to which the data is transferred, and then click the **Transfer Files** button () on the toolbar.

The file transfer starts.

To perform multitransfer:

Multitransferring is a method for simultaneously transferring files to more than one computer. You can specify the transfer destination as a default folder or specify the transfer destination as the same name as the transfer source, to avoid the trouble of entering the folder name.

1. Select the files or folders you want to transfer, and then click the **Customized Transfer** button () on the toolbar of the **File Transmission** window.
2. In the displayed dialog box, specify the computer and the folder to which the data will be transferred, and then click the **Transfer Files** button.

The file transfer starts. When more than one computer is selected, data is transferred to each computer.

7.6.8 Performing operations on files of a remotely controlled computer

When you perform operations on files of a remotely controlled computer from the controller, you cannot only call and perform operations from the computer view, but also use the **File Transmission** window.

If you open a computer file from the **File Transmission** window, the file is transferred from the computer to the controller. Therefore, the computer user is not affected when you edit the file. The file is transferred to the folder that was specified in the options of the **File Transmission** window.

When files with the same name are opened from different computers, the controller receives the files in the same order as the files are opened. In this case, a newly received file overwrites the file received earlier, and the file received last is opened.

To edit a computer file from the File Transmission window:

1. In the **File Transmission** window, select the computer file you want to edit, and then select **File** and then **Open** from the menu.

   Tip

   You can also open a file by double-clicking the file.

2. Edit the displayed file.
3. Close the file after editing it.

4. In the displayed dialog box, click the **Yes** button.

The file edited on the controller is transferred to the original location on the computer, and overwrites the old file.

You can set a file to be automatically transferred, removed, or kept on the controller. To do so, click the **Options** button on the toolbar, select the **File** tab of the displayed dialog box, and then change the settings for remote files.

If the file is not set to be automatically transferred or removed, the controller file is not transferred when you close the file, but remains in the temporary folder.

To manually transfer or remove a file:

When you open a computer file from the **File Transmission** window, the file is temporarily saved on the controller. If the file is not set to be automatically transferred or removed, the controller file is not transferred when you close the file, but instead kept on the controller.

You can check the files kept on the controller in the **File Transmission** window of the remote files list. In this window, you can transfer the files kept on the controller or remove them from the controller.

1. From the menu of the **File Transmission** window, select **View** and then **Download Manager**.
2. From the menu of the **File Transmission** window of the remote control list, select **Edit** and then **Transfer Files** or **Delete After Transfer**.

The edited file is transferred to the original location on the computer.

When **Transfer Files** is selected, the processing is the same as when copying the file, so the file is also kept on the controller. When **Delete After Transfer** is selected, the processing is the same as when moving the file, so the file is not kept on the controller.

To remove a file from the controller, select **File** and then **Remove** from the menu. A dialog box showing the deletion progress is displayed, and the file kept on the controller is removed.

Related Topics:

- 7.6.10 Setting file transfer options

7.6.9 Editing a file from the File Transmission window

In the **File Transmission** window, you cannot only transfer files, but also perform the operations below on the folders or files of the controller and remote computer. Note that to perform these operations, you need the necessary permissions to access the folders or files.

- Creating a folder
- Deleting a folder or file
- Changing the properties of a folder or file
- Changing the name of a folder or file

To create a folder:

1. Select the location (drive or folder) where the new folder will be created.
2. On the toolbar, click the **New** button ().

3. Enter the folder name.

The new folder is created at the selected location.

To remove a folder or file:

1. Select the folder or file that you want to remove.
2. On the toolbar, click the **Remove** button ( ).

> **Tip**
>
> You can also remove the folder or file by pressing the **Delete** key on the keyboard.

3. In the displayed dialog box, click the **Yes** button or the **Delete All** button.

The selected folder or file is removed. A dialog box showing the deletion progress is displayed on the controller.

To change the properties of a folder or file:

1. Select the folder or file whose properties you want to change.
2. From the menu, select **File** and then **Property**.
3. In the displayed dialog box, specify the properties as necessary, and then click **OK**.

The properties are changed as specified. You can only change the properties of a selected folder or file. The properties of the folders or files in a lower level are unchanged.

To change the name of a folder or file:

1. Select the folder or file that you want to change.
2. Click the folder name or file name. Alternatively, from the menu of the **File Transmission** window, select **File** and then **Rename**.
3. Enter the name.

The name of the folder or file is changed.

7.6.10 Setting file transfer options

To efficiently use the **File Transmission** window, we recommend that you set options in the **Options** dialog box. In the options, you can set items such as the type of files to display and the actions to take after file transfers.

To set file transfer options:

1. On the toolbar of the **File Transmission** window, click the **Options** button ( ).
2. In the displayed dialog box, specify options, and then click **OK**.

The specified information is saved.

The setup items in the **Options** dialog are as follows:

- The **View** tab
  On the **View** tab, specify the options related to the display of the **File Transmission** window.
- The **File** tab
  On the **File** tab, specify the actions to take when a computer file is open or closed.

7.7 Using the connection list

7.7.1 Setting up a connection environment for individual computers

You can set up a connection environment for individual computers. By setting up a connection environment for individual computers, you can make sure that the connection settings are correct without having to change the environment every time you connect to a computer.

To set up a connection environment for a single computer:

1. Select the computer for which you want to set up a connection environment.
2. On the toolbar, click the **Properties** button ().
3. On the **Settings** tab of the displayed dialog box, select **Set up the connection options**.
4. Specify the options as necessary, and then click **OK**.
   For some items, advanced setup items might be displayed in the **Details** field. Specify these items as well.

The connection environment is set up for the selected computer. The settings specified here are applied from the next time you make a connection.

To set up a connection environment for multiple computers:

To specify the same conditions for multiple computers you want to connect, you can set up a connection environment in a batch operation.

1. Select the computers for which you want to set up a connection environment.
2. On the toolbar, click the **Properties** button ().
3. On the **Settings** tab of the displayed dialog box, click the **Settings** button in **Agent**.
4. In the displayed dialog box, select **Set up the connection options**.
5. Specify the options as necessary, and then click **OK**.

The connection environment is set up for the selected computers.

To set up a connection environment for multiple computers of the same group or network in a batch operation, select the **Group** icon or the **Network** icon, and then perform the above procedure.

To set up a connection environment for a computer found in a search:

You can set up a specific connection environment for a computer that was found by searching the network. In this case, set up a connection environment for the network used in the search, instead of for the computer. You cannot set up a connection environment for computers found in a search. However, you can set up a connection environment before performing the search.

1. Select the network.
2. On the toolbar, click the **Properties** button ().
3. On the **Setup** tab of the displayed dialog box, click the **Settings** button for **Found Agent PC**.

4. In the displayed dialog box, select **Set up the connection options**.

5. Specify the options as necessary, and then click **OK**.

The connection environment settings for the computer that was found in the search are saved. The connection environment specified here is applied from the next time you connect to the computer found in the search.

To set up a connection environment for a request agent:

You can set up a connection environment if you want to perform remote control from a request agent. In this case, set up a connection environment for the request server, instead of for the request agent. You cannot set up a connection environment for request agents. However, you can set up a connection environment before the connection request is received.

1. Select the request server.

2. On the toolbar, click the **Properties** button ().

3. On the **Settings** tab of the displayed dialog box, click the **Settings** button in **Request Agent**.

4. In the displayed dialog box, select **Set up the connection options**.

5. Set the options as necessary, and then click **OK**.

The connection environment is set up for the computer (request agent) being connected to the request server.

7.7.2 Displaying or closing the connection list

To display the connection list:

You can use the following two methods to display the connection list:

- From the menu of the **Remote Controller** window, select **Connection List** and then **Change List**.
- In the **Remote Controller** window, click the **Connect** button, and then select **Change List** from the displayed menu.

You can display the connection list without connecting a computer. You can also issue a request to connect a computer from the connection list.

To close the connection list:

1. From the menu of the connection list, select **File** and then **Close**.

If you edited the connection list before closing it, the dialog box is displayed to check whether you want to save the changes before closing the connection list. To save the changes, select **File** and then **Save** or **Save As** from the menu.

7.7.3 Connecting a computer from the connection list

You can connect a computer by double-clicking its icon displayed on the connection list. You can also use the icon of a computer found in a search.

In addition, if you double-click the icon of a request agent, the computer that issued the connection request can be connected to. In this case, inactive request agents (whose connection request has been canceled) can also be connected to.

When a computer is connected to, the IP address, host name, or the path for the computer is recorded in the address bar of the **Remote Controller** window.

7.7.4 Creating the connection list

There are different methods available for creating the connection list. Select a method that is appropriate for the scale and operation of the network that you want to manage.

- By adding the connected computers in the **Remote Controller** window
- By using the existing connection list
- By adding the computers found in a search
- By importing from the hosts file
- By using the backup file

In addition, when you add a new item to the connection list (such as a group, computer, or dividing line), the location where the item is created varies as described below, depending on the item you selected first.

- If you create an item by selecting the root or group, the new item is created to the end of the hierarchy below the selected root or folder.
- If you create an item by selecting a computer or dividing line, the new item is created in the next position (in the same hierarchy level) of the selected computer or dividing line.

To create the connection list by adding the connected computers in the Remote Controller window:

1. From the menu of the **Remote Controller** window, select **Connection List** and then **Add to List**.
   You can also select the **Connect** button and then **Add to List**.

2. In the **Set New Agent** dialog box, specify the computer names in **Name**.
   The names specified here will be displayed in the **Name** field of the connection list.

3. To save the connection options for the connected computers, select **Save connection options**.
   For details about how to specify the connection options for a computer, see 7.7.1 Setting up a connection environment for individual computers.

4. Click **OK**.

The computers are added to the connection list.

To create the connection list by using the existing connection list:

You can add the computers to the existing connection list. You can use the connection list to create a group and then add the computers to the group, or create a dividing line to organize the computer configuration information. After a dividing line is created, the computer configuration can be easily understood from the menu by clicking the **Connect** button in the **Remote Controller** window.

The following describes the procedure for creating a group, computer, or dividing line:

1. On the connection list, select the location where you want the group, computer, or dividing line to be created.
2. From the menu of the connection list, select **File**, **New**, and then **Group**, **Agent**, or **Separator**.
3. To create a group or computer, specify the information on both the **User** tab and **Settings** tab of the displayed dialog box, and then click **OK**.
   Note that the information on the **Settings** tab can be changed even after the group or computer is created.

The group, computer, or dividing line is created in the connection list.

To create the connection list by adding the computers found in a search:

You can use the connection list to search for computers on the network, and add the computers that can be connected to to the connection list. The procedure for this method can be divided into three major steps:

1. Create a **Network** icon for specifying the range of the addresses to be searched.
2. Use the **Network** icon to search for computers.
3. Add the computers found in the search to the connection list.

For details about how to specify the search scope, view the search results, or set search restrictions, see 7.5.27 Searching for connectable computers by using the connection list.

> **Tip**
>
> The **Network** icon can be used for specifying the scope of the search. You can specify any range of addresses within the same subnet for each **Network** icon. By creating a **Network** icon on the connection list, you can repeatedly perform the search within the same scope. You can also search for computers by clicking the **Connect** button in the **Remote Controller** window, and then selecting the **Network** icon in the displayed connection list.

To search for computers and then add them to the connection list:

1. In the connection list, select the location where you want the **Network** icon to be created.
2. From the menu of the connection list, select **File**, **New**, and then **Network**.
3. On both the **User** tab and the **Setup** tab of the **New Network** dialog box, specify the information and then click **OK**.
   Note that the information on the **Setup** tab can be changed even after the **Network** icon is created.
4. Double-click the **Network** icon created on the connection list.
   The **Search Agents** dialog box is displayed, and the search for the computers is performed within the specified scope.
5. When the search is complete, click the **Details** button to display the **Computer** tab.
6. Arrange the information displayed on the **Computer** tab, so that only the computers to be added to the connection list are displayed.

   > **Tip**
   >
   > For example, if you want to use the connection list to manage the configurations of all computers on the network, regardless of whether the computers are running, select all items that are in the statuses from

Waiting for connection to **Not responding**. However, if you want to only add the computers that can be currently connected to the connection list, select **Waiting for connection** only.

7. Click the **Close** button.

The computers displayed on the **Computer** tab of the **Search Agents** dialog box are added as subitems of the **Network** icon. Note that if you click the **Close** button during the search, only the computers that have been found so far are added.

Important note

The computers found in a search are temporarily displayed. The computer information disappears when you close the connection list. To save the information of the computers found in a search, move the computers into another group by dragging and dropping them. By doing so, you can save the computers as one item of the connection list. Once the computers are saved, they are handled as regular computers, and computer names and descriptions can also be changed.

To create the connection list by importing from the hosts file:

If you use the hosts file, you can add all computers that are defined in the hosts file to the connection list in a batch operation. The procedure for importing computers from the hosts file is as follows:

1. On the connection list, select the location where you want the computer to be added (read the hosts file information).
2. From the menu of the connection list, select **File**, **Import**, and then **Hosts File**.
3. In the **Open** dialog box, select the hosts file, and then click the **Open** button.

All of the computers defined in the hosts file are added to the connection list. Note that the information in the hosts file is handled according to the following rules:

- Spaces or tabs before and after an item are ignored.
- Lines that start with the character # are ignored.
- The characters between the first space or tab and the next space or tab are treated as a name.
- Aliases are ignored.
- If a line contains an IP address, a host name and the character #, the character string after the # is treated as a description of the computer.

To create the connection list by using the backup file:

You can save the connection list as a backup file with any name by selecting **File** and then **Save As** from the menu.

When you import the backup file, the connect list items can be added as they were saved. The procedure for importing the connection list from the backup file is as follows:

1. In the connection list, select the location where you want the computer to be added (read the information in the backup file).
2. From the menu of the connection list, select **File**, **Import**, and then **System File**.
3. In the **Open** dialog box, select the backup file, and then click the **Open** button.

The connection list information is added to the specified location as it was saved.

7.7.5 Moving or copying a connection list item

You can move or copy a network, group, computer, request server, or dividing line that is displayed on the connection list.

You can choose from the following three methods to move or copy a connection list item. Note that when you move or copy a folder, the items contained in the folder are also moved or copied.

- Moving an item by dragging and dropping it. (You can copy an item by holding down the **Ctrl** key while moving the item.)
- Using the **Cut** button, the **Copy** button, or the **Paste** button on the toolbar
- Moving by clicking the **Shift Up** button or the **Shift Down** button

Notes on moving or copying a request server that is running:

- When you cut a request server, a message is displayed to make sure that the request server can be stopped.
- When you move a request server, the request server keeps running after being moved.
- When you copy a request server, the request server is stopped at the copy destination.

7.7.6 Removing a connection list item

You can remove a network, group, computer, request server, or dividing line that is displayed in the connection list.

To remove a connection list item:

1. From the connection list, select the item you want to remove.
2. On the toolbar, click the **Remove** button ().

The selected item is removed.

> **Tip**
>
> You can also remove an item by pressing the **Delete** key.

If you try to remove a request agent that is currently running, a message appears to make sure that the request server can be stopped. Note that the same message also appears if you try to remove a folder that contains a request server that is running.

When a request agent is removed, all requests for connecting the computer are canceled.

7.7.7 Changing the name of a connection list item

You can change the name of a network, group, computer, or request server that is displayed in the connection list.

To change the name of a connection list item:

1. In the connection list, select the icon whose name you want to change.

2. From the menu of the connection list, select **File** and then **Rename**.

3. Enter the new name.

The name of the selected item is changed.

7.7.8 Changing the properties of a connection list item

You can change the properties of a network, group, computer, or request server that is displayed in the connection list.

You can change the name, address (port number of the request server), and descriptions. You can also change the following properties:

- For networks
  You can change the method for searching for computers and the connection environment for the computers found in a search.
- For groups
  In a batch operation, you can change the properties of the computers, networks, and request servers contained in a group.
- For computers
  You can change the connection environment.
- For request servers
  You can change the properties of the request server and the connection environment of the computer that requests for a connection.

To change the properties of a connection list item:

1. On the connection list, select the icon whose properties you want to change.
   You can also select multiple icons to change properties in a batch operation.

2. On the tool bar, click the **Properties** button ().

3. In the displayed dialog box, change the settings as necessary.

4. Click **OK**.
   If the group you selected contains a lower-level group, or if you selected multiple items, a message is displayed to check whether you want to change the properties of the lower-level group.

The properties of the selected item are changed.

Note that the properties cannot be changed for a computer that was found in a search or is requesting a connection (request agents). Move the computer to another group, and then change the properties.

7.7.9 Searching for connection list items

You can use a character string that is contained in a name, address, or description as a keyword to search for items displayed on the connection list. If you specify multiple keywords, items that contain all keywords are matched.

To search for connection list items:

1. Select the icon from where you want the search to start.
2. From the menu of the connection list, select **Edit** and then **Find**.
3. In the displayed dialog box, enter the information as necessary.
4. Click the **Search** button.

The dialog box is closed, and the system performs a downward search from the first icon you selected. The first icon that matches the search condition is displayed and highlight. To continue the search by using the same keyword, select **Edit** and then **Find Next** from the menu, or press the **F3** key.

When no more items are found, the **Seach Completed** dialog box is displayed.

7.7.10 Viewing the properties of a connection list item

You can view the properties of a network, group, computer, or request server that is displayed in the connection list.

To view the properties of a connection list item:

1. On the connection list, select the icon whose properties you want to view.
2. On the toolbar, click the **Properties** button ().

You can view the properties of the selected item in the displayed dialog box.

7.7.11 Creating a request server

To receive a connection request from an agent, you need to create a request server on the connection list.

To create a request server:

1. On the connection list, specify the location where you want the **Request Server** icon to be created.
2. From the menu, select **File**, **New**, and then **Request Server**.
3. On the **User** tab of the **New Request Server** dialog box, specify the information in the **Name**, **Port**, and **Description** fields.
   In **Port**, specify the port number to be used when connecting from the agent. The default setting is 31019.
4. On the **Settings** tab, specify the properties for the request server. If you do not specify the properties now, you can specify them later.
5. Click **OK**.

The request server is created, and the **Request Server** icon () is displayed in the specified location.

As is the case with items such as a group or computer, you can change the name and properties of the **Request Server** icon. For details about how to change the properties of a request server, see 7.7.8 Changing the properties of a connection list item.

Related Topics:

- 7.7.12 Starting or stopping a request server

7.7.12 Starting or stopping a request server

To receive a connection request from an agent, you need to display the connection list and then start the request server. From the display status of the icon, you can check whether a request server is running or has been stopped. The running and stopped statuses of the icon are as shown below:

 : The running status

 : The stopped status

You can start a request server automatically or manually.

To automatically start a request server:

1. On the connection list, select the **Request Server** icon.
2. On the toolbar, click the **Properties** button ().
3. On the **Settings** tab of the displayed dialog box, select **Start Request Server when Management List starts**.

The request server automatically starts when the connection list is displayed.

To manually start a request server:

1. On the connection list, select the **Request Server** icon.
2. On the toolbar, click the **Start** button ().

The selected request server starts.

Note that an error occurs and the request server does not start in the following situations:

- When the port number that the request server is trying to use is already in use
- When the controller, which was started from the connection list that was used the last time, is currently connected to the computer

To stop a request server:

1. On the connection list, select the **Request Server** icon.
2. On the toolbar, click the **Stop** button ().
3. In the message dialog box, which is displayed to make sure that the request server can be stopped, click the **Yes** button.

The selected request server stops.

Note that if you cut or remove a request server while it is running, the request server stops.

7.8 Using the recording function

7.8.1 Playing back a recording

When you are playing back a recorded file, you might want to pause the playback to provide a detailed explanation, or only play a specific part that you might want to emphasize. You can use a remote control device to pause or skip the recording, as necessary. You can also control the play speed by using fast-forward or slow-play mode. You can perform the following operations when playing back a recording:

To stop playback:

1. On the toolbar of the remote control device, click the **Stop** button ().

Playback stops.

To pause playback:

1. On the toolbar of the remote control device, click the **Pause** button ().

Playback pauses.

To restart playback:

1. On the toolbar of the remote control device, click the **Play** button ().

If you click the **Play** button while playback is paused, playback restarts from the position where it was paused. If you click the **Play** button while playback is stopped, playback restarts from the beginning of the recorded file, instead of from the position where the playback was stopped.

To skip playback:

1. Select the slider on the seek bar, and then move it to the desired position.

The recording between the positions where the playback stopped and where you slided to is skipped. If you slide the slider back to the beginning, the recording automatically starts at the beginning.

> **Tip**
>
> You can use this function during playback or while playback is paused. The slider cannot be moved (skipped) if playback is stopped.

If you skipped through the recording during playback, playback restarts from the position where you skipped to. If you skipped through the recording while playback is paused, playback pauses at the position where you skipped to.

To play faster (fast forward):

1. On the toolbar of the remote control device, click the **Fast Forward** button ().

The recording is played at a speed three times that of regular mode.

To play slowly (slow-play):

1. On the toolbar of the remote control device, click the **Slow** button ( ).

The recording is played at a speed one-third that of regular mode.

7.8.2 Displaying the playback view

You can display the playback view on the remote control device in the same way you can display the computer view in the **Remote Controller** window.

To enlarge or reduce the playback view:

1. From the menu of the remote control device, select **View**, **Zoom**, and then **Automatically**.

The playback view is automatically enlarged or reduced to match the window size of the remote control device. You can also display the playback view in a size 50%, 100%, or 200% of the normal size. To do so, select **View** from the menu, and select **Zoom** and then **50%**, **100%**, or **200%**. The default setting is 100% (actual size).

To display in a full screen:

1. From the menu of the remote control device, select **View** and then **Full Screen**.

The playback view is displayed in full screen. To exit from full-screen mode, select **Full Screen** from the pop-up menu.

To match the window of the remote control device with the size of the playback view:

1. From the menu of the remote control device, select **Window** and then **Fit to Frame**.

The window of the remote control device is enlarged or reduced according to the size of the playback view.

To tile windows of multiple remote control devices:

1. From the menu of the remote control device, select **Window** and then **Arrange Vertically**, **Arrange Horizontally** or **Arrange All**.

The windows of the remote control devices are tiled in the controller view.

7.8.3 Recording remote control information

You can record the window information of a computer that is connected to the controller. The recording can be paused or restarted after being paused.

To record remote control information:

1. From the menu of the **Remote Controller** window, select **File**, **Record Screen**, and then **Start**.
2. In the displayed dialog box, specify the storage location and the name of the file to be recorded.
   The extension of the recorded file is jcr.
3. Click the **Save** button.

The computer view is recorded.

To stop the recording, select **File**, **Record Screen**, and then **Stop**.

> **Tip**
>
> You can also right-click the icon on the status bar when the icon is in the recording status, and then start recording from the displayed menu.

Related Topics:

- 7.8.4 Pausing or restarting the recording
- 7.8.5 Playing back recorded data
- 7.8.7 Converting a recorded file into AVI format

7.8.4 Pausing or restarting the recording

You can pause or restart the recording. This function enables you to only record the window information that is necessary.

To pause the recording:

From the menu of the **Remote Controller** window, select **File**, **Record Screen** and then **Pause**.

The recording is paused.

To restart the recording:

From the menu of the **Remote Controller** window, select **File**, **Record Screen**, and then **Restart**.

The recording is restarted.

Related Topics:

- 7.8.5 Playing back recorded data

7.8.5 Playing back recorded data

When you record remote control information, the view information of the computer is saved as recorded data. To play back recorded data, use the remote control device.

To play back recorded data:

1. From the menu of the **Remote Controller** window, select **File**, **Play Screen**, and then **Play**.
2. In the displayed dialog box, select the recorded file that you want to play back, and then click the **Open** button.

The remote control device starts, and the recorded file is played back automatically.

You can check the playback progress from the seek bar displayed on the bottom of the remote control device. When playback starts, the slider on the seek bar moves from left to right.

If the seek bar is not displayed, select **View** from the menu of the remote control device and then **Seek Bar**.

Related Topics:

- 7.8.3 Recording remote control information
- 7.8.1 Playing back a recording
- 7.8.7 Converting a recorded file into AVI format

7.8.6 Checking the information of a recorded file

To check the information of the recorded file that is being displayed, select **File** from the menu of the remote control device and then **Properties**. You can check the following information in the **Properties** dialog box that is displayed:

- Location (where the recorded file is stored)
- Size
- Connection destination (the IP address, host name, or path for the computer on which the file was recorded)
- Version (the version of the agent installed on the computer on which the file was recorded, or the RFB version)
- Resolution (of the computer on which the file was recorded)
- Color palette (the number of colors of the computer on which the file was recorded)
- Recording start date and time (which is displayed in the format *MM*/*DD*/*YYYY hh*:*mm*:*ss*, where MM is the month; DD is the day; YYYY is the year; hh is the hour; mm is the minutes; and ss is the seconds)
- Recording time# (which is displayed in the format *mm* minutes *ss* seconds, where mm is the minutes and ss is the seconds)

#: If the recording time exceeds one hour, it is displayed in minutes.

7.8.7 Converting a recorded file into AVI format

To play a recorded file, you need a remote control device that provides the controller. Therefore, the recorded files can be played only in an environment where the controller is installed. However, by converting a recorded file into an AVI file, you can play the recorded information on a computer without the controller installed.

In addition, after converting a recorded file into an AVI file, you can use other applications to edit the file, such as adding a title or comments. However, note that if you changed the computer resolution during the recording, the recorded file cannot be correctly played back even if it has been converted into an AVI file.

Use the conversion wizard to convert a recorded file into an AVI file. The following describes how to use the conversion wizard to convert a recorded file into an AVI file.

To convert a recorded file into the AVI format:

1. From the menu of the **Remote Controller** window, select **File**, **Play Screen**, and then **Convert**.
   The conversion wizard starts.
2. Select the recorded file that you want to convert, and then click the **Next** button.
3. Specify the AVI file into which the file is converted, and then click the **Next** button.
4. Select the compression format that you want to use to convert into an AVI file, and then click the **Next** button.

5. Specify the frame rate and image quality, and then click the **Next** button.

6. The conversion starts, and the conversion progress is displayed.

7. After the conversion is completed, click the **Complete** or **Play** button.

The conversion wizard is closed.

If you click the **Play** button, the application that is associated with the AVI file starts, and the conversion wizard is closed. The default settings in Windows are used to start Windows Media Player.

7.9 Using the remote control agent

7.9.1 Displaying the status window of the remote control agent

You can move the **Remote Control Agent** icon from the status bar, and display it as the status window.

To display the status window:

1. Right-click the **Remote Control Agent** icon, and then select the **Show Menu** menu.
2. From the submenu, select **Immediately** or **If Connected**.

If you select **Immediately**, the status window is displayed immediately after the selection. If you select **If Connected**, the status window is displayed only when the controller is connected.

To hide the status window:

1. Right-click anywhere in the status window, and then select the **Minimize** menu.

The status window is closed, and the **Remote Control Agent** icon is displayed in the status bar.

Note that you can also hide the status window by clicking the **-** button.

7.9.2 Stopping the remote control agent

The remote control agent is automatically stopped when you close the OS of the computer. If the remote control agent was manually started, it stops when you log off Windows.

You can also stop the remote control agent without closing Windows.

To manually stop the remote control agent:

1. Right-click the **Remote Control Agent** icon or anywhere in the status window.
2. Select **Exit**.
   When the status window is displayed, you can also use the **x** button instead of the menu.

The remote control agent is stopped.

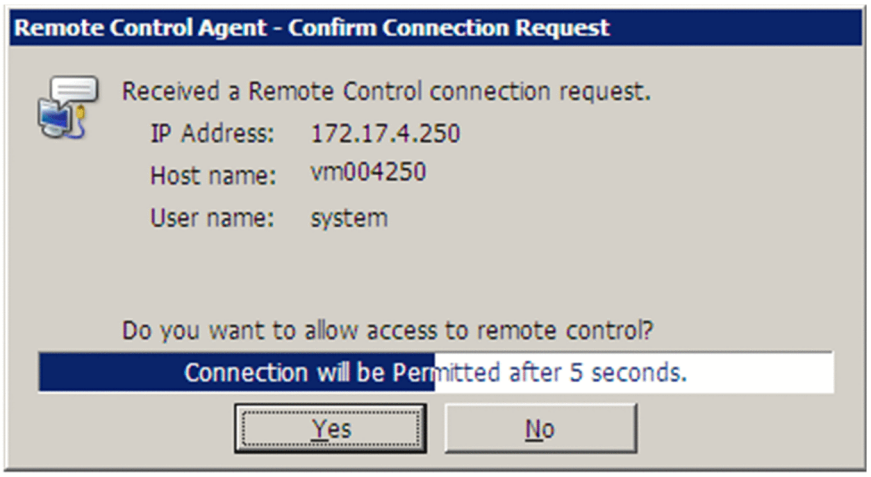
Important note

If you did not allow the user to stop the remote control agent when specifying agent configuration, the user cannot manually stop the remote control agent. In this case, the **Exit** menu becomes inactive.

7.9.3 Approving or rejecting a connection request from the controller

You can approve or reject a connection request from the controller. To reply to a connection request from the controller, you need to select **User permission is required to start remote control session.** during agent setup. For example, after this item is selected, you can reject the connection request from the controller when you are editing a document that contains personal information, thus allowing you to maintain security.

When the controller issues a connection request, the **Confirm Connection Request** dialog box appears on the agent.



Select whether to approve or reject a connection in this dialog box. If you do not reply to this dialog box, the connection is automatically approved or rejected depending on the agent setup. Note that if the agent is not logged on, the controller is unconditionally connected.

7.9.4 Changing the connection mode on the computer end

When you are using the control mode to perform remote control, the keyboard and mouse on the computer end cannot be used. If you need to use the keyboard or mouse on the computer end, you can forcibly release control mode, and change it to standard mode.

To forcibly release control mode:

1. Simultaneously press the **Ctrl**, **Alt**, and **Delete** keys.

The computer is now in standard mode, and you can operate from the computer end.

When the connection mode of the computer is changed from control mode to standard mode, the system notifies the controller of the change of the connection mode. If the controller is in standard mode, then nothing happens. However, if the controller is in control mode, a dialog box appears to make sure that you really want to change the connection mode of the controller from control mode to standard mode. If you reply in this dialog box to allow the controller to be changed to standard mode, the controller is also changed to standard mode, and you can operate the computer from both the controller and the computer. However, if you do not allow the controller to be changed to standard mode, then the computer remains in control mode, and you cannot operate it from the computer end.

7.9.5 Disconnecting from remotely controlled computers

You can disconnect a controller from the computer end, if an agent is installed on the remote computer.

Tip

Depending on the agent configuration, the remote control agent can be automatically stopped when the last controller is disconnected from.

To disconnect the controllers one-by-one:

1. Right-click the **Remote Control Agent** icon, and then select the **Disconnect** menu.
2. Select the controller that you want to disconnect.

The selected controller is disconnected.

When the status window is displayed, use the **Disconnect Controller** button () instead of the menu.

To disconnect controllers simultaneously:

1. Right-click the **Remote Control Agent** icon, and then select the **Disconnect All** menu.

All connected controllers are disconnected from.

When the status window is displayed, use the **Disconnect All Controllers** button () instead of the menu.

Related Topics:

- 7.9.1 Displaying the status window of the remote control agent

7.9.6 Issuing a connection request to the controller

Use the Requester wizard to issue a connection request from a computer to the controller.

Important note

The Requester wizard can only be used on online-managed computers.

Important note

To start remote control by issuing a connection request to the controller, the request server on the controller end must be started. For details about how to start a request server, see 7.7.12 Starting or stopping a request server.

Tip

In the Requester wizard, you can export the wizard settings to a file. If you want to simultaneously issue a connection request from multiple computers to the same controller, you can easily do so by importing the exported setup file to each computer.

To issue a connection request to the controller:

1. Start the Requester wizard.
   From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Remote Control Agent**, and then **Requester Wizard**.
   The Requester wizard starts.

2. Specify the controller that you want to connect to, and then click the **Next** button.

   Tip

   If you have already exported the settings for the Requester wizard, you can specify the wizard settings in a batch operation by clicking the **Import** button to import the setup information.

3. Specify the action according to the controller's reply, and then click the **Next** button.

4. Specify the message to be displayed on the controller end when requesting a connection, and then click the **Next** button.

5. Select the action to take after the wizard is complete, and then click the **Complete** button.

   Tip

   When you click the **Export** button, the settings for the wizard are exported to a file.

A connection request is issued according to the settings. Remote control starts when the connection request is approved on the controller end.

When a computer issues a connection request to the controller, an icon () is displayed on the task bar of the computer. The connection request is effective as long as this icon is displayed.

Tip

You can specify two types of authentication information for the agent: address authentication (approval controller) and user authentication (user ID and password). However, only user authentication can be used when a computer is connected based on a connection request from the controller.

7.9.7 Canceling connection requests

When a computer issues a connection request to the controller, an icon () is displayed on the task bar of the computer. The connection request is effective as long as this icon is displayed.

You can use this icon to cancel connection requests. By using this icon, you cannot only cancel all connection requests, but also specific connection requests only.

To cancel a connection request:

1. Right-click the icon.

2. From the displayed menu, select **Disconnect** and then either the controller you want to disconnect or **Disconnect All**.

The connection request is canceled. If all of the connection requests are canceled, the icon disappears from the task bar.

Note that the connection request is automatically canceled when either of the following is performed:

- The agent is stopped.
- The computer is logged off from.

You can also cancel connection requests from the controller end. If a connect request is canceled from the controller, a message informing you that the connection request has been canceled is displayed on the computer.

7.10 Using the chat function

7.10.1 Setting the operating environment for the chat server

You can specify the port number or password for connecting to the chat server.

To set the operating environment for the chat server:

1. Start the chat server, and then display the **Chat Server** icon ( ).
2. Right-click the **Chat Server** icon, and then select **Options** from the displayed menu.
3. In the displayed dialog box, set the operating environment, and then click **OK**.

The dialog box is closed, and the settings are applied.

Related Topics:

- 7.10.3 Starting the chat server
- 7.10.4 Chat server functional differences due to the starting method used by the agent

7.10.2 Setting the operating environment for the Chat window

You can set the user information to be displayed during a chat session, availability of notifications, or the window display format.

Tip

Some items cannot be set when the chat server is connected to. Therefore, set the operating environment when the chat server is not connected to.

To set the operating environment for the Chat window:

1. From the menu of the **Chat** window, select **Tools** and then **Options**.
2. In the displayed dialog box, set the operating environment, and then click **OK**.

The dialog box is closed, and the settings are applied.

7.10.3 Starting the chat server

If you start the chat server, you can use the **Chat** window to start chatting. When the chat server is running, the **Chat Server** icon ( ) is displayed on the task bar. You can send or receive messages in the **Chat** window in the same way as operating as a client.

You can start the chat server either automatically or manually. You can make the chat server a resident process by setting the chat server to be automatically started. You can select how to best use the chat server according to the situation in

which the chat function is used. For example, you can set the chat server to be automatically started when the chat function is used for the help desk.

To automatically start the chat server:

For a controller, add the chat server to Windows Startup. For a computer that has the agent installed, set the chat server to be automatically started when the agent starts, or add the chat server to Windows Startup.

To add the chat server to Windows Startup:

1. Open the **Chat** window.

   Tip

   To open the **Chat** window, perform one of the following:

   - From the menu of the **Remote Controller** window, select **Tools** and then **Chat**.
   - For a controller: From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Manager**, **Tools**, and then **Remote Control - Chat**.
   - For a computer that has the agent installed: From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Remote Control Agent**, and then **Chat**.

2. From the menu, select **Tools**, **Chat Server**, and then **Start When Windows Starts**.

The **Chat Server** shortcut is created in the user's **Startup** group. The chat server automatically starts from the next time the user logs on.

To automatically start the chat server when the agent starts:

To automatically start the chat server when the agent starts, select **Start the chat server when remote control agent starts.** in **Remote Control Settings** during agent setup.

To manually start the chat server:

1. Open the **chat** window.

   Tip

   To open the **Chat** window, perform one of the following:

   - From the menu of the **Remote Controller** window, select **Tools** and then **Chat**.
   - For a controller: From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Manager**, **Tools**, and then **Remote Control - Chat**.
   - For a computer that has the agent installed: From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Remote Control Agent**, and then **Chat**.

2. From the menu, select **Tools**, **Chat Server**, and then **Start Chat Server**.

The chat server starts, and the **Chat Server** icon is displayed on the task bar.

Tip

From the **Tools** menu of the **Chat** window, if you select **Chat Server** and then **Hide When Minimized**, you can hide the task bar when the chat server is minimized. The **Chat Server** icon is displayed even when the task

bar is hidden, so you can redisplay the task bar by double-clicking the **Chat Server** icon. In addition, when a connection is made from another **Chat** window, the chat server pops up automatically.

Related Topics:

- 7.10.11 Using the **Chat Server** icon

7.10.4 Chat server functional differences due to the starting method used by the agent

When a chat server is started automatically by the agent, the functions of the chat server are different from when it is manually started. The differences are described below:

- The following menus of the **Chat** window cannot be used (because they are inactive):
  - The **Connect** menu in the **File** menu
  - The **Disconnect** menu in the **File** menu
  - The **Chat Server** menu in the **File** menu
- The items on the **User** tab of the **Options** dialog box can always be changed.
- The **Chat** window is closed and the task bar is hidden if you perform the operations below in the **Chat** window. Note that the **Chat** window can be redisplayed by double-clicking the **Chat Server** icon or when a message is received.
  - Selecting **File** and then **Exit** from the menu
  - Clicking the **x** button on the title bar
  - Displaying the Chat window icon

7.10.5 Starting a chat session

You can start a chat session when the **Chat** window is connected to a chat server. You can use the following two methods to start a chat session:

- Connect to another chat server from the **Chat** window.
- Start the chat server, and then wait for the connection from another **Chat** window.

The following explains how to start a chat session by connecting to another chat server from a **Chat** window. For details about how to start the chat server, see 7.10.3 Starting the chat server.

To start a chat session by connecting to a chat server:

1. Start the **Chat** window.

Tip

To start the **Chat** window:

- From the menu of the **Remote Controller** window, select **Tools** and then **Chat**.

- For a controller: From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Manager**, **Tools**, and then **Remote Control - Chat**.
- For a computer that has the agent installed: From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Remote Control Agent**, and then **Chat**.

2. From the menu of the **Chat** window, select **File** and then **Connect**.
3. In the displayed dialog box, specify the address of the chat server you want to connect to, and then click **OK**.

Tip

If a password has been specified for the chat server you want to connect to, the **Enter Password** dialog box is displayed. In this case, enter the password, and then click **OK**. Note that the connection fails if an incorrect password is entered three times in a row. If this happens, connect to the chat server from the **Chat** window again.

A message is displayed informing you that the specified chat server has been connected to.

Tip

When a computer is connected to a chat server, this computer can connect to one or more other chat servers from the **Chat** window. However, when a chat server is running on a computer, the computer cannot connect to other chat servers. In this case, stop the chat server, and then connect the computer to another chat server.

7.10.6 Sending chat messages

You can chat with other connected users via messages. Messages sent by other users are automatically displayed.

To send a chat message:

1. In the message input box in the **Chat** window, enter the message.
2. Click the **Send** button ().

The message is sent.

Tip

To send messages to specific users only, specify the recipients of the message in **User List box**. Messages are sent to the selected users only. The default is that all users are selected.

7.10.7 Ending a chat session

How to end a chat session depends on whether the chat server is running on the computer, or the chat server is connected to the computer. The details are described below.

When the chat server is running on the computer

- Close the **Chat** window.
- Stop the chat server.

When the chat server is connected to the computer

- Close the **Chat** window.
- Stop the connection to the chat server.

The following describes how to do the above in detail.

To close the Chat window:

1. From the menu of the **Chat** window, select **File** and then **Exit**.

The Chat window is closed. A message appears in the following situations:

- When the chat information is not saved, a message is displayed to check whether you want to save the information. For details abotu how to save a chat session, see 7.10.8 Saving chat information.
- When the chat server is running, a message is displayed to check whether you want to stop the chat server.

To stop the chat server:

1. From the menu of the **Chat** window, select **Tools** and then **Chat Server**, and then remove the selection of **Start Chat Server**.

The chat server is stopped, and the **Chat** window becomes inactive.

To disconnect from the chat server:

1. On the toolbar of the **Chat** window, click the **Disconnection** button ().

   When more than one chat server is connected to, a dialog box is displayed for selecting the chat server to disconnect from.

2. Select the chat server that you want to disconnect from, and then click **OK**.

The selected chat server is disconnected from. If the chat server is disconnected from normally, a message informing you that the chat server has been disconnected from is displayed in the **Chat** window.

7.10.8 Saving chat information

You can save chat information in a file. The chat logs can also be saved.

To save chat information:

1. On the toolbar of the **Chat** window, click the **Save As** button ().

2. In the displayed dialog box, specify the storage location and file name, and then click the **Save** button.

The chat information is saved with the specified name.

Tip

To save the chat information into another file, select **File** from the menu of the **Chat** window and then **Save As**.

When saving the file, you can specify the file type. You can select the file type from the following file formats:

- Text file (*.txt)
  Saves all information displayed in the chat view.
- Rich text format file (*.rtf)
  Saves all information and styles (character fonts and colors) displayed in the chat view.
- All files (*.*)
  Saves all information displayed in the chat view. In this case, you can specify any file extension.

7.10.9 Printing chat information

You can print the information displayed in the **Chat** window.

To print chat information:

1. On the toolbar of the **Chat** window, click the **Print** button ( ).
2. In the displayed dialog box, specify the items such as the printer and number of copies, and then click **OK**.

The displayed chat information is printed.

7.10.10 Starting remote control from the Chat window

When the controller is installed on the computer, you can start the controller from the **Chat** window. If you received a chat message, you can directly start remote control when you need to connect the user.

To start remote control from the Chat window:

1. From **User List Box** of the **Chat** window, select the user that you want to connect.
2. From the menu, select **Tools** and then **Remote Control**.

The controller starts, and the computer of the selected user is connected.

7.10.11 Using the Chat Server icon

When the chat server is running, the **Chat Server** icon ( ) is displayed on the task bar. You can use this icon to perform chat-related operations.

To view the connected users:

1. On the task bar, right-click the **Chat Server** icon, and then select **Users**.

The names of the users currently connected are displayed in the format *nickname@host-name*.

To disconnect a chat user:

1. On the task bar, right-click the **Chat Server** icon, and then select **Disconnect**.
2. Select the user that you want to disconnect, and then click **OK**.

> **Tip**
>
> You can also select multiple users to disconnect them simultaneously.

The selected user is disconnected. In the **Chat** window of the disconnected user, a message is displayed informing them that the server has been disconnected.

To specify options:

1. On the task bar, right-click the **Chat Server** icon, and then select **Options**.
2. In the displayed dialog box, specify the options for the chat server, and then click **OK**.

The dialog box is closed, and the settings are saved.

8

Managing Network Connections of Devices

This chapter explains how to connect devices to or disconnect devices from the network within the organization.

8.1 Enabling the network monitor

If you enable the network monitor for a computer that is managed online, you can automate the discovery of network-connected devices or manage the network connections of devices in the network segment to which the computer belongs.

To enable the network monitor:

1. Display the Device module.
2. In **Device Inventory** in the menu area, select the desired network segment from **Network List**.
3. In the information area, select a computer on which the agent has been installed.
4. In **Action**, select **Enable Network Access Control**.

The network monitor of the selected computer is enabled. The network of the selected network segment is monitored.

For computers for which the network monitor is enabled,  or  is displayed as the management type. In addition,  is displayed in the group in the menu area.

Important note

Do not uninstall the network monitor agent from a computer for which the network monitor is enabled. Uninstalling the network monitor agent disables the network monitor for the network segment to which the computer belongs.

Important note

If the menu area displays the operation status of the network monitor as **Managing** or **Starting management**, the following restrictions apply:

- The group of the applicable network cannot be deleted.
- Computers for which the network monitor is enabled cannot be excluded or deleted.

Important note

When enabling the network monitor for a computer running Windows Server 2003, make sure that WinPcap is not installed. If WinPcap is installed, uninstall WinPcap before enabling the network monitor.

Important note

A component (a network monitor agent) must be registered on the management server to enable the network monitor.

Tip

You can also enable the network monitor by selecting **Network Access Control** and then **Assign Network Access Control Settings** in the Settings module, and then using the **Assign Network Access Control Settings** view.

Tip

You can also enable the network monitor by using the provided media to install JP1/IT Desktop Management - Network Monitor on the computer on which the agent is installed.

Tip

If a computer for which the network monitor is enabled belongs to multiple network segments, the network monitor is enabled on all of the network segments.

8.2 Disabling the network monitor

Disable the network monitor if the network monitoring of a specific network segment is not needed or if you want to stop monitoring a network.

To disable the network monitor:

1. Display the Device module.
2. In **Device Inventory** in the menu area, select the desired network segment group from **Network List**.
3. In the information area, select a computer for which the network monitor is enabled.
   The management type of the computer for which the network monitor is enabled is displayed as  or  .
4. In **Action**, select **Disable Network Access Control**.

The network monitor for the selected computer is disabled, and the network is no longer monitored.

Tip

Disabling the network monitor uninstalls the network monitor agent from the computer.

If the network monitor is disabled, the management type changes back to  or  .

The network monitor cannot be disabled if the operation status of the network monitor displayed in the menu area is **Stopped management**.

Important note

If the operation status of a computer on which the network monitor agent is installed is **Stopped management** or **Failed to stop management**, the computer cannot be excluded.

Important note

A component (a network monitor agent) must be registered on the management server to disable the network monitor.

Tip

You can also disable the network monitor by selecting **Network Access Control** and then **Assign Network Access Control Settings** in the Settings module, and then using the **Assign Network Access Control Settings** view.

Tip

If a computer for which the network monitor is disabled belongs to multiple network segments, the network monitor is disabled on all of the network segments.

Tip

If a computer has the network monitor agent installed and cannot connect to the management server, you can disable the network monitor by selecting and deleting **JP1/IT Desktop Management - Network Monitor** from **Programs and Features** in the Windows Control Panel on the computer. If you want to disable the network monitor in this way, you must follow the instructions in the operations window for disabling it, and then change the information on the management server (that is, the management type of the target computer).

Related Topics:

- 8.1 Enabling the network monitor

8.3 Allowing network connections

You can manually allow a computer to connect to a network if the computer has been verified as secure or quarantined.

You can only allow network connections from computers in network segments for which network monitor is enabled.

To allow a network connection:

1. Display the Device module.
2. In the menu area, select **Device Inventory** and then **Network List**. In the **Network List** view, select the network segment containing the computer that you want to allow to connect to the network.
3. In the information area, select the computer that you want to allow to connect to the network. Select **Action** and then **Deny Network Access**.
4. In the displayed dialog box, click **OK**.

The selected computer is allowed to connect to the network.

If you select **Add Notes**, you can keep track of information on when and why network connections are allowed. Information entered here is added to the **Notes** tab.

> **Tip**
>
> You can allow a network connection by selecting **Computer Security Status** and then **Network List** in the Security module, and then using the **Network List** view. You can also allow a network connection by selecting **Network Access Control** and then **Network Filter Settings** in the Settings module, and then using the **Network Filter Settings** view.

Related Topics:

- 8.4 Blocking network connections

8.4 Blocking network connections

You can manually block network connections for cases in which someone brings in a computer from outside or if security measures are not fully implemented on a computer.

You can only block network connections of computers in network segments for which the network monitor is enabled.

To block a network connection:

1. Display the Device module.
2. In the menu area, select **Device Inventory** and then **Network List**. In the **Network List** view, select the network segment containing the computer that you want to block.
3. In the information area, select the computer that you want to block from the network. Select **Action** and then **Deny Network Access**.
4. In the displayed dialog box, select **Continue Operation**, and then click **OK**.

The selected computer is blocked from the network. The **Connection to Network** setting of the network control list changes to **Deny**.

If you select **Send User Notification**, you can send a message to the user of the selected computer. If you select more than one computer, you can send the same message to the users of those computers.

If you select **Add Notes** for a selected computer, you can keep track of information on when and why its network connection is blocked. Information entered here will be added to the **Notes** tab.

Important note

If a network connection is manually blocked, the network connection is automatically disallowed.

Important note

Network connections are not blocked from computers in network segments for which the network monitor is disabled, even if **Connection to Network** is **Deny**.

Tip

You can allow a network connection by selecting **Computer Security Status** and then **Network List** in the Security module, and then using the **Network List** view. You can also allow a network connection by selecting **Network Access Control** and then **Network Filter Settings** in the Settings module, and then using the **Network Filter Settings** view.

Tip

When a network connection is blocked, a message might be displayed to indicate that an IP address conflict has occurred for the device.

Related Topics:

- 8.3 Allowing network connections

8.5 Reconnecting a device that was automatically blocked from the network

If a device is automatically blocked from the network because of the network policy or the expiration of the network control list, the device can be reconnected to the network.

Devices can be automatically blocked from the network on the following occasions:

- An attempt is made to connect devices to networks where connection is not allowed.
- A security policy violation occurs.
- It is outside the period permitted by the network control list.
- The network control list has been deleted.

The following methods can be used to reconnect devices blocked from the network:

Allow network connections by setting devices to be managed or excluded.

If the network monitor does not allow newly discovered devices to connect to the network, the discovered devices are not allowed to connect to the network but are registered in the network control list and blocked from the network automatically. If you check the discovered devices and set the devices to be managed or excluded, the devices are recognized as devices within the organization, and the network control list setting automatically changes to allow network connections. This allows the devices to connect to the network.

Implement security measures to make sure that network connections are automatically allowed.

If you specify security policy settings by selecting **Action Items** and then **Network Connection Control**, network connections are automatically blocked depending on the judgment. In this case you should implement security measures. The next time a judgment is made, devices can be connected to the network if they comply with the security policy.

Change the period in the network control list during which to allow network connections.

If a network connection period is defined in the network control list, network connections are automatically blocked outside that period. If devices need to connect to the network, change the period to allow network connections.

Outside the period, the icon  is displayed to indicate that a device is unavailable.

Reregister the network control list to allow network connections.

If you delete a device or hardware resource, the corresponding network control list is automatically deleted. If you then attempt to reconnect a device to the network, the network connections will be blocked automatically if the network monitor is configured to disallow network connections of new devices. In this case, change the network control list setting of the discovered devices to allow network connections, so that the devices can connect to the network.

If an agent is installed on a computer and you have specified security policy settings by selecting **Action Items** and then **Network Connection Control**, the network connections of that computer are controlled after reconnection according to a security judgment. To allow devices to reconnect automatically, make sure that they comply with the security policy.

Tip

In addition to the reconnection methods above, devices can also be manually reconnected.

You can forcibly allow blocked devices to connect to the network. For details on how to allow network connections manually, see 8.3 Allowing network connections.

8.6 Managing network monitor settings

8.6.1 Adding network monitor settings

You can add network monitor settings to the list in the **Network Access Control Settings** view of the Settings module. If you add network monitor settings, you can specify whether to allow newly discovered devices in each network segment to connect to the network.

To add network monitor settings:

1. Display the Settings module.
2. In the menu area, select **Network Access Control** and then **Network Access Control Settings**.
3. In **Network Access Control Settings** in the information area, click **Add**.
4. In the displayed dialog box, specify a name for the network monitor settings, set a behavior for the discovered device, and then click **OK**.

The network monitor settings are added and displayed in the **Network Access Control Settings** list.

Adding network monitor settings is not enough to control a network. You also need to assign the network monitor settings.

8.6.2 Editing network monitor settings

You can edit network monitor settings in the list in the **Network Access Control Settings** view of the Settings module.

To edit network monitor settings:

1. Display the Settings module.
2. In the menu area, select **Network Controls** and then **Setting Network Controls**.
3. In the information area, click the **Edit** button for the network monitor settings that you want to edit.
4. In the displayed dialog box, edit the necessary information, and then click **OK**.

The selected network monitor settings are updated.

8.6.3 Removing network monitor settings

You can remove network monitor settings from the list in the **Network Access Control Settings** view of the Settings module.

> **Tip**
>
> You cannot remove network monitor settings assigned to network segments. Release the assignment of network monitor settings before removing them.

To remove a network monitor setting:

1. Display the Settings module.
2. In the menu area, select **Network Controls** and then **Setting Network Controls**.
3. In the information area, select the network monitor setting that you want to remove, and then click **Remove**.
4. In the displayed dialog box, click **OK**.

The selected network monitor setting is removed from the list of network monitor settings.

8.6.4 Assigning network monitor settings

You can assign network monitor settings to each network segment, and manage network connections of newly discovered devices in each network segment.

> **Tip**
>
> To assign network monitor settings, the network monitor function must be installed on the network segment.

To assign network monitor settings:

1. Display the Settings module.
2. In the menu area, select **Network Access Control** and then **Assign Network Access Control Settings**.
3. In the upper part of the information area, select the network segment where the network monitor settings are to be assigned. Next, in the lower part of the information area, select the computer for which the network monitor is to be enabled. Finally, click **Enable Network Access Control**.
4. In the displayed dialog box, select the network monitor settings to be assigned, and then click **OK**.

The network monitor settings are assigned to the network segment, and displayed in the list of assigned network monitor settings.

8.6.5 Changing assignment of network monitor settings

You can change the assignment of network monitor settings to network segments in the **Assign Network Access Control Settings** view of the Settings module.

> **Tip**
>
> You cannot change the assignment of network monitor settings if the network monitor is disabled. Enable the network monitor before changing the assignment of network monitor settings.

To change the assignment of network monitor settings:

1. Display the Settings module.

2. In the menu area, select **Network Access Control** and then **Assign Network Access Control Settings**.

3. In the upper part of the information area, select the network segment for which the assignment of network monitor settings is to be changed. Then, click **Change Assigned Setting**.

4. In the displayed dialog box, select the network monitor settings to be assigned, and then click **OK**.

The assignment of network monitor settings to the selected network segment is changed.

8.7 Managing the network control list

8.7.1 Adding devices to the network control list

You can add devices to the network control list in the **Network Filter Settings** view of the Settings module. If you add devices to the network control list, you can allow or block the network connections of the devices. You can also specify the network connection period.

To add devices to the network control list:

1. Display the Settings module.
2. In the menu area, select **Network Access Control** and then **Network Filter Settings**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, specify whether to allow network connections, and then click **OK**.

Devices are added to the network control list.

Related Topics:

- 8.7.2 Editing devices in the network control list
- 8.7.3 Removing devices from the network control list
- 6.9 Removing a device

8.7.2 Editing devices in the network control list

You can edit device settings in the network control list in the **Network Filter Settings** view of the Settings module.

To edit a device in the network control list:

1. Display the Settings module.
2. Select **Network Access Control** and then **Network Filter Settings** in the menu area.
3. In the information area, click the **Edit** button for the device that you want to edit.
4. In the displayed dialog box, edit the necessary information, and then click **OK**.

The network control settings of the selected device are updated.

8.7.3 Removing devices from the network control list

You can remove devices that were registered manually from the network control list in the **Network Filter Settings** view of the Settings module.

To remove a device from the network control list:

1. Display the Settings module.

2. In the menu area, select **Network Access Control** and then **Network Filter Settings**.
3. In the information area, select the device that you want to remove, and then click **Remove**.
4. In the displayed dialog box, click **OK**.

The selected device is removed from the network control list.

> **Important note**
>
> You can remove information from the network control list if the information was added manually. From the Settings module of the network control list, you cannot remove devices that were detected by the network monitor or information that was added automatically through means such as a network search. To remove automatically added information from the network control list, remove the device information. To determine whether information was added automatically, check the network control list to see if the information is displayed in **Host Name**.

Related Topics:

- 8.7.1 Adding devices to the network control list
- 8.7.2 Editing devices in the network control list

8.7.4 Editing the automatic update of the network filter list

In the **Network Filter Settings** view of the Settings module, you can edit the automatic update of the network filter list.

To edit the automatic update of the network filter list:

1. Display the Settings module.
2. In the menu area, select **Network Access Control** and then **Network Filter Settings**.
3. In the information area, click the **Edit** button for **Automatic Updates on Network Filter List**.
4. In the dialog box that appears, specify the automatic update of the network filter list.
5. Click **OK**.

The automatic update of the network filter list are changed.

8.8 Managing special connections

8.8.1 Adding special connection settings

You can add special connection settings to **Exclusive Communication Destination for Access-Denied Devices** in the **Network Access Control Settings** view of the Settings module. This enables blocked devices to connect to the network only for special types of communication.

To add special connection settings:

1. Display the Settings module.
2. In the menu area, select **Network Controls** and then **Setting Network Controls**.
3. In **Exclusive Communication Destination for Access-Denied Devices** in the information area, click **Add**.
4. In the displayed dialog box, enter the special connection settings, and then click **OK**.

The special connection settings are added to the list of **Exclusive Communication Destination for Access-Denied Devices**.

Related Topics:

- 8.8.2 Editing special connection settings
- 8.8.3 Removing special connection settings

8.8.2 Editing special connection settings

You can edit special connection settings in **Exclusive Communication Destination for Access-Denied Devices** in the **Network Access Control Settings** view of the Settings module.

To edit special connection settings:

1. Display the Settings module.
2. In the menu area, select **Network Controls** and then **Setting Network Controls**.
3. In the information area, click the **Edit** button for the special connection settings that you want to edit.
4. In the displayed dialog box, edit the necessary information, and then click **OK**.

The selected special connection settings are updated.

Related Topics:

- 8.8.1 Adding special connection settings
- 8.8.3 Removing special connection settings

8.8.3 Removing special connection settings

You can remove special connection settings in **Exclusive Communication Destination for Access-Denied Devices** in the **Network Access Control Settings** view of the Settings module.

To remove special connection settings:

1. Display the Settings module.
2. In the menu area, select **Network Controls** and then **Setting Network Controls**.
3. In the information area, click the **Remove** button for the special connection settings that you want to remove.
4. In the displayed dialog box, click **OK**.

The selected special connection settings are removed from the list of **Exclusive Communication Destination for Access-Denied Devices**.

Related Topics:

- 8.8.1 Adding special connection settings
- 8.8.2 Editing special connection settings

8.9 Enabling the JP1/NETM/NM - Manager linkage settings

If JP1/NETM/NM - Manager linkage is enabled, you can use JP1/IT Desktop Management to control network connections to the network segments that are managed by JP1/NETM/NM - Manager.

To enable the JP1/NETM/NM - Manager linkage settings:

1. Display the Settings module.
2. In the menu area, select **Network Access Control** and then **Network Access Control Settings**.
3. In the information area, in **JP1/NETM/NM - Manager Link Settings**, click **Edit**.
4. In the dialog box that appears, if **Continue the operation** appears, check the message that appears, and then select **Continue the operation**.
5. Select **Link with JP1/NETM/NM - Manager**.
6. Click **OK**.

The JP1/NETM/NM - Manager linkage settings are enabled.

9

Managing the Security Status

This chapter explains how to conduct security management within an organization and understand the security status.

9.1 Checking the security status

By default, managed computers have the default policy applied. Immediately after JP1/IT Desktop Management is used to specify computers that should be managed, the administrator can view the security status evaluated by the default policy, regardless of whether the administrator has set the security policy settings.

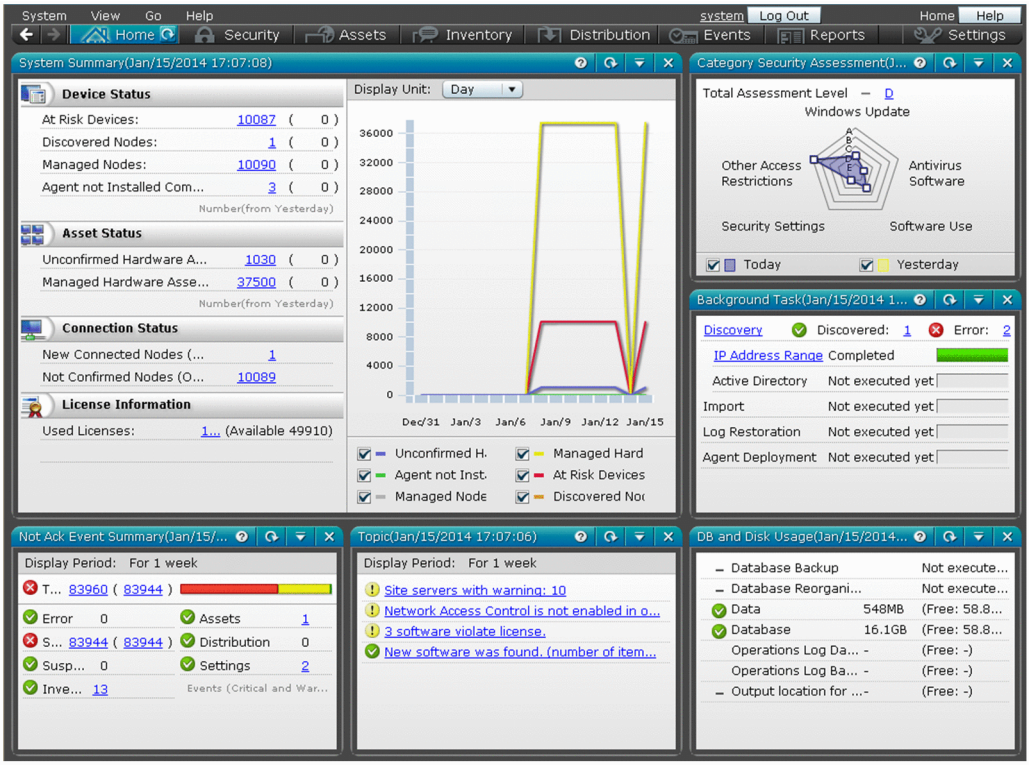
> **Tip**
>
> Immediately after operation starts, it is recommended that you check the security status evaluated based on the default policy and then address any issues. This will maintain a basic level of security. After that, you should set security policies that satisfy your organization's security requirements for security management.

You can check the security status from the Home module panels, the Security module, reports, and the Events module.

Checking the security status in the Home module panels

The number of computers that are not safe is displayed in **At Risk Devices** in the **System Summary** panel of the Home module. If you click the number, you will see the **Computer Security Status** view of the Security module, and then you can check the security status of each computer.

The **Category Security Assessment** panel lets you review a comprehensive security assessment of the computers and shows you the security areas that need to be addressed.

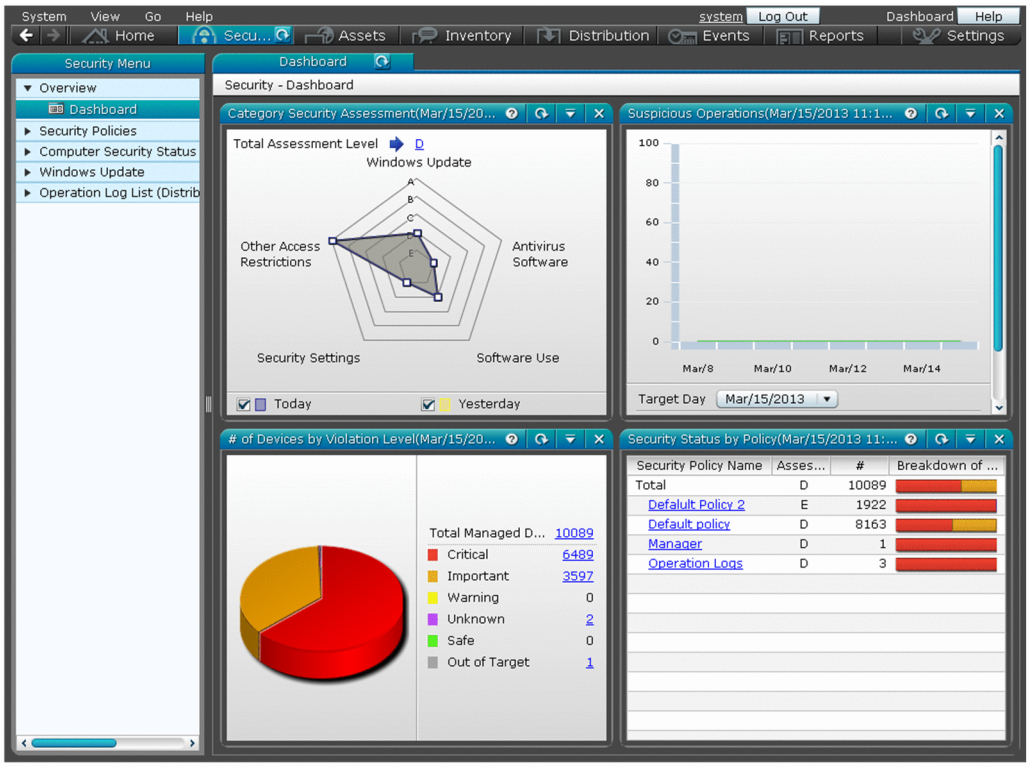


Checking the security status in the Security module

In the Security module, you can check the security status in the **Overview** view, the **Security Policy** view, and the **Computer Security Status** view.

Checking the status in the **Overview** view

You can view the summary of the security status. Clicking the links in the panels displays detailed information, which helps you investigate specific issues.



Checking the status in the **Security Policy** view

You can see the rate of conformance to each of the security policies and the number of computers where security settings are inappropriate.

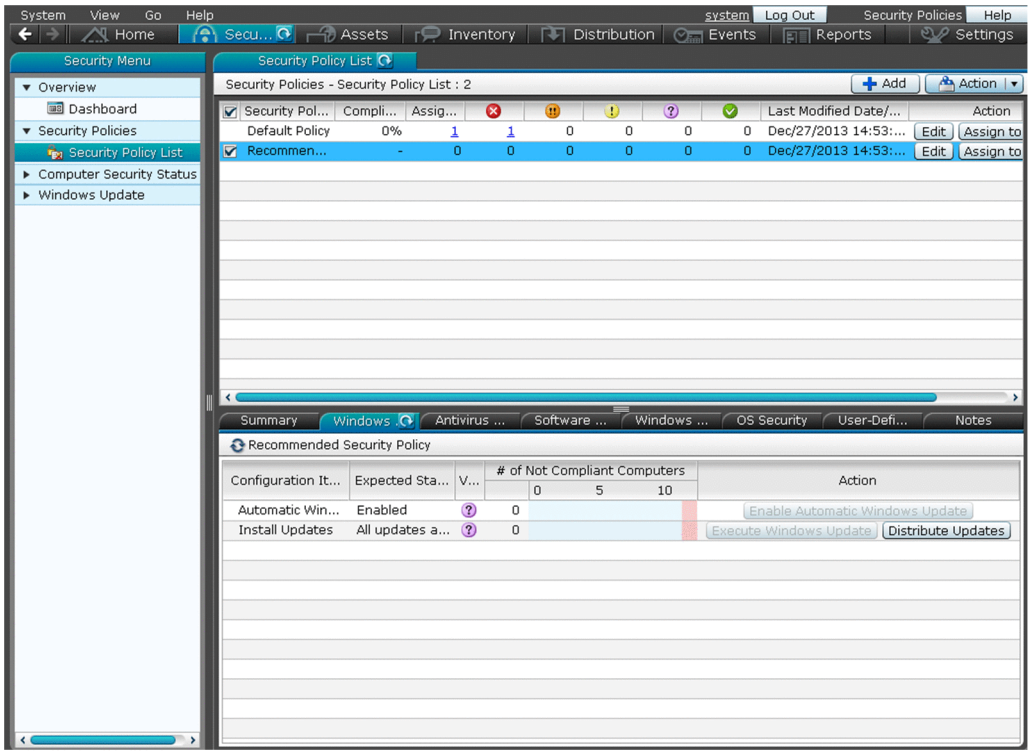
The security policies might not be adhered to if 0 is not displayed for (danger), (warning), and (caution).

Click the number of computers to display the **Computer Security Status** view and check the security status of the computers.

You can use this view to automate the implementation of measures on computers where security policies are applied.

The rate of conformance and number of applied computers are calculated based on the number of computers whose security status has been judged. The rate of conformance is the percentage of the number of computers that comply with the security policies out of the total number of computers whose security status has been judged against the applicable security policies. Applied computers are represented by the number of computers whose security status has been judged against the applicable security policies. However, the rate of conformance and number of applied computers are not calculated in the following situations:

- When all of the judgment items specified in the security policies are addressed to devices that are out of the range of judgment
- When either or both **Prohibited operation** and **Operation log** in the security policies are set to **Enabled**, and all the other security configuration items are set to **Disabled**

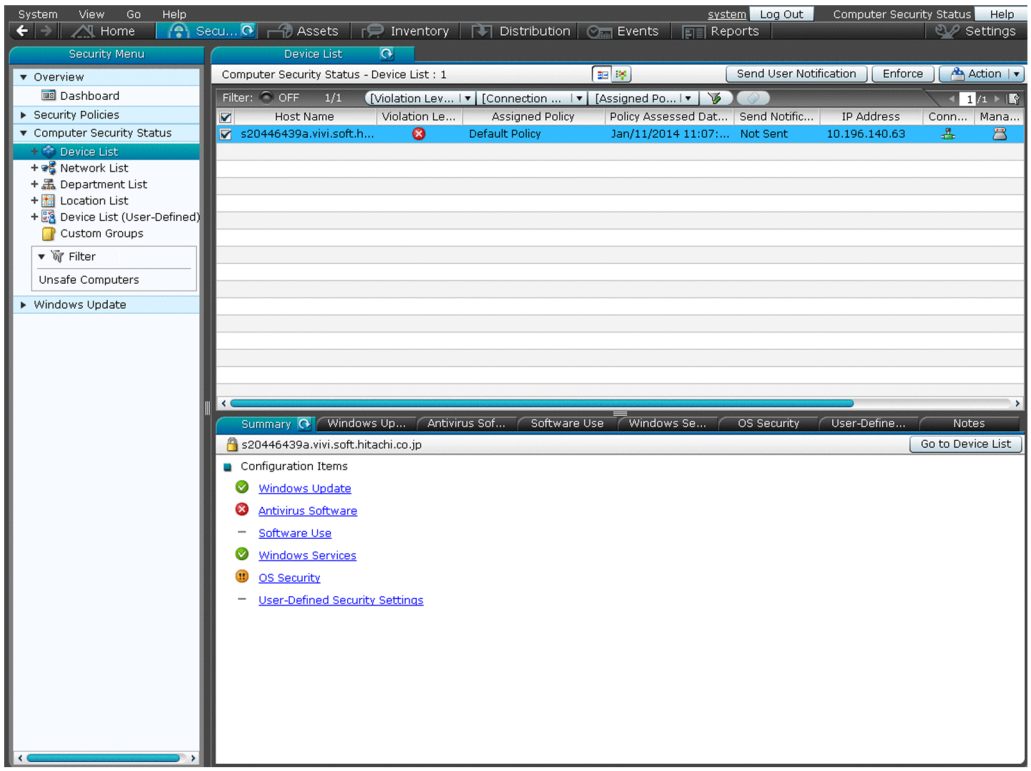


Checking status in the **Computer Security Status** view

You can check the security status of each computer.

You can see a list of the violation levels of all computers, or you can see the violation levels grouped by category. You can directly check the security setting status. You can use this view to automate the implementation of measures of computers where security policies are applied.

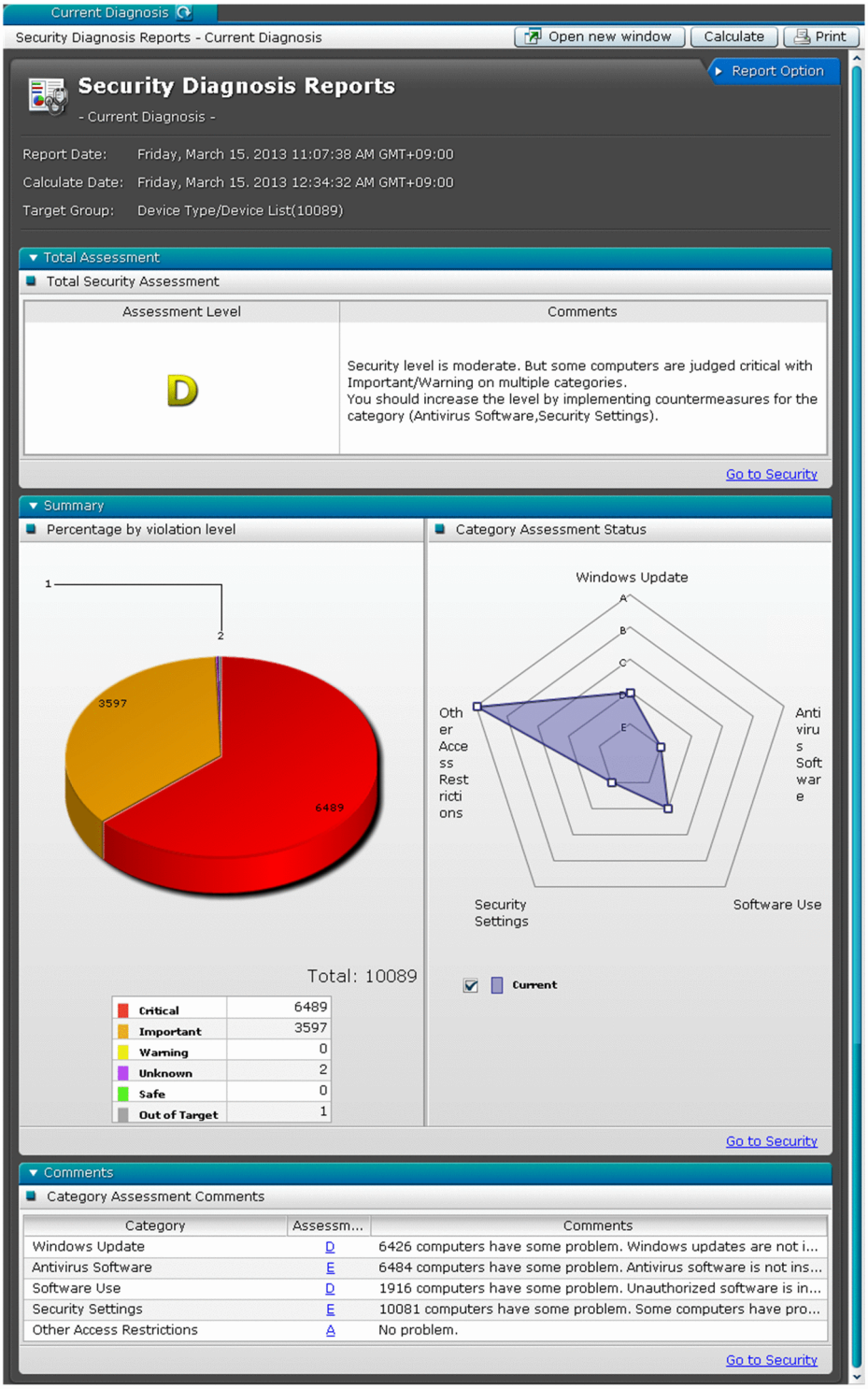
The security policies might not be adhered to if the violation level is displayed as (danger), (warning), or (caution). Review the security status for each security item, and then address any security issues.



Checking the status in a report

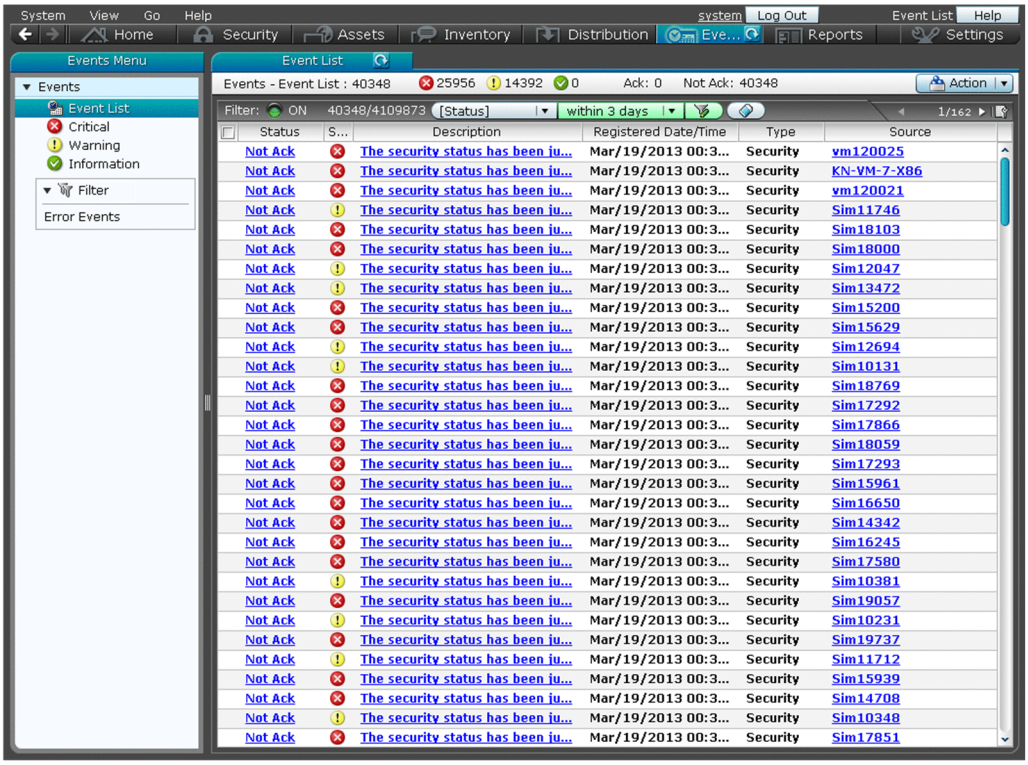
You can check the security status in **Summary Reports**, **Security Diagnosis Reports**, and **Security Detail Reports**.

Summary Reports lets you review security assessment reports. **Security Diagnosis Reports** lets you review the comprehensive security status, such as overall security assessment results and the current status. **Security Detail Reports** displays the details of violation levels and the percentage of each violation level for each security category.



Checking the status in the Events module

You can check security events in the Events module. You can also check minor events that do not violate security policies.



9.2 Specifying users to be excluded from being evaluated

The security status of each user account is evaluated against security items. You can configure settings so that the security status of specific user accounts is excluded from being evaluated.

To specify the users to be excluded from being evaluated:

1. Create a setting file for specifying the users who should not be evaluated.
2. Make sure that the setting file is stored in the following folder.
   - If the system is in a single server configuration: *JP1/IT Desktop Management-installation-folder*\mgr\conf
   - If the system is in a multi-server configuration: *data-folder-shared-among-servers*\mgr\conf

The security status of the user accounts specified in the setting file will not be evaluated as a target.

Related Topics:

- A.5 Format of a user settings file excluded from security status judgment

9.3 Using security policies

9.3.1 Adding security policies

You can add security policies to the list in the **Security Policy** view of the Security module. Assign the added policies to computers or groups. If security policies are assigned, you can manage the security status of the computers or the groups.

To add a security policy:

1. Display the Security module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, configure the security rules settings and then click **OK**.

The security policy is added and displayed in the list of security policies.

Tip

When a security policy is created, the default settings are the same as the default policy.

Related Topics:

- 9.3.2 Editing security policies
- 9.3.3 Copying security policies
- 9.3.4 Removing security policies
- 9.3.5 Assigning security policies
- 9.3.6 Canceling the assignment of security policies

9.3.2 Editing security policies

You can edit security policies if a change occurs with the security policies of your organization or if you want to keep your security policies up to date.

To edit a security policy:

1. Display the Security module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.
3. In the information area, click the **Edit** button for the security policy that you want to edit.
4. In the displayed dialog box, edit the security rules and then click **OK**.

Tip

Clicking the **Restore Default Settings** button in the dialog box restores all the default settings.

The selected security policy is updated.

Related Topics:

- 9.3.1 Adding security policies
- 9.3.3 Copying security policies
- 9.3.4 Removing security policies
- 9.3.5 Assigning security policies
- 9.3.6 Canceling the assignment of security policies

9.3.3 Copying security policies

If you want to create one security policy similar to another policy, you can make a copy of the security policy and then make minor changes to it.

To copy a security policy:

1. Display the Security module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.
3. In the information area, select the security policy that you want to copy. Next, select **Action** and then **Duplicate Policy**.
4. In the displayed dialog box, configure the security rules settings and then click **OK**.

The security policy that you have copied is added to the list.

Related Topics:

- 9.3.1 Adding security policies
- 9.3.2 Editing security policies
- 9.3.5 Assigning security policies

9.3.4 Removing security policies

You can remove unneeded security policies if a change occurs with the security policies of your organization or if the number of managed computers has been reduced.

Tip

You cannot remove security policies assigned to computers or groups. Cancel the assignment of the security policies before removing them. In addition, you cannot remove the default policy.

To remove a security policy:

1. Display the **Security** module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.
3. In the information area, select the security policy that you want to delete. Next, select **Action** and then **Remove Policy**.
4. In the displayed dialog box, click **OK**.

The selected security policy is removed.

Related Topics:

- 9.3.1 Adding security policies
- 9.3.6 Canceling the assignment of security policies

9.3.5 Assigning security policies

You can quickly figure out the security status based on the default policy, because the default policy is automatically applied to managed computers. To manage different computers or different groups by different rules, create and assign new security policies. You can figure out the security status based on the assigned security policies.

To assign a security policy to a computer:

1. Display the Security module.
2. In **Computer Security Status** in the menu area, select the group that contains the computer to assign a security policy to.
3. In the information area, select the computer to assign a security policy to. Next, select **Action** and then **Assign Policy**.
4. In the displayed dialog box, select a security policy and then click **OK**.

The security policy is assigned to the computer.

To assign a security policy to a group:

1. Display the Security module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.
3. In the information area, click the **Assign to Group** button for the security policy that should be assigned to the group.
4. In the displayed dialog box, select the group and then click **OK**.

The security policy is assigned to the group.

> **Tip**
>
> You can also assign security policies to groups when you configure security policy settings.

Related Topics:

- 9.3.1 Adding security policies
- 9.3.6 Canceling the assignment of security policies

9.3.6 Canceling the assignment of security policies

You can cancel the assignment of security policies if a change occurs with security rules in your organization or if a change occurs with the target of security management.

To cancel security policy assignment for a computer:

1. Display the Security module.
2. In **Computer Security Status** in the menu area, select the group containing the computer of which you want to cancel security policy assignment.
3. Select the computer in the information area, and then select **Cancel Policy** in **Action**.

The security policy assignment is canceled. The default policy is applied unless other security policies are assigned indirectly.

To cancel security policy assignment for a group:

1. In the menu area, select **Security Policy** and then **Security Policy List**.
2. In the information area, click the **Assign to Group** button for the security policy that you want to cancel the assignment of.
3. In the displayed dialog box, de-select the group for which you want to cancel the security policy assignment of, and then click **OK**.

The security policy assignment is canceled. The default policy is applied unless other security polices are assigned indirectly.

Related Topics:

- 9.3.5 Assigning security policies
- 9.3.4 Removing security policies

9.3.7 Adding user-defined security settings to a security policy

You can add any computer security-related policies as user-defined security settings to a security policy. After you add user-defined security settings, the status of computer security settings can be determined by using any judgment conditions.

To add user-defined security settings:

1. Display the Security module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.

3. In the information area, click the **Add** button or select the security policy to which you want to add user-defined security settings, and then click the **Edit** button.
4. In the dialog box that appears, select **Security Configuration Items**, and then select **User-Defined Security Settings**.
5. Click the **Enable** button.
6. Click the **Add** button.
7. In the dialog box that appears, specify the user-defined item name, definitions, and violation level, and then click **OK**.
8. Click **OK**.

The user-defined security settings are added to the security policy.

Related Topics:

- 9.3.1 Adding security policies
- 9.3.2 Editing security policies

9.3.8 Controlling the network connections of devices in response to the evaluated security status

You can use action items in security policies to control the network connections of computers in response to the evaluated security status.

The controlling of network connections requires the monitoring of network segments where computers belong. For details about how to monitor network connections, see 8. Managing Network Connections of Devices.

Tip

You can block or allow network connections by selecting **Device Inventory** and then **Device List** in the Device module, selecting a computer in the **Device List** view, and then using **Action**.

To block or allow the network connections of devices in response to the evaluated security status:

Take the following steps to block or allow network connections in response to the evaluated security status:

1. Display the **Security** module.
2. Select **Security Policy** and then **Security Policy List**. In the **Security Policy List** view, click the **Edit** button for the security policy assigned to the computer that messages should be sent to.
3. In the displayed dialog box, select **Action Items** and then **Network Connection Control**.
4. Click **Enabled**.
5. Specify the violation level for blocking network connections and the conditions for rejecting connections, and then click **OK**.

If the evaluated security status exceeds the violation level, computers are blocked from the network. If a computer is blocked from the network, contact the user of the computer and request the user to address the security issues. If the

security status returns to normal and goes below the violation level, the network connection will automatically be allowed again.

9.4 Enforcing the correction of security policy violations

You can forcibly correct security policy violations of computers remotely from the management server. The items that can forcibly be corrected are only the security configuration items that can automatically be corrected.

An agent for online management must be installed on a computer to correct security policy violations on the computer.

To correct security policy violations forcibly:

1. Display the Security module.
2. In **Computer Security Status** of the menu area, select the group containing the computer that is violating security policies and needs to be corrected forcibly.
3. In the information area, select the computer that is violating security policies and needs to be corrected. Next, click the **Enforce** button.

   You can select multiple computers to correct them at once.
4. In the displayed dialog box, check the security correction items and then click **OK**.

Security measures are implemented to return the computer to the normal status.

> **Tip**
>
> You can also enforce corrections by using the tab at the bottom of the information area in the **Security Policy List** view, which is displayed by selecting **Security Policy** and then **Security Policy List**.

9.5 Delivering messages to users

If you want to send messages to computer users, you can create and send them to individual users. In addition, you can automate the delivery of messages in response to the evaluated security status.

Only the computers for online management can deliver messages.

> **Tip**
>
> You can also send messages from the **Device List** view, which is displayed when you select **Device Inventory** and then **Device List** in the Device module. For details, see 6.22 Sending a notification to a user.

To send a message to a user:

1. Display the Security module.
2. In **Computer Security Status** in the menu area, select the group containing the computer to send the message to.
3. In the information area, select the computer to send the message to, and then click **Send User Notification**.
   You can select multiple computers to send the same message to simultaneously.
4. In the displayed dialog box, set the message and click **OK**.
   To keep track of the history of and the reasons for sending messages, check **Add Notes**. The information entered here is added to the **Notes** tab.

Messages are delivered to the computer users.

To automate the delivery of messages:

1. Display the Security module.
2. Select **Security Policy** and then **Security Policy List**. In the **Security Policy List** view, click the **Edit** button for the security policy assigned to the computer to which messages should be delivered.
3. In the displayed dialog box, select **Action Items** and then **Send User Notification**.
4. Set the violation level and the message to be sent, and then click **OK**.

The message will be sent to the computer when the specified violation level is exceeded.

9.6 Suppressing the use of external media

You can suppress writing to or reading from external media by establishing policies regarding prohibited operations.

To suppress the use of external media:

1. Display the Security module.
2. In the menu area, select **Security Policy** and **Security Policy List**.
3. In the information area, select the security policy to edit, and then click **Edit**.
   To add a new security policy, click **Add**.
4. Select **Other Access Restrictions**, which is a security configuration item.
   The suppression of device operations are disabled if the view is disabled. To enable it, click the **Enabled** button in the top-left corner.
5. In **External Device Restriction**, configure the external media settings that should be suppressed.

   Tip

   The external media that can be suppressed depends on the OS of the computer. Select the tab for the OS and then check the external media to be suppressed. If the **Operating System** column is blank after checking, you cannot suppress external media on that particular OS.
6. Click **OK**.

The use of external media is suppressed according to the established policy regarding prohibited operations.

If hardware asset information about specific USB devices is registered, the USB devices will not be suppressed if you check **Allow registered USB device usage**. For details on how to register USB devices, see 9.7 Registering USB devices.

Tip

The timing when the **External Device Restriction** settings take effect differs for each device as follows:

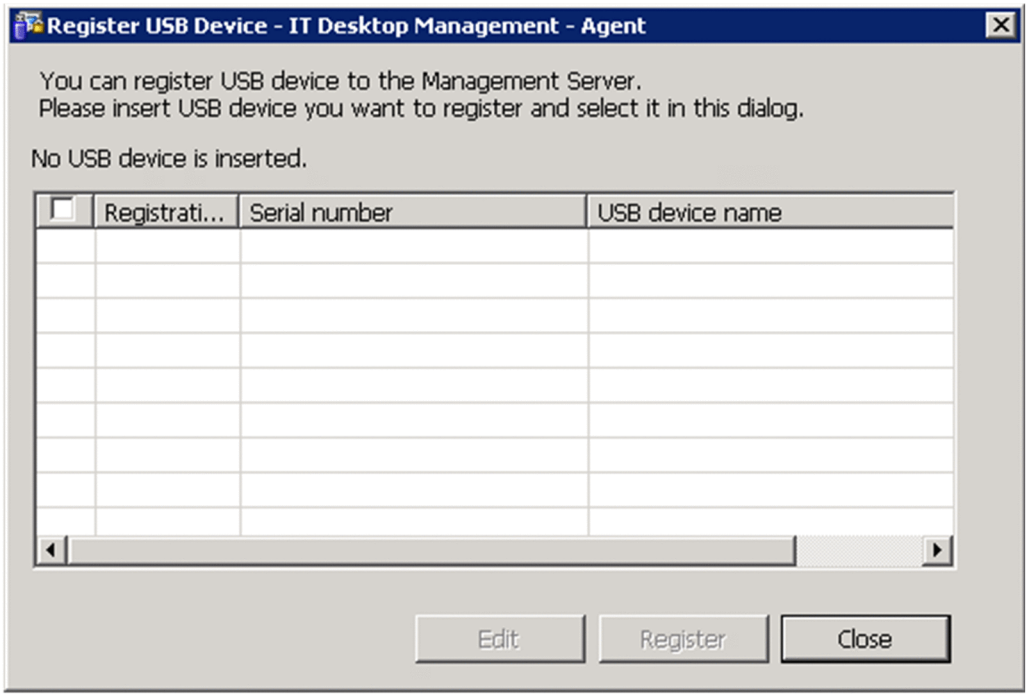
- USB or IEEE 1394 devices:
  The settings take effect when a security policy is applied to the target computer. However, the settings do not take effect on devices already connected to the computer (but the settings will take effect if the devices are reconnected).*
  *: The **Restrict reading/writing** settings on USB devices also take effect on the devices being connected.
- Other devices:
  If you assign a security policy that has **External Device Restriction** items configured, a message appears prompting the user to restart the computer. The settings take effect when the computer is restarted.

9.7 Registering USB devices

You can connect USB devices to a computer where an agent for online management is installed, and then register hardware asset information about the USB devices.

To register USB devices:

1. Log in to a computer where an agent for online management is installed.
2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Agent**, **Administrator Tool**, and then **Register USB Device**.
   The **Register USB Device** dialog box is displayed.



   If password protection is set for the agent at the time of USB device registration, a dialog box appears and prompts you to enter a password. Enter the password that is set for the agent. By default, the JP1/IT Desktop Management password `manager` is set.

3. Connect the USB device to the computer.

> **Important note**
>
> There are two types of USB devices: a device that can be recognized separately, and a device that is recognized by vendors. When connecting the agent to a USB device that is recognized by vendors, a confirmation message is displayed. Registering a USB device that is recognized by vendors enables the device to be treated as the same hardware asset if a different device of the same vendor is registered. For this reason, if you have suppressed the usage of a USB device in the security policy, the USB device is permitted to be used on a per-vendor basis.

4. To register a USB device that is recognized per vendor, select the USB device to be registered in **Recognized USB devices**, and then click the **Edit** button.
   To register a USB device that is recognized separately, go to step 7.
5. In the displayed dialog box, select **Product Unit** and then click **Advanced**.

6. In the displayed dialog box, edit **Registration condition** and then click **OK**.

   In **Registration condition**, specify the fixed part of the device instance ID to be used to identify the USB device. For example, if the device instance ID is `USB\VID_xxxx&PID_003F`, specify `USB\VID_xxxx&PID_00` if `3F` of `PID_003F` changes depending on the environment.

7. In **Recognized USB devices**, select the USB device to be registered, and then click **Register**.

8. In the displayed dialog box, specify whether to confirm the asset status, and then click **OK**.

   If necessary, enter information about the person to be registered for the hardware asset information related to the USB device.

   Information about the selected USB device is collected and registered as an unconfirmed hardware asset.

9. Log in to

   JP1/IT Desktop Management.

10. In the **Hardware Assets** view of the Assets module, change the **Asset Status** of the registered USB device to something other than **Disposed**.

Registration of the USB device is completed.

Important note

When the **Register USB Device** dialog box is displayed on a computer, the suppression of USB devices is temporarily disabled on the computer even if reading from and writing to USB devices are suppressed.

Tip

Device instance IDs of some USB devices with security features after authentication differ from the device instance IDs before authentication. When registering such devices, you must register the device instance IDs both before and after authentication.

Tip

When you connect registered USB devices that are separately recognized to a computer where an agent for online management is installed, information about the files stored in the USB devices is collected. The collected information is displayed in the **File List** tab in the **Hardware Assets** view of the Assets module. Note that the **File List** tab is displayed only when **Device Type** is **USB Device**. No information about the files is collected for USB devices that are recognized separately.

9.8 Managing program updates

9.8.1 Automating the delivery of program updates

You can automate the downloading of program updates and the delivery of the program updates to a managed computer, according to a security policy established by the administrator.

As a security measure, for example, you can establish a security policy to automate the delivery of program updates to computers where updates have not been applied. The program updates are downloaded from Microsoft Japan, and then the program update files are automatically registered. After that, the program update files are automatically delivered to the computers according to the evaluated security status.

To automate the delivery of program updates:

1. Display the Security module.
2. In the menu area, select **Security Policy** and **Security Policy List**.
3. At the top of the information area, click **Add**.
4. In the displayed dialog box, click **Windows Update**.
5. In the displayed dialog box, select **Enable** in **Install Updates**, and then specify **Configuration Item**, **Expected Status**, and **Violation Level**. Next, select **Auto Enforce**, select **Distribute Updates**, and then click **OK**.
6. In **Computer Security Status** in the menu area, select the group containing the program updates that should be automatically distributed.
7. At the top of the information area, select the computer where the program updates should be distributed automatically. Next, select **Action** and then **Assign Policy**.
8. In the displayed dialog box, select the security policy that should be assigned, and then click **OK**.

The program updates are automatically applied to computers where updates have not been applied.

Related Topics:

- 9.8.2 Manually registering and delivering program updates

9.8.2 Manually registering and delivering program updates

In addition to automatically delivering program updates, the administrator can manually register and distribute program updates. For example, the administrator can manually register and distribute important security-related updates immediately without waiting for automatic delivery by JP1/IT Desktop Management.

If program updates need to be registered and delivered manually, the administrator must download the program updates and register the program update files.

To register and deliver program updates manually:

1. Download the program updates.
   The program updates can be downloaded from the Microsoft Japan website.

2. Display the Security module.

3. In the menu area, select **Windows Update** and then **Update List**.

4. In **Action** in the information area, select **Add Windows Update**.

5. In the displayed dialog box, enter information about the program updates to be added. Select **Register Windows Update File** and then enter the information required for registration. After entering the information, click **OK**.
   The program update is added to **Update List**, and the program update files are registered.

   Tip

   Add program updates to the update group if only the specific update should be applied. The program updates are applied to the computers according to the auto-enforce settings in security policies to which an update group is set.

The program updates are applied to the computer according to the auto-enforce settings in security policies.

Tip

If the administrator cannot connect to the Internet from the administrator's computer, the administrator can register program update files if the administrator uses a computer that can connect to the Internet, download program updates from the Microsoft Japan website, and then use the data.

9.8.3 Manually adding program updates to the Update List

If the management server is not connected to the Internet and the **Update List** cannot be updated automatically, the administrator can manually update the information for update programs by using another computer that can connect to the Internet.

Also, the administrator can add program updates manually if the administrator wants to add information about program updates (or make the updates the target of security evaluation) sooner than when obtaining the information from the Customer Support website.

To manually update the Update List when the management server is not connected to the Internet:

1. From a computer that can connect to the Internet, access the Customer Support website.

2. From the Customer Support website, download the support information file for updating the Update List offline.

3. From the computer, open the Security module.

4. In the menu area, select **Windows Update**, and then **Update List**.

5. From the **Action**, select **Update Information from Customer Support Offline**.

6. In the displayed dialog box, specify the downloaded file and then click the **OK** button.

The downloaded file will be uploaded to your computer and the Update List is updated.

To manually add the Update List sooner than when obtaining the information from the Customer Support website:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then **Update List**.
3. From the **Action**, select **Add Windows Update**.
4. In the displayed dialog box, enter the information related to the program update, and then click the **OK** button.
   For details about the information related to program updates to be added, see the Microsoft Japan website.

The program update information you entered is added to the Update List.

9.8.4 Manually registering program updates

When manually registering program updates, you need to check the information related to the program updates on the Microsoft Japan website and set that information when registering the updates.

To manually register mandatory programs:

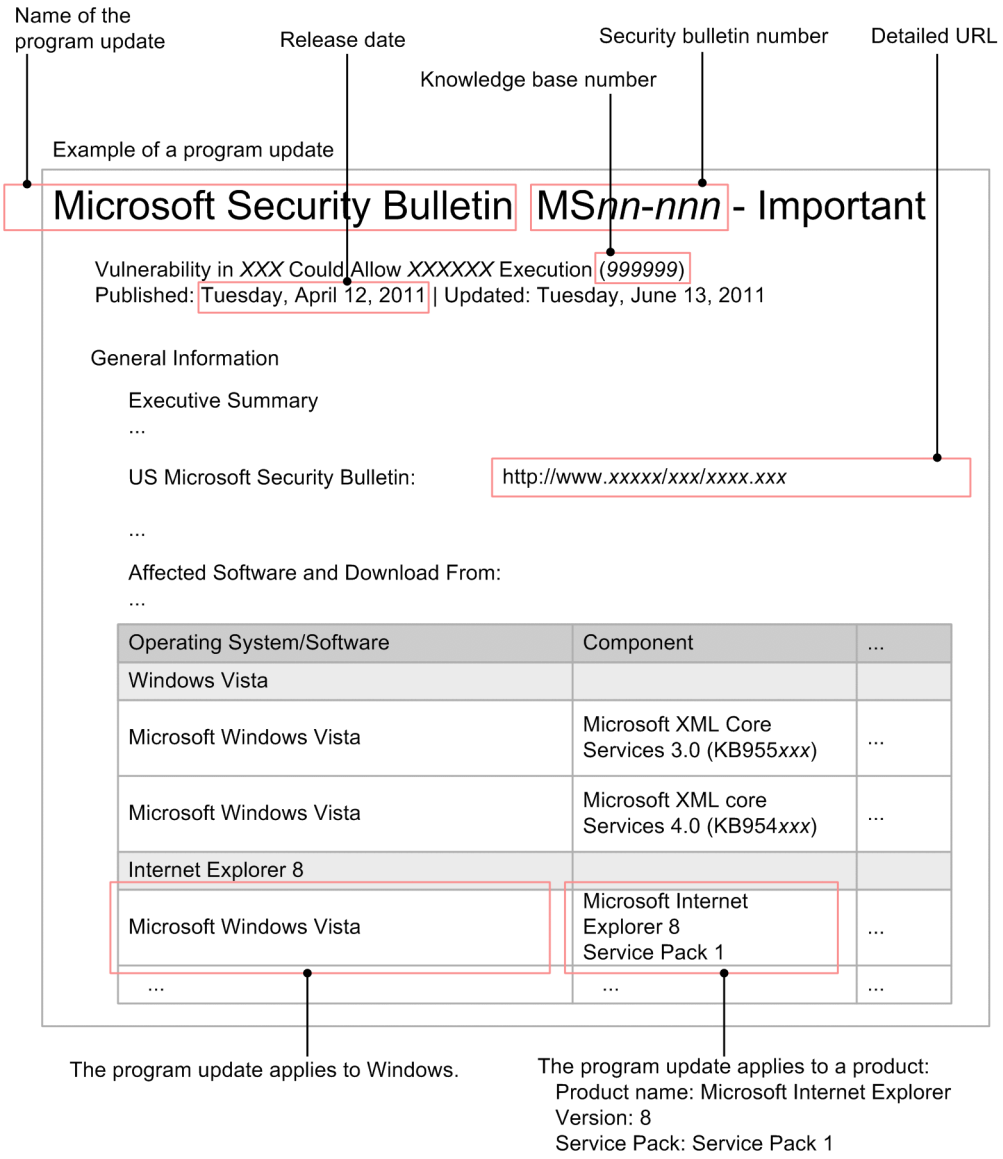
1. Open the security page.
   From the Microsoft Japan website, open the security page (security home page).
2. From the security page, check the detailed information about the program updates.
   From the security page, click the link to the program updates and display the information page for the program updates (security information), and check the detailed information.

   Tip

   We recommend that you keep the detailed information displayed to make it easy to register the information.
3. Register the program updates into JP1/IT Desktop Management.
   In the **Update List** of the Security module, select **Action** and then click **Add Windows Update**.
4. In the displayed dialog box, enter information about the program update, and then click the **OK** button.

The information about the program updates is registered.

The following figure shows an example of the correspondence between program update information on the Microsoft Japan website and the values to be set for each item:



9.8.5 Registering program update files

When program updates are manually registered and are to be delivered, program update files must be registered.

Tip

When the management server can access the Customer Support and Microsoft Japan websites, and when program updates are set to be delivered by security policy-based tasks, the program update files that are to be delivered will be registered automatically at the time when an auto-enforce executes.

Tip

When registering program update files that are not displayed in the **Update List** view, you need to register program update information beforehand. For details about registering program update information, see 9.8.3 Manually adding program updates to the Update List.

Tip

When registering the program update file related to program update information that was registered manually, or when the management server cannot access the Internet, you need to download the execution file for the program update from the Microsoft Japan website beforehand.

If the Update List is being updated offline, you can download program updates by displaying the **Windows Update** view, go to the **Windows Update Information** page, and click **Execution File Download URL**.

To register program update files:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then **Update List**.
3. In the information area, select the program for which you want to register the program update file, and then from the **Action**, select **Register Windows Update File**.
4. In the displayed dialog box, enter the information about the program update to be registered, and then click the **OK** button.

The program update file will be registered, and  is displayed in the **Registration Status** column of the list.

Note that the registered program update files are not added to the **Package List** view of the Distribution module. The program update files can be distributed only by the auto-enforce set in the security policy. Tasks for distributing program update cannot be created manually. Executed tasks can be checked in the Distribution module.

9.8.6 Creating program update groups

In the menu area, program updates can be sorted into any group that is managed. This type of group is called a program update group.

By creating program update groups, you can use them to manage program updates as follows:

- Enable integrated management of program updates that is to be evaluated by specifying the same program update group as the judgement condition for the program update between different security policies.
- When applying a program update to a computer after testing that everything is okay, you can enable automated distribution by registering program updates into program update groups.

To create a program update group:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then move the cursor to **Update Group**.
3. Click the displayed  to the right of the item.
4. From the displayed menu, click  .
5. Enter the name of the group in the displayed text box.

The program update group is added to the menu area.

Tip

Program update groups can also be created from the menu that is displayed by right-clicking **Update Group** in the menu area.

Related Topics:

- 9.8.8 Removing program update groups
- 9.8.7 Changing program update group names
- 9.8.9 Adding program updates to a program update group
- 9.8.10 Removing program updates from a program update group

9.8.7 Changing program update group names

You can change the name of a program update group, such as when the view point of the group information is changed.

To change the name of a program update group:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then under **Update Group**, move the cursor to the group whose name you want to change.
3. Click the displayed  to the right of the item.
4. From the displayed menu, click  .
5. Enter the name of the program update group in the displayed text box.

The name of the group is changed.

Tip

The group name can also be changed from the menu that is displayed by right-clicking the program update group in the menu area.

Related Topics:

- 9.8.6 Creating program update groups
- 9.8.8 Removing program update groups
- 9.8.9 Adding program updates to a program update group
- 9.8.10 Removing program updates from a program update group

9.8.8 Removing program update groups

You can remove unneeded program update groups.

To remove program update groups:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then under **Update Group**, move the cursor to the group you want to delete.
3. Click the displayed  to the right of the item.
4. From the displayed menu, click  .
5. In the displayed view, click the **OK** button.

The program update group is removed.

> **Tip**
>
> The program update group can also be removed from the menu that is displayed by right-clicking the program update group in the menu area.

Related Topics:

- 9.8.6 Creating program update groups
- 9.8.7 Changing program update group names
- 9.8.9 Adding program updates to a program update group
- 9.8.10 Removing program updates from a program update group

9.8.9 Adding program updates to a program update group

In order to group program updates that are the target to be evaluated, you need to add the program update information to a created program update group.

To add program updates to a program update group:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then **Update List**.
3. In the information area, display the information you want to add to the program update group.
4. Select the information you want to add, and from the **Action**, select **Add to Update Group**.
5. In the displayed view, select the program update group to which you want the information to be added and then click the **OK** button.

The selected program update group adds the information.

Tip

The information can also be added from **Add to Update Group** that is displayed by right-clicking the information in the information area.

Tip

The information can also be added by dragging the information into the information area and dropping it on to any program upate group in the menu area.

Related Topics:

- 9.8.6 Creating program update groups
- 9.8.8 Removing program update groups
- 9.8.7 Changing program update group names
- 9.8.10 Removing program updates from a program update group

9.8.10 Removing program updates from a program update group

If you want to exclude program updates in a program update group from being evaluated by a security policy, you can remove information that was added to the program update group.

To remove program updates from a program update group:

1. Open the Security module.
2. In the menu area, select **Windows Update**, and then under **Update Group**, select the program update group from which you want to remove information.
3. In the information area, select the information you want to delete, and from the **Action**, select **Remove from Update Group**.
4. In the displayed view, click the **OK** button.

The information is removed from the selected program update group.

Tip

The information can also be removed from the menu **Remove from Update Group** that is displayed by right-clicking the information in the information area.

Related Topics:

- 9.8.6 Creating program update groups
- 9.8.8 Removing program update groups
- 9.8.7 Changing program update group names
- 9.8.9 Adding program updates to a program update group

10 Operation Log Management

This chapter describes how to trace user operations.

10.1 Specifying settings to collect operation logs for storage on a management server

This section describes how to specify settings to collect operation logs from a computer and store them on a management server.

Important note

To collect operation logs, the agent must be installed in advance on a computer from which operation logs are to be collected.

Important note

In a multi-server configuration system, a management server cannot obtain operation logs.

Tip

In the Settings module, select **Server Configuration** and then the **Server Configuration Settings** view. In the information area, check that a management server is selected for **Operations Log Backup**. If a management server is not selected, select a management server for **Operations Log Backup**.

Tip

If you want to collect operation logs for storage only on a site server, this setting is not required.

To specify settings for collecting operation logs for storage on a management server:

1. In setup, enable **Acquisition of Operations Logs**.
   Specify a folder and the disk space required for storing operation logs. You can also enable or disable automatic backup.
2. In the security policy, specify settings to obtain operation logs.
   You can select the type of operation logs to obtain. If you want to detect suspicious operations, you can also specify detection conditions.
3. Assign the security policy to a group or a computer.

The operation logs of a computer to which the security policy has been assigned are collected and stored on a management server.

Related Topics:

- (2) Managing a security policy
- 10.3 Viewing operation logs
- 10.2 Specifying settings to collect operation logs for storage on a site server

10.2 Specifying settings to collect operation logs for storage on a site server

This section describes how to specify settings to collect operation logs from a computer and store them on a site server.

Note that a site server for storing operation logs must be built in advance.

Important note

To collect operation logs, the agent must be installed in advance on a computer from which operation logs are to be collected.

Tip

If you want to collect operation logs for storage only on a management server, this setting is not required.

To specify settings for collecting operation logs for storage on a site server:

1. Specify a server configuration.
   For each network segment, specify a site server on which to store operation logs.
2. In the security policy, specify settings to obtain operation logs.
   You can select the type of operation logs to obtain. If you want to detect suspicious operations, you can also specify detection conditions.
3. Assign the security policy to a group or a computer.

The operation logs of a computer to which the security policy has been assigned are collected and stored on a site server.

Related Topics:

- (2) Managing a security policy
- 10.1 Specifying settings to collect operation logs for storage on a management server
- 10.3 Viewing operation logs
- 15.1 Managing server configurations

10.3 Viewing operation logs

You can view a list of user operation logs stored on a management server. Tracing the history of file transfers or identifying computers on which suspicious operations were performed allows you to identify information leakage at an early stage, and to take measures against it.

> **Tip**
>
> To obtain operation logs, specify settings for operation logs in setup. In addition, the operation log policy must be enabled in advance.

To view operation logs:

1. Display the Security module.
2. In the menu area, select **Operation Logs** and then **Operation Log List**.

Operation logs are displayed in the information area. Clicking  on the scroll bar scrolls the displayed operation logs by day, and clicking  on the scroll bar scrolls the logs by month. The order in which operation logs that have the same operation date and time are displayed might change on each window page.

At the top of the view, a time chart is displayed, and the dates for which operation logs are displayed are in a frame. If you click the button for a date, operation logs for that date are displayed at the top. Note that you can click only the dates for which **Online** or **Restore** is displayed when you move the mouse over them. If the time chart is too wide to be fully displayed, click  or  to scroll the chart. For the dates for which **Archive** is displayed when you move the mouse over them, you can import operation logs if the logs have been backed up.

If you specify operations that involve file transfers to be detected as suspicious operations in the security policy, when a suspicious file transfer is detected in an operation log,  is displayed in the **Suspicious Operations** field. To search operation logs for suspicious file transfer operations in the operation log list, use this symbol to filter the list to make the search easier.

> **Tip**
>
> In addition, if operation logs are specified in setup to be automatically stored, old operation logs are backed up. Operation logs that are more than one month old are removed from the database. Therefore, if you want to view past operation logs, import the backed up operation logs.

> **Important note**
>
> If operation logs are not stored on a management server, the **Operation Log** view is not displayed.

> **Tip**
>
> You can export operation logs by using the `ioutils exportoplog` command. We recommend that you export operation logs if you want to use them in other materials.

Tip

You can view the operation logs for a device selected in the Device module.

To view the operation logs of the device, in the Device module, select **Device information**, and in the **Device list** view, from **Action** select **To Operation Logs**. The view then switches to the Security module, from which you can view the operation logs. If both operation logs and distributed operation logs have been obtained, the view for checking the distributed operation logs can be displayed by following the steps described above.

Related Topics:

- 10.4 Viewing distributed operation logs
- 10.6 Viewing suspicious operation logs
- 10.8 Tracing operation logs
- 10.9 Importing old operation logs into a management server
- 17.16 ioutils exportoplog (exporting operation logs)

10.4 Viewing distributed operation logs

You can search the details of user operation logs stored on a site server and view them in a list. Tracing the history of file transfers or identifying computers on which suspicious operations were performed allows you to identify information leakage at an early stage, and to take measures against it.

To view distributed operation logs:

1. Display the Security module.
2. In the menu area, select **Operation Logs (Distributed operation log)** and then **Extraction Target List**.
3. In the information area, click the  button.
4. In the displayed dialog box, select filter conditions for the operation logs that you want to view, and then click **OK**.
   In the information area, a list of the following is displayed: the date, the total number of source devices, and the number of operation logs.

   Tip

   You can save filter conditions by clicking the **Save As** button.
5. From the list in the information area, click the total number of source devices for which you want to view details.
   - If the total number of source devices is 10,000 or less:
     In the information area, a list of the following is displayed: the number of site servers for source devices and management sources, as well as the number of operation logs.
   - If the total number of source devices exceeds 10,000:
     In the information area, a list of the following is displayed: the number of site servers for management sources, the number of source devices, and the number of operation logs.
     From the list, click the number of source devices for which you want to view details.
     In the information area, a list of the following is displayed: the number of site servers for source devices and management sources, as well as the number of operation logs.
6. From the list in the information area, click the source devices for which you want to view details.

Operation logs for each selected source are extracted and displayed.

To change the filter conditions for **Extraction Target List**, select the **Extraction Target List** tab, click the  button, and then perform the procedure beginning from step 4.

Important note

If distributed operation logs have not been obtained, the **Operation Log (distributed operation log)** view is not displayed.

Tip

Save the filter conditions for each list displayed in **Extraction Target List** and the operation log list displayed in **Extraction Results**. Because the specifiable filter conditions differ among the lists, if you attempt to apply

filter conditions for one list to another, some conditions might not be applied. In addition, if filter conditions are edited or saved in another list, the originally specified conditions might be deleted.

Tip

You can view the operation logs of a device selected in the Device module.

To view the operation logs of the device, in the Device module, select **Device information**, and in the **Device list** view, from **Action** select **To Operation Logs**. The view then switches to the Security module, from which you can view the operation logs.

Related Topics:

- 10.3 Viewing operation logs
- 10.8 Tracing operation logs
- 10.9 Importing old operation logs into a management server
- 10.6 Viewing suspicious operation logs
- 17.16 ioutils exportoplog (exporting operation logs)

10.5 Specifying settings for detecting suspicious operations

To detect suspicious operations, specify settings for **Suspicious Operations to be Notified** in the operation log policy.

To specify settings for suspicious operations:

1. Display the Security module.
2. In the menu area, select **Security Policy** and then **Security Policy List**.
3. In the information area, select the security policy that you want to edit, and then click the **Edit** button.
   To add a security policy, click the **Add** button.
4. In the security configuration items, click **Operation Logs**.
   If the view is inactive, the operation log policy is disabled. To enable the policy, click the **Enabled** button in the upper-left corner.
5. Specify settings for suspicious operations in **Suspicious Operations to be Notified**.
6. Click **OK**.

If suspicious operations are detected, operation logs for suspicious file transfer operations are displayed in the Security module, and events for all suspicious operations are displayed in the Events module.

Related Topics:

- 10.6 Viewing suspicious operation logs
- 10.7 Viewing events for suspicious operations

10.6 Viewing suspicious operation logs

If you select one or more of the following items for **Suspicious Operations to be Notified** for the operation log policy, when suspicious operations are detected, operation logs for suspicious file transfer operations are displayed in the Security module.

- **Send/Receive E-mail with Attachments**
- **Use Web/FTP Server**
- **Copy/Move the File to External Device**

To view operation logs for suspicious operations:

1. Display the Security module.
2. In the menu area, select **Operation Logs** and then **Operation Log List**. For distributed operation logs, select **Operation logs (distributed operation log)** and then **Extraction Results**.
3. Use the filter to display operation logs for which **Suspicious Operations** is marked with the warning icon ().

Operation logs for suspicious operations are displayed. Check the details of the operation logs, and take action if necessary.

Related Topics:

- 10.7 Viewing events for suspicious operations
- 10.3 Viewing operation logs
- 10.9 Importing old operation logs into a management server
- 10.8 Tracing operation logs

10.7 Viewing events for suspicious operations

If you specify settings for **Suspicious Operations to be Notified** in the operation log policy, when suspicious operations are detected, events for suspicious operations are displayed in the Events module.

To view events for suspicious operations:

1. Display the Events module.
2. Use the filter to display events for which **Type** is **Suspicious Operation**.

Events for suspicious operations are displayed. Check the event details, and take action if necessary.

> **Tip**
>
> You can specify settings to automatically send you a notification email if an event for a suspicious operation occurs.

Related Topics:

- 10.6 Viewing suspicious operation logs
- 15.8.1 Specifying settings for event notification

10.8 Tracing operation logs

You can trace the history of a file used by a user, such as when the file was created, where it was transferred from, or where it was transferred to. Check the trace results to identify problems such as information leakage.

To trace operation logs:

1. Display the Security module.
2. In the menu area, select **Operation Logs** and then **Operation Log List**. For distributed operation logs, select **Operation logs (distributed operation log)** and then **Extraction Results**.
3. In the information area, click the **Trace** button of the operation logs that you want to trace.

In the **Log Tracing** dialog box, the trace results based on the selected operation logs are displayed.

To view the details of operation logs, click the **Operation Details** link.

> **Tip**
>
> If you want to trace operation logs that include older logs that have been backed up, import in advance the old operation logs. For details about how to import old operation logs, see 10.9 Importing old operation logs into a management server.

> **Tip**
>
> You can export operation logs by using the `ioutils exportoplog` command. We recommend that you export operation logs if you want to use them in other materials.

Related Topics:

- 10.3 Viewing operation logs
- 10.6 Viewing suspicious operation logs
- 17.16 ioutils exportoplog (exporting operation logs)

10.9 Importing old operation logs into a management server

If the operation logs for a file to be traced have already been removed, you can import old operation logs from an operation log backup.

Important note

If the operation logs for the relevant period have been deleted from the backup folder, you cannot import them.

Tip

To import old operation logs, in the **Automatic Backup Settings for Operation Logs** view in setup, specify a location in which to store the operation logs. Note that the amount of operation log data that can be imported is determined according to **Required capacity** in the **Operation Log Settings** view in setup. If you want to import operation logs for a longer period, specify the longer period in **Maximum restore period for operation logs**.

To import old operation logs:

1. Display the Security module.
2. In the menu area, select **Operation Logs** and then **Operation Log List**.
3. From **Action**, select **Restore Archived Logs**.

   ### Important note

   If there is no operation log backup file, you cannot perform this operation.

4. In the displayed dialog box, specify the period for which operation logs are to be imported, and then click **OK**.
   Operation logs are imported and the import status is displayed.
5. Click the **Close** button.

The operation logs for the specified period are imported. If the specified period includes a period that was specified for data already imported in the past, the operation logs for the period that does not include the previously specified period are imported.

Tip

If you cannot specify a period of a sufficient length for operation logs to be imported because of the amount of data previously imported, delete the operation logs for the unnecessary period. From **Action**, select **Remove Restored Logs**, delete the operation logs for the unnecessary period, and then import operation logs.

Tip

You can export operation logs by using the `ioutils exportoplog` command. We recommend that you export operation logs if you want to use them in other materials.

Related Topics:

- 10.3 Viewing operation logs
- 10.8 Tracing operation logs
- 10.6 Viewing suspicious operation logs
- 17.16 ioutils exportoplog (exporting operation logs)

10.10 Maintaining operation logs for site servers

10.10.1 Backing up operation logs on site servers

You can back up operation logs stored on a site server, in case of server failure.

To back up operation logs on a site server:

1. From the folder that was specified in **Operation log data folder** in site server setup, copy each folder with a name in *YYYYMMDD*# format to the backup folder.
   #: *YYYY*: year, *MM*: month, *DD*: day

The operation logs in the copied date folders are backed up.

Tip

In addition to backing up operation logs on a site server in case of failures, you must also back up operation logs before uninstalling a site server or disposing of a site server computer. You can view backed up operation logs again by importing them into another site server.

Related Topics:

- 10.10.2 Importing backed up operation logs into a site server

10.10.2 Importing backed up operation logs into a site server

You can import operation logs backed up from a site server into a site server, and then view them in the operation window. Note that the site server from which operation logs were backed up does not have to be the same computer into which the backed up operation logs are imported.

To import backed up operation logs:

1. Stop the site server service.
2. Copy the backed up data (a folder with a name in date format) to the operation log data folder on the site server into which the operation logs are to be imported.
3. Execute the `recreatelogdb` command to recreate the index information for the operation logs.
4. Start the site server service.

The backed up operation logs are imported into the site server to which they are copied, and you can view them in the operation window.

Important note

Because the site server stops while the `recreatelogdb` command is being executed, any operation logs generated during that period cannot be viewed until the command execution is complete. After the `recreatelogdb` command is finished executing, when the site server starts, creation of index information

for operation logs also starts. Because creation of index information places a heavy load on the site server, depending on the amount of operation log data, it might take several days to complete. In addition, any operation logs generated while the index information is being created cannot be viewed until creation of the index information is complete. Take these factors into account before executing the `recreatelogdb` command.

Related Topics:

- 10.10.1 Backing up operation logs on site servers
- 17.17 recreatelogdb (recreating an operation log index on the site server)

10.10.3 Actions to be taken when site server disk capacity is insufficient

If operation logs are stored on a site server, when the free space on the disk on which the logs are stored becomes insufficient, operation logs are no longer automatically stored. When this occurs, resolve the problem by providing the disk with more space and continuing to use the same location, or by changing the location for storing operation logs.

After you change the location to store operation logs, obtained operation logs are stored in the changed location. Both the operation logs stored in the previous location and the operation logs stored in the changed location can be viewed in the operation window.

When adding or disposing of a hard disk, if you want to change the location for storing operation logs, including those already obtained, after changing the storage location, you must use a command to migrate the operation log data.

The following describes the steps to follow:

To use the same storage location:

1. Ensure that there is enough free space for storage on the disk by deleting unnecessary operation logs or files, or by adding a logical disk.
   To delete unnecessary operation logs, execute the `deletelog` command.
2. Restart the site server service (JP1_ITDM_Remote Site Service).

Obtained operation logs will be stored in the same location.

To change the storage location:

1. In site server setup, change the location for storing operation logs.

Obtained operation logs will be stored in the new location.

To change the location for storing operation logs, including those already obtained:

1. In site server setup, change the location for storing operation logs.
2. Migrate the operation log data by executing the `movelog` command.

The operation logs that have already been obtained are migrated to the new storage location. Operation logs to be obtained will also be stored in the new location.

Related Topics:

- 17.19 deletelog (deleting operation logs on the site server)

- 17.18 movelog (moving operation logs on the site server)

10.10.4 Action to be taken in case of failure in a site server database

When you search the operation logs on a site server, index information for the operation logs is used. Because of this, if a failure occurs in the site server database, and operation log data and index information are no longer consistent or index information is lost, you cannot properly search the operation logs stored on the site server.

In this case, recreating the index information for the operation logs on the site server allows you to resume proper searches of the operation logs stored on the site server.

To take action in case of a failure in the site server database:

1. Execute the `recreatelogdb` command on the site server.

Index information for operation logs is recreated and you can search the operation logs.

> **Important note**
>
> Because the site server stops while the `recreatelogdb` command is executed, the operation logs generated during that period cannot be viewed until execution of the command completes. After the completion of the `recreatelogdb` command, when the site server starts, creation of index information for operation logs also starts. Because creation of index information places a heavy load on the site server, depending on the amount of operation log data, it might take several days to complete. In addition, the operation logs generated while the index information is created cannot be viewed until creation of the index information completes. Take into account the impact described above before executing the `recreatelogdb` command.

Related Topics:

- 17.17 recreatelogdb (recreating an operation log index on the site server)

11 Asset Management

This chapter describes how to manage hardware assets, software licenses, and contracts.

11.1 Using hardware asset information

11.1.1 Adding hardware asset information

To manage the stocktaking schedule and asset status of managed devices, select **Hardware Assets** in the Assets module, and then you can add hardware asset information to the list in the Hardware Assets view. Also, by associating contract information with hardware asset information, you can check the costs generated from asset operation on the **Hardware Asset Costs** report.

To add hardware asset information:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select a group.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, enter the asset information, and then click **OK**.

> **Tip**
>
> To add other hardware asset information, click the **Save/Add** button.

The hardware asset information is added and displayed in the hardware asset list.

> **Tip**
>
> If you set a device as a management target, its hardware asset information is automatically registered. The automatically registered hardware asset information is associated with the device information. When you edit the hardware asset information, the device information can also be managed accordingly. We recommend that you use this method to add the hardware asset information when you need to manage both device information and hardware asset information.

> **Important note**
>
> When you change the **host name** in the device information, the **device name** in the hardware asset information is not automatically changed, even if the device information and hardware asset information are associated with each other. If you change the **host name** in the device information, and if the **device name** in the hardware asset information is the same as the **host name** in the device information, manually change the **device name** in the hardware asset information.

> **Tip**
>
> You can also batch-add hardware asset information by importing a CSV file. We recommend that you create and then import a CSV file if you need to add a large amount of hardware asset information.

Tip

To set the security policy to allow the use of a USB device, connect the USB device to an online-managed computer, and then register the hardware asset information.

Related Topics:

- 11.1.2 Editing hardware asset information
- 11.1.3 Removing hardware asset information
- 11.1.6 Changing the asset status
- 11.1.7 Changing the planned asset status
- 11.4.1 Importing hardware asset information
- 11.5 Exporting asset information
- 9.7 Registering USB devices

11.1.2 Editing hardware asset information

When the user information of a hardware asset is changed, or another hardware asset associated with a hardware asset is changed, you can edit hardware asset information.

To edit hardware asset information:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select the group that contains the hardware asset information that you want to edit.
3. In the information area, select the hardware asset information that you want to edit, and then click the **Edit** button.
   You can batch edit hardware asset information by selecting multiple items.
4. In the displayed dialog box, edit the hardware asset information, and then click **OK**.

The selected hardware asset information is updated.

Important note

When the hardware asset information and device information are associated with each other, the **device information** that has been collected automatically overwrites the device information that has been edited.

Tip

You can also batch-edit hardware asset information by importing a CSV file. If you need to edit a large amount of hardware asset information, we recommend that you export the hardware asset information into a CSV file, and then edit and import the CSV file.

Tip

To only change the **asset status** and basic hardware asset information, you can also click the **Change Status** button, and then make changes from the displayed dialog box.

Tip

To only change the **planned asset status** and **planned date**, select **Change Asset Status (Planned)** from **Action**, and then make changes from the displayed dialog box.

Related Topics:

- 11.1.1 Adding hardware asset information
- 11.1.3 Removing hardware asset information
- 11.1.6 Changing the asset status
- 11.1.7 Changing the planned asset status
- 11.4.1 Importing hardware asset information
- 11.5 Exporting asset information

11.1.3 Removing hardware asset information

You can remove the hardware asset information that is no longer needed. Hardware asset information can be removed only if the **asset status** is **unconfirmed** or **expired**.

Note that when hardware asset information is removed, its association with contract information and other hardware asset information is also removed.

To delete hardware asset information:

1. Display the Assets module.
2. From **Hardware Asset** in the menu area, select the group that contains the hardware asset information that you want to remove.
3. In the information area, select the hardware asset information that you want to remove, and then select **Remove Hardware Assets** from **Action**.

   You can batch-remove hardware asset information by selecting multiple items.
4. In the displayed dialog box, click **OK**.

The selected hardware asset information is removed.

Related Topics:

- 11.1.1 Adding hardware asset information
- 11.1.2 Editing hardware asset information
- 11.1.6 Changing the asset status
- 11.1.7 Changing the planned asset status

- 11.4.1 Importing hardware asset information
- 11.5 Exporting asset information

11.1.4 Setting the display interval for the End User Form view in the Assets module

When the hardware asset information and device information of the managed computer are associated with each other, you can set an interval for displaying the **End User Form** view on an online-managed computer. By periodically requesting that users enter user information, your management workload can be reduced.

Note that to display the **End User Form** view, the agent must be installed on the user computer.

To set the interval at which the End User Form view appears:

1. Display the Assets module.
2. From **Hardware Asset** in the menu area, select a group.
3. From **Action**, select **Enable End User Form (Frequent Pop-up)**.
4. In the dialog box that appears, specify the display interval, and then click **OK**.

The interval at which the **End User Form** view appears is set.

> **Tip**
>
> You can specify the items to be displayed in the **End User Form** view by selecting **Asset management** in the Settings module and then **Asset Field Definitions**.

Related Topics:

- 15.5.1 Adding asset management items

11.1.5 Adding an asset status

You can add an item to **Asset Status**. By doing so, you can match the management of asset statuses to the operation being performed.

To add an asset status:

1. Display the **Asset Field Definitions** view in the Settings module.
2. In **Custom Fields (Hardware Assets)**, click the **Edit** button in **Asset Status**.
3. In the **Edit Custom Filds** dialog box, click the **Add** button.
4. In the **Add New Item** dialog box, enter the item name, and then click **OK**.
   For example, enter Solving Trouble.
5. In the **Edit Custom Filds** dialog box, click **OK**.

The asset status item is added. Note that you can add up to 100 items that are different from the default.

In the **Edit Custom Filds** dialog box, you can edit, remove, or sort the existing items.

Tip

You cannot edit or remove the default items (**Unconfirmed**, **In Stock**, **In Use**, and **Expired**). In addition, you cannot remove asset statuses that were added by an administrator and saved as a filter condition.

Tip

You can also add an asset status by selecting **Add New** when setting the hardware asset information.

11.1.6 Changing the asset status

To change the **asset status** or basic asset information (such as department and location), in addition to the **Edit Hardware Asset** dialog box, you can also use the **Change Asset Status** dialog box.

To change the asset status:

1. Display the Assets module.
2. From **Hardware Asset** in the menu area, select the group that contains the hardware asset information whose **asset status** you want to change.
3. In the information area, select the hardware asset information whose **asset status** you want to change, and then click the **Change Status** button.
   You can also batch-change hardware asset information by selecting multiple items.
4. In the displayed dialog box, change the **asset status**, and then click **OK**.
   If you select **Add Notes**, information such as the asset statuses before and after the change, the date of change, and reasons for change can be recorded. The information entered here will be added to the **Notes** tab.

The **asset status** of the selected hardware asset information is updated.

Tip

To edit another item, click the **Edit** button, and then edit in the displayed dialog box.

Related Topics:

- 11.1.1 Adding hardware asset information
- 11.1.2 Editing hardware asset information
- 11.1.3 Removing hardware asset information
- 11.1.7 Changing the planned asset status
- 11.4.1 Importing hardware asset information
- 11.5 Exporting asset information

11.1.7 Changing the planned asset status

To change the **planned asset status** and **planned date**, in addition to the **Edit Hardware Asset** dialog box, you can also use the **Change Asset Status (Planned)** dialog box.

By specifying the **planned asset status**, you can use the digest report or mail notification to check a hardware asset that is planned to be changed. For example, for a hardware asset whose asset status will be changed from **In Use** to **In Stock**, you can take the asset back to the storage after receiving a notification of the status change.

To change the planned asset status:

1. Display the Assets module.
2. From Hardware Asset in the menu area, select the group that contains the **hardware asset** information whose **planned asset status** you want to change.
3. In the information area, select the hardware asset information whose **planned asset status** you want to change, and then select **Change Asset Status (Planned)** from **Action**.
   You can batch-change the hardware asset information by selecting multiple items.
4. In the dialog box, change the **planned asset status** and **planned date**, and then click **OK**.
   If you select **Add Notes**, information such as the asset statuses before and after the change, the date of change, and reasons for change can be recorded. The information entered here will be added to the **Notes** tab.

The **planned asset status** and **planned date** of the selected hardware asset information are updated.

> **Tip**
>
> To edit another item, click the **Edit** button, and then edit in the displayed dialog box.

Related Topics:

- 11.1.1 Adding hardware asset information
- 11.1.2 Editing hardware asset information
- 11.1.3 Removing hardware asset information
- 11.1.6 Changing the asset status
- 11.4.1 Importing hardware asset information
- 11.5 Exporting asset information

11.1.8 Manually updating a stocktaking date

You can manually update the **stocktaking dates** for the hardware asset information and software license information. We recommend that you take stock individually of small-quantity assets nearby.

To manually update a stocktaking date:

1. Display the Assets module.
2. From **Hardware Asset** or **Software License** in the menu area, select the group that contains the asset information whose **stocktaking date** needs to be updated.

3. In the information area, select the asset information whose **stocktaking date** needs to be updated, and then select **Update Tracked Date (Directly)** from **Action**.
   You can batch update asset information by selecting multiple items.

4. In the displayed dialog box, enter the stocktaking date, and then click **OK**.
   If you select **Add Notes**, information such as the stocktaking date, stocktaking method, and reasons for stocktaking can be recorded. The information entered here will be added to the **Notes** tab.

The **stocktaking date** for the selected asset information is updated.

Tip

You can also batch update **stocktaking dates** by using a CSV file that contains the **asset numbers** or **license numbers**.

Tip

For hardware asset information, you can set the stocktaking date to be automatically updated. JP1/IT Desktop Management determines whether a device exists from the network connection of the device or the data entry of the device user. When the existence of the device is confirmed, the stocktaking date is automatically updated.

Tip

You can also batch update **stocktaking dates** by importing the hardware asset information or software license information.

Related Topics:

- 11.1.9 Batch updating stocktaking dates by using a CSV file
- 11.1.10 Setting automatic update for the stocktaking date
- 11.4.1 Importing hardware asset information
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.1.9 Batch updating stocktaking dates by using a CSV file

You can use a CSV file to batch-update the **stocktaking dates** of the hardware asset information and software license information.

We recommend this method if you use bar codes, instead of JP1/IT Desktop Management, to manage asset numbers. Export the information read by a barcode reader into a CSV file. The CSV file must be in the either of the following:

For hardware asset information

The **asset number** list of the hardware asset information whose **stocktaking date** needs to be updated

For software license information

The **license number** list of the software license information whose **stocking date** needs to be updated

To batch-update the stocktaking dates by using a CSV file:

1. Display the Assets module.
2. From **Hardware Asset** or **Software License** in the menu area, select the group that contains the asset information whose **stocktaking date** needs to be updated.
3. From **Action**, select **Update Tracked Date (from CSV)**.
4. In the displayed dialog box, click the **Select** button, and then specify the CSV file that was created in advance.
   You can download a sample of the CSV file by clicking the link of **Download CSV Sample File**.
5. Enter the stocktaking date, and then click **OK**.
   If you select **Add Notes**, information such as the stocktaking date, stocktaking method, and reasons for stocktaking can be recorded. The information entered here will be added to the **Notes** tab.

The **stocktaking dates** of the asset information corresponding to the **asset numbers** and **license numbers** that are contained in the CSV file are updated in a batch.

Important note

If an error occurs when updating the stocktaking date, an asset which is not managed by JP1/IT Desktop Management exists. Check the asset numbers, and register the unmanaged asset.

Tip

For hardware asset information, you can set the stocktaking date to be automatically updated. JP1/IT Desktop Management determines whether a device exists from the network connection of the device or the data entry of the device user. When the existence of the device is confirmed, the stocktaking date is automatically updated.

Tip

You can also batch update the stocktaking dates by importing the hardware asset information and software license information. In this case, you can set a different stocktaking date for the information of each asset.

Related Topics:

- 11.1.11 Taking stock by using a barcode reader
- 11.1.8 Manually updating a stocktaking date
- 11.1.10 Setting automatic update for the stocktaking date
- 11.4.1 Importing hardware asset information
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.1.10 Setting automatic update for the stocktaking date

You can set automatic update for the **stocktaking date** of hardware asset information. When automatic update is set, the **stocktaking date** is automatically updated at the following timing, so the workload of stocktaking can be reduced.

For online management

When the last alive confirmation date/time of the device is updated, or user information is entered

For offline management

When the device information is notified to the management server

To set automatic update for the stocktaking date:

1. Display the Assets module.
2. From **Hardware Asset** in the menu area, select a group.
3. From **Action**, select **Update Tracked Date (Automatically)**.
4. In the displayed dialog box, select one of the following, and then click **OK**.

   For an offline-managed device, the **stocktaking date** is the day when the device information is notified to the management server.

   Setting the last alive confirmation date/time of the device as the **stocktaking date**

   When the connection to the network is confirmed, the existence of the device is confirmed, and the stocktaking date is automatically updated. Note that devices that are not connected with the network cannot be automatically updated.

   Setting the day when the user finishes the data entry in the **End User Form** view as the **stocktaking date**

   Display the **End User Form** view on a user computer. Set the **End User Form** view to be periodically displayed, so that the existence of the computer can be confirmed when the user enters information, and the stocktaking date can be automatically updated. You can specify when to display the **End User Form** view by selecting **Enable End User Form (Frequent Pop-up)** from **Action**. Note that to display the **End User Form** view, the agent must be installed on the user computer. For user computers on which the agent is not installed, the stocktaking date cannot be automatically updated.

The **stocktaking date** is automatically updated at the selected timing.

Tip

You can also batch update the **stocktaking dates** by using a CSV file that contains the **asset numbers** or **license numbers**.

Tip

You can also batch update the **stocktaking dates** by importing the hardware asset information and software license information. In this case, you can set a different **stocktaking date** for the information of each asset.

Related Topics:

- 11.1.8 Manually updating a stocktaking date
- 11.1.9 Batch updating stocktaking dates by using a CSV file
- 11.4.1 Importing hardware asset information

- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.1.11 Taking stock by using a barcode reader

You can easily take stock by using a barcode reader. We recommend that you use this method to take stock if you are using a barcode reader that can export information into a CSV file to management assets, in addition to JP1/IT Desktop Management.

1. Actually count the devices.

   Use the barcode reader to check all the devices in your organization.

2. Export the asset information list.

   Export the device information actually read by the barcode reader to into a CSV file.

   Edit the CSV file, so that each line only contains the **asset number** of one device that was actually counted.

3. Update the stocktaking dates.

   After the CSV file containing the hardware asset information is created, read the CSV file to batch-update the stocktaking dates. For details about how to update the stocktaking date, see 11.1.9 Batch updating stocktaking dates by using a CSV file.

   The **stocktaking dates** for the hardware asset information contained in the CSV file are updated.

   Important note

   If an error occurs when updating the stocktaking date, an asset which is not managed by JP1/IT Desktop Management exists. Check the asset numbers, and register the unmanaged asset.

4. Check the uncounted devices.

   The hardware asset information whose **stocktaking date** is not updated is displayed in the **Hardware Asset** view of the Assets module. To actually count the devices, export the items such as **Asset #**, **Department**, **Location**, and **User Name**. For details about how to export, see 11.5 Exporting asset information.

5. Check the use status with the device user.

   After you create the hardware asset list, check the actual location of the device with the device user.

   If the device is found

   In the list, record the fact that the device has been found, and make corrections if necessary.

   If the device is not found

   The device might be lost. Instruct the user to report the missing device in writing. If necessary, change the **asset status** to **Disposed** in the **Hardware Asset** view of the Asset module. Also, record the information such as the cause or date of loss on the **Notes** tab.

6. Apply the results of the stocktaking

   Apply the count results for the devices whose existence has been confirmed.

   Update the **stocktaking date** for the devices that were not physically confirmed during the stocktaking but found later.

Related Topics:

- 11.1.8 Manually updating a stocktaking date
- 11.1.10 Setting automatic update for the stocktaking date

- 11.4.1 Importing hardware asset information

11.1.12 Associating contract information with hardware asset information

You can associate contract information with hardware asset information. When such an association is established, you can manage the trends of the contract costs and contract types of hardware assets.

For details about how to create contract information, see 11.3.1 Adding contract information.

To associate contract information with hardware asset information:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select the group that contains the hardware asset information for which you want to set contract information.
3. In the information area, select the hardware information for which you want to set contract information, and then select **Associate Contract** from **Action**.
4. In the displayed dialog box, select the contract information, and then click **OK**.

The contract information is associated with the hardware asset information.

Tip

You can also associate contract information with the hardware asset information on the **Contract Information** tab of the Hardware Assets view.

Tip

You can also associate the contract information by using **Associated Information** in the dialog box for adding or editing hardware asset information.

Related Topics:

- 11.3.6 Linking hardware assets (contract)

11.1.13 Associating multiple items of hardware asset information

You can establish an association between multiple items of hardware asset information to collectively manage hardware asset information of devices, such as information of computers, displays, and CD/DVD drives.

To associate multiple items of hardware asset information:

1. Display the Assets module.
2. From **Hardware Asset** in the menu area, select the group that contains the hardware asset information for which you want to establish an association.

3. In the information area, select the hardware asset information for which you want to establish an association, and then select **Associate Hardware Asset** from **Action**.

4. In the displayed dialog box, select the hardware asset information, and then click **OK**.

An association between multiple items of hardware asset information is established.

Important note

When you are collectively managing multiple assets, if you change the **asset status** of a computer, the **asset status** of the associated device, such as a display or CD/DVD drive is not changed. For example, if you update the **stocktaking date**, you need to update the **stocktaking dates** for all associated items of the hardware asset information.

Tip

You can also establish an association between multiple items of hardware asset information on the **Associated Assets** tab of the Hardware Assets view.

Tip

You can also establish an association between multiple items of hardware asset information by using **Associated Information** in the dialog box for adding or editing hardware asset information.

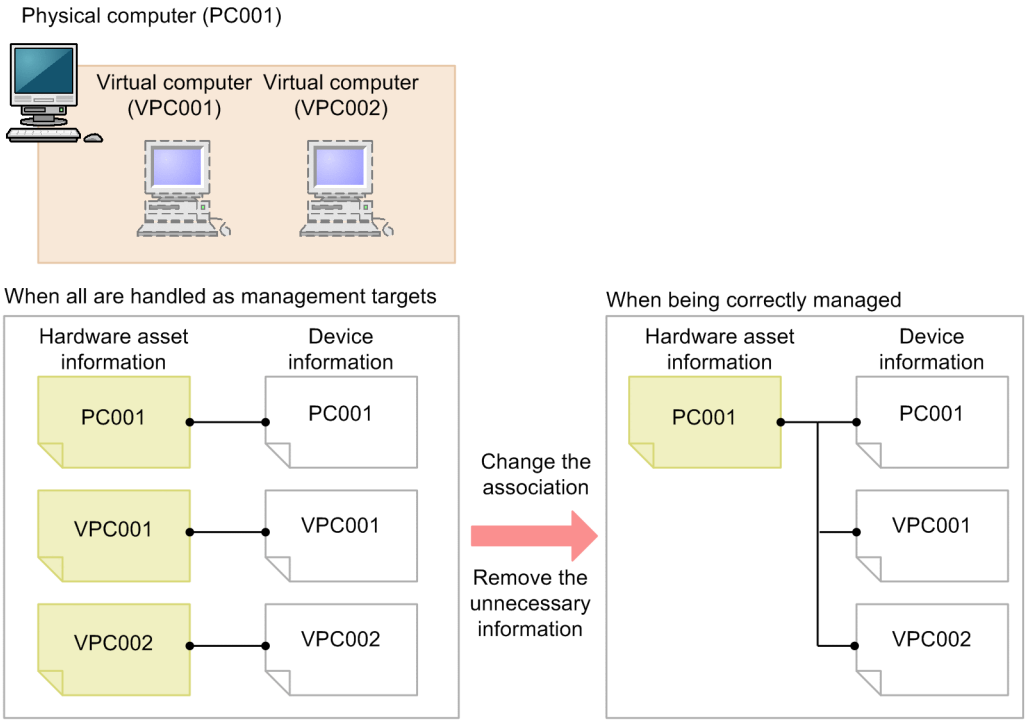
11.1.14 Changing the device information associated with the hardware asset information

You can manually change the device information associated with the hardware asset information.

You can associate the device information with hardware asset information of different devices or the hardware asset information with multiple items of device information.

For example, in an environment in which two virtual computers are configured on one physical computer, the hardware asset information of three different computers is registered if each computer is handled as a management target. However, only one computer actually exists. To correctly manage the hardware asset information, you need to associate the device information of the two virtual computers with the hardware asset information of the physical computer, and remove the unnecessary hardware asset information of the virtual computers.

The following example illustrates how to change the associated device information to correctly manage the hardware asset information.



To change the device information associated with the hardware asset information:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select the group that contains the hardware asset information whose association you want to change.
3. In the information area, select the hardware asset information whose association you want to change, and then display the **Device Information** tab.
4. On the **Device Information** tab, select the device information whose association you want to change.
5. Click the **Change Hardware Asset Association** button on the tab.
6. In the displayed dialog box, select the hardware asset information to be associated with the device information.

The device information associated with the hardware asset information is changed.

Related Topics:

- 11.1.15 Setting primary information associated with hardware asset information

11.1.15 Setting primary information associated with hardware asset information

When multiple items of device information are associated with the same hardware asset information, you can specify primary information as a representative of the device information. When the primary information is specified, its device information is applied to the hardware asset information.

To specify primary information:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select the group that contains the hardware asset information that is associated with multiple items of device information.
3. In the information area, select the hardware asset information that is associated with multiple items of device information, and then display the **Device information** tab.
4. On the **Device information** tab, select the device information that you want to specify as the primary information.
   Note that you cannot select multiple items of device information.
5. Click the **Change Primary Inventory** button on the tab.
6. In the displayed dialog box, click **OK**.

The primary information is set for the device information that is associated with the hardware asset information. The ✔ mark appears in the **Primary Inventory** item of the primary information.

Related Topics:

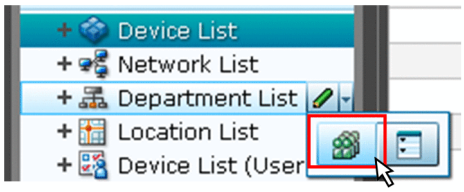
- 11.1.14 Changing the device information associated with the hardware asset information

11.1.16 Adding the definition for a department or location

If the departments or locations to manage increase, you can add a definition for a new department or location. After the definition is added, the new department or location is displayed in the menu area of the Assets module and the Device module.

To add the definition for a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



> **Tip**
>
> Alternatively, you can perform the following: In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the window that appears, click either **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

3. In the displayed dialog box, click the **Edit** button in **Type**.
4. In the displayed dialog box, add the department or location.

5. Click **OK**.

6. Click **OK**.

The the definition for the department or location is added, and the added group is displayed in the menu area of the Assets module and Device module.

Related Topics:

- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location

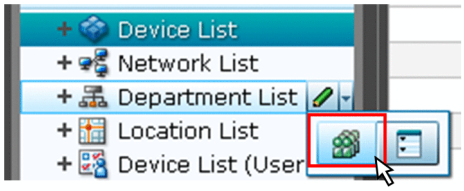
11.1.17 Editing the definition for a department or location

If the organizational structure of the departments you are managing or the name of a location was changed, you can edit the definition for the department or location. After the definition is edited, the edited department or location is displayed in the menu area of the Assets module and the Device module.

To edit the definition of a department or location:

1. Display the Assets module.

2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



> **Tip**
>
> Alternatively, you can perform the following: In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the window that appears, either click **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

3. In the displayed dialog box, click the **Edit** button in **Type**.

4. In the displayed dialog box, edit the name of the department or location, or hierarchical structure.

5. Click **OK**.

6. Click **OK**.

The definition for the department or location is edited, and the edited group is displayed in the menu area of the Assets module and Device module.

The user information (actual status) of each device is unchanged even if you changed a definition. Therefore, the definition that is different from the actual status is added to the menu area of the Assets module and Device module. To ensure the actual status is consistent with the definition, update the user information according to the definition after you edited the definition for a department or location. After you update the user information, delete only the hierarchies that exist in the old organizational system, so that the menu area display is consistent with the definition. For details

about how to delete only the hierarchies that were used in the old system, see 6.31 Removing only hierarchies that were used in the old organizational system.

Tip

After you change the department definition, the department information displayed in the following views in the Assets module also changes: **Software License List** in **Software Licenses**, **Software License Status List** in **Software License Status**, and **Contract List** in **Contracts**.

Related Topics:

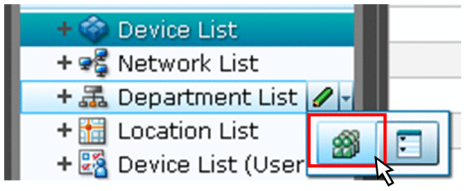
- 6.28 Adding the definition for a department or location
- 6.30 Removing the definition for a department or location

11.1.18 Removing the definition for a department or location

If you no longer manage a department or location, you can remove the definition for the department or location. After the definition is removed, the removed department or location no longer appears in the menu area of the Assets module and the Device module.

To remove the definition for a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



3. In the displayed dialog, click the **Edit** button in **Type**.
4. In the display the window, remove the definition for the department or location.
5. Click **OK**.
6. Click **OK**.

The definition for the department or location is removed.

The user information (actual status) of each device is unchanged even if you remove a definition. Therefore, the removed hierarchy is still displayed in the menu area of the Assets module and the Device module. To ensure the actual status is consistent with the definition, update the user information according to the definition after you edited the definition for a department or location. After you update the user information, delete only the hierarchies that exist in the old organizational system, so that the menu area display is consistent with the definition. For details about how to delete only the hierarchies that were used in the old system, see 6.31 Removing only hierarchies that were used in the old organizational system.

Tip

After you delete the department definition, in the following views of the Assets module, Unknown appears for the department:

- The **Software License List** view in **Software Licenses**
- The **Software License Status List** view in **Software License Status**
- The **Contract List** view in **Contracts**

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location

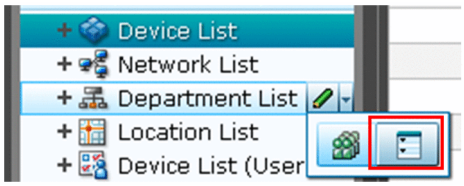
11.1.19 Removing only hierarchies that were used in the old organizational system

Even if you remove the hierarchies (definitions) for the departments or locations in the Settings module in association with an organizational change, the removed hierarchies will still appear in the menu area of the Assets or Device module. To ensure that the display in the menu area is consistent with the definitions, you need to remove only the hierarchies that were used in the old organizational system. You can do so in the dialog box that you display from the menu area of the Assets module, the Device module, or the Security module.

The example below explains how to remove such hierarchies from the Assets module.

To remove only hierarchies that were used in the old organizational system:

1. Display the Assets module.
2. In the menu area, select **Hardware Asset**, select **Department List** or **Location List**, and then click the icon that appears.



3. In the dialog box that appears, select the hierarchies that you want to remove.
4. Click the **Remove** button.
5. In the dialog box that appears, click **OK**.
6. Click the **Close** button.

Only the hierarchies that were used in the old organizational system are removed, and the display of the menu area in the Assets module or the Device module is now consistent with the definitions.

11.1.20 Changing the name of a department or location

If the organizational structure of the departments you are managing or the name of a location was changed, you can change the name of the department or location.

To change the names of a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then move the cursor over the group for which you want to change the name.
3. Click  that is displayed to the right of the item.
4. In the displayed menu, click  .
5. In the displayed text area, enter the name of the department or location.

The name of the department or location is changed. The group name in the device user information is also changed to the new name.

> **Tip**
>
> You can also right-click the department or location in the menu area, and then change the name from the displayed menu.

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location
- 6.33 Deleting a department or location

11.1.21 Deleting a department or location

You can remove an unnecessary department or location.

To remove a department or location:

1. Display the Assets module.
2. In the menu area, select **Hardware Assets** and then **Department List** or **Location List**, move the cursor over the group that you want to remove.
3. Click  displayed on the right side of the item.
4. In the displayed menu, click  .
5. In the displayed dialog box, click **OK**.

The group that contains the department or location is removed. The department or location is also removed from the device user information.

Tip

You can also right-click the department or location in the menu area, and then remove it from the displayed menu.

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location
- 6.32 Changing the name of a department or location

11.2 Using software license information

11.2.1 Adding managed software information

Select **Managed Software** in the Assets module, and then you can add managed software information to the **Managed Software List**. When managed software information is added, you can check the number of used software licenses.

You can view the managed software information in the **Software List** view by selecting**Software Inventory** in the Device module and then **Software List**. You can also view the managed software information in the **Software License List** view by selecting **Software License** in the Assets module and then **Software License List**.

To add managed software information:

1. Display the Assets module.
2. In the menu area, select **Managed Software** and then **Managed Software List**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, enter the information, and then click **OK**.

The managed software information is added and displayed in the list.

> **Tip**
>
> You can also batch-add managed software information by importing a CSV file. We recommend that you create and import a CSV file if you need to add a large amount of managed software information.

If you specify the software that corresponds to the managed software information, the number of used licenses can be counted based on the collected software information, so that you can understand the usage of the licenses. You can specify multiple software programs. For example, by specifying different versions of the same software, you can know the accumulated number of used licenses regardless of the versions.

You can also be aware of the insufficient number of software licenses and identify the computers on which software is illegally used, by assigning software licenses to computers and adding the corresponding software license information. The relevant information can be displayed in the **Software (License Violation)** panel by selecting **Overview** and then **Dashboard**.

Related Topics:

- 11.2.2 Editing managed software information
- 11.2.3 Removing managed software information
- 11.4.3 Importing managed software information
- 11.5 Exporting asset information

11.2.2 Editing managed software information

When the specified managed software or the number of software licenses is changed, you can edit the managed software information.

To edit managed software information:

1. Display the Assets module.
2. In the menu area, select **Managed Software** and then **Managed Software List**.
3. In the information area, select the managed software information that you want to edit, and then click the **Edit** button.
   You can batch-edit managed software information by selecting multiple items.
4. In the displayed dialog box, edit the managed software information, and then click **OK**.

The selected managed software information is updated.

> **Tip**
>
> You can also batch-edit hardware asset information by importing a CSV file. If you need to add a large amount of hardware asset information, we recommend that you export the hardware asset information into a CSV file, and then edit and import the CSV file.
>
> You can also batch-edit managed software information by importing a CSV file. If you need to edit a large amount of hardware asset information, we recommend that you export the managed software information into a CSV file, and then edit and import the CSV file.

Related Topics:

- 11.2.1 Adding managed software information
- 11.2.3 Removing managed software information
- 11.4.3 Importing managed software information
- 11.5 Exporting asset information

11.2.3 Removing managed software information

You can remove the managed software information that is no longer needed.

Note that when managed software is removed, its association with software license information is also removed.

To remove managed software information:

1. Display the Assets module.
2. In the menu area, select **Managed Software** and then **Managed Software List**.
3. In the information area, select the managed software information that you want to remove, and the select **Remove Managed Software** from **Action**.
   You can batch-remove managed software information by selecting multiple items.
4. In the displayed dialog box, click **OK**.

The selected managed software information is removed.

Related Topics:

- 11.2.1 Adding managed software information
- 11.2.2 Editing managed software information
- 11.4.3 Importing managed software information
- 11.5 Exporting asset information

11.2.4 Adding software license information

Select **Software License** in the Assets module, and then you can add software license information to the list in the **Software License** view. Also, by associating contract information with software license information, you can check the costs generated from asset operation on the **Software License Costs** report displayed in the report view.

To add software license information:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, enter the software license information, and then click **OK**.

> **Tip**
>
> To add the information of more than one software license, click the **Save/Add** button.

The software license information is added and displayed in the software license list.

> **Tip**
>
> You can also batch-add software license information by importing a CSV file. We recommend that you create and import a CSV file if you need to add a large amount of software license information.

In addition, you can know if there is an insufficient number of software licenses and identify the computers on which software is being illegally used, by assigning software licenses to computers and adding the corresponding software license information. The relevant information can be displayed in the **Software (License Violation)** panel by selecting **Overview** and then **Dashboard**.

Related Topics:

- 11.2.5 Editing software license information
- 11.2.6 Removing software license information
- 11.2.8 Changing a license status
- 11.2.9 Changing the planned license status
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.2.5 Editing software license information

When the number of licenses, license status, or computer allocation of the software licenses is changed, you can edit the software license information.

To edit software license information:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, select the software license information that you want to edit, and then click the **Edit** button.
   You can batch-edit software license information by selecting multiple items.
4. In the displayed dialog box, edit the software license information, and then click **OK**.

The selected software license information is updated.

If you want to transfer some of the software licenses from one department to another, edit the software license information of the department that currently holds the licenses and of the department that is to receive the licenses, as follows:

1. From the number of software licenses held by the department that currently holds the licenses, deduct the number of licenses to be transferred.
2. To the number of licenses held by the department that is to receive the licenses, add the number of licenses you deducted in step 1.
   If the receiving department does not have any software license information, add software license information for that department.

Tip

You can also edit software license information by importing a CSV file. If you need to edit a large amount of software license information, we recommend that you export the software license information into a CSV file, and then edit and import the CSV file.

Tip

To change the license status only, you can also click the **Change Status** button and then edit in the displayed dialog box.

Tip

To change the **planned license status** and **planned date** only, you can also select **Change License Status (Planned)** from **Action** and then make changes from the displayed dialog box.

Related Topics:

- 11.2.4 Adding software license information
- 11.2.6 Removing software license information
- 11.2.8 Changing a license status

- 11.2.9 Changing the planned license status
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.2.6 Removing software license information

You can remove the software license information that is no longer needed. You can remove software license information only if its license status is **Expired**. Therefore, change the license status to **Expired** before removing the software license information.

Note that when software license information is removed, its association with managed software information and contact information is also removed.

To remove software license information:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, select the software license information that you want to remove, and then select **Remove Software Licenses** from **Action**.
   You can batch-remove software license information by selecting multiple items.
4. In the displayed dialog box, click **OK**.

The selected software license information is removed.

Related Topics:

- 11.2.4 Adding software license information
- 11.2.5 Editing software license information
- 11.2.8 Changing a license status
- 11.2.9 Changing the planned license status
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.2.7 Adding a license status

You can add an item to **License Status**. By doing so, you can match the management of license statuses to the operation being performed.

To add a license status:

1. Display the **Asset Field Definitions** view in the Settings module.
2. In **Custom Fields (Software License)**, click the **Edit** button in **License Status**.
3. In the **Edit Custom Filds** dialog box, click the **Add** button.

4. In the **Add New Item** dialog box, enter the item name, and then click **OK**.
5. In the **Edit Custom Filds** dialog box, click **OK**.

The license status item is added. Note that you can add up to 100 items that are different from the default.

In the **Edit Custom Filds** dialog box, you can edit, remove, or sort the existing items.

Tip

You cannot edit or remove the default items (**In Use** and **Expired**).

Tip

You can also add a license status by selecting **Add New** when setting the software license information.

11.2.8 Changing a license status

To change the license status, in addition to the **Edit Software License** dialog box, you can also use the **Change License Status** dialog box.

To change the license status:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, select the software license information whose **license status** you want to change, and then click the **Change Status** button.
   You can also batch-change software license information by selecting multiple items.
4. In the displayed dialog box, change the **license status**, and then click **OK**.
   If you select **Add Notes**, information such as the license statuses before and after the change, the date of change, and reasons for change can be recorded. The information entered here will be added to the **Notes** tab.

The **license status** of the selected software license information is updated.

Tip

To edit another item, click the **Edit** button, and then edit in the displayed dialog box.

Related Topics:

- 11.2.4 Adding software license information
- 11.2.5 Editing software license information
- 11.2.6 Removing software license information
- 11.2.9 Changing the planned license status
- 11.4.2 Importing software license information

11.2.9 Changing the planned license status

To change the planned license status, in addition to the **Edit Software License** dialog box, you can also use the **Change License Status (Planned)** dialog box.

For example, for a software license that will expire, you can change the **planned license status**, so that the software license will be disposed of on the planned date.

To change the planned license status:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, select the software license information whose **planned license status** you want to change, and then select from **Change License Status (Planned)** from **Action**.
   You can batch-change the software license information by selecting multiple items.
4. In the displayed dialog box, change the **planned license status** and **planned date**, and then click **OK**.
   If you select **Add Notes**, information such as the license statuses before and after the change, the date of change, and reasons for change can be recorded. The information entered here will be added to the **Notes** tab.

The **planned license status** and **planned date** of the selected software license information are updated.

> **Tip**
>
> To edit another item, click the **Edit** button, and then edit in the displayed dialog box.

Related Topics:

- 11.2.4 Adding software license information
- 11.2.5 Editing software license information
- 11.2.6 Removing software license information
- 11.2.8 Changing a license status
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.2.10 Manually updating a stocktaking date

You can manually update the **stocktaking dates** for the hardware asset information and software license information. We recommend that you take stock individually of small-quantity assets nearby.

To manually update a stocktaking date:

1. Display the Assets module.
2. From **Hardware Asset** or **Software License** in the menu area, select the group that contains the asset information whose **stocktaking date** needs to be updated.

3. In the information area, select the asset information whose **stocktaking date** needs to be updated, and then select **Update Tracked Date (Directly)** from **Action**.
   You can batch update asset information by selecting multiple items.

4. In the displayed dialog box, enter the stocktaking date, and then click **OK**.
   If you select **Add Notes**, information such as the stocktaking date, stocktaking method, and reasons for stocktaking can be recorded. The information entered here will be added to the **Notes** tab.

The **stocktaking date** for the selected asset information is updated.

Tip

You can also batch update **stocktaking dates** by using a CSV file that contains the **asset numbers** or **license numbers**.

Tip

For hardware asset information, you can set the stocktaking date to be automatically updated. JP1/IT Desktop Management determines whether a device exists from the network connection of the device or the data entry of the device user. When the existence of the device is confirmed, the stocktaking date is automatically updated.

Tip

You can also batch update **stocktaking dates** by importing the hardware asset information or software license information.

Related Topics:

- 11.1.9 Batch updating stocktaking dates by using a CSV file
- 11.1.10 Setting automatic update for the stocktaking date
- 11.4.1 Importing hardware asset information
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.2.11 Batch updating stocktaking dates by using a CSV file

You can use a CSV file to batch-update the **stocktaking dates** of the hardware asset information and software license information.

We recommend this method if you use bar codes, instead of JP1/IT Desktop Management, to manage asset numbers. Export the information read by a barcode reader into a CSV file. The CSV file must be in the either of the following:

For hardware asset information

The **asset number** list of the hardware asset information whose **stocktaking date** needs to be updated

For software license information

The **license number** list of the software license information whose **stocking date** needs to be updated

To batch-update the stocktaking dates by using a CSV file:

1. Display the Assets module.
2. From **Hardware Asset** or **Software License** in the menu area, select the group that contains the asset information whose **stocktaking date** needs to be updated.
3. From **Action**, select **Update Tracked Date (from CSV)**.
4. In the displayed dialog box, click the **Select** button, and then specify the CSV file that was created in advance.
   You can download a sample of the CSV file by clicking the link of **Download CSV Sample File**.
5. Enter the stocktaking date, and then click **OK**.
   If you select **Add Notes**, information such as the stocktaking date, stocktaking method, and reasons for stocktaking can be recorded. The information entered here will be added to the **Notes** tab.

The **stocktaking dates** of the asset information corresponding to the **asset numbers** and **license numbers** that are contained in the CSV file are updated in a batch.

Important note

If an error occurs when updating the stocktaking date, an asset which is not managed by JP1/IT Desktop Management exists. Check the asset numbers, and register the unmanaged asset.

Tip

For hardware asset information, you can set the stocktaking date to be automatically updated. JP1/IT Desktop Management determines whether a device exists from the network connection of the device or the data entry of the device user. When the existence of the device is confirmed, the stocktaking date is automatically updated.

Tip

You can also batch update the stocktaking dates by importing the hardware asset information and software license information. In this case, you can set a different stocktaking date for the information of each asset.

Related Topics:

- 11.1.11 Taking stock by using a barcode reader
- 11.1.8 Manually updating a stocktaking date
- 11.1.10 Setting automatic update for the stocktaking date
- 11.4.1 Importing hardware asset information
- 11.4.2 Importing software license information
- 11.5 Exporting asset information

11.2.12 Allocating software licenses to computers

You can allocate software licenses to the computers that have permissions to use the software.

When the managed software information is registered, you can know if there is an insufficient number of software licenses and identify the computers on which software is being illegally used. The relevant information can also be displayed in the **Software (License Violation)** panel by selecting **Overview** and then **Dashboard**.

To allocate software licenses to computers:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, select the software license that you want to allocate, and then select **Assign Computer** from **Action**.
   You can batch-allocate more than one software license by selecting multiple items.
4. In the displayed dialog box, select the computers to which you want to allocate the software license, and then click **OK**.

The software license is allocated to the selected computers.

On the **Licensed Computers** tab of the **Managed Software** view, you can view the information about the computers to which the software is allocated. If you select **Show Only Computers Not Installed**, the computers which the license has already been allocated to, but the software has not yet been installed on are displayed.

On the **Installed Computers** tab of the **Managed Software** view, you can view the information about the computers to which the software is allocated. If you select **Show Only Computers Not Licensed**, the computers which the license has not yet been allocated to, but the software has already been installed on are displayed.

Tip

On the **Assigned Computers** tab of the **Software Licenses** view, you can add computers to allocate software licenses.

Tip

You can also add computers to more allocate software licenses by using **Assign Computers** in the dialog box for adding or editing software license information.

Related Topics:

- 11.2.4 Adding software license information
- 11.2.1 Adding managed software information

11.2.13 Transferring software licenses

You can transfer software licenses that have already been allocated to a device to another device.The types of devices between which you can transfer software licenses are PCs, servers, printers, network devices, and unknown devices.

When a device is replaced, you can transfer the software licenses that were allocated to the old device to a new device. You can also batch-transfer all software licenses that are allocated to multiple devices, so the transfer operation is simple.

Important note

If the same type of the software license is already allocated to the destination device, the software license cannot be transferred. In this case, remove the allocation of the software license from the destination device first.

To transfer software licenses:

1. Display the Device module.
2. In the Device module, select the source device from which you want the software licenses to be transferred.
3. From **Action**, select **Move Software Licenses**.
4. In the displayed dialog box, select the destination device, and then click **OK**.

The software licenses are transferred to the selected device. The allocation of the software licenses is removed from the source device.

11.2.14 Associating the contract information with a software license

To manage the trends of the contract costs and contract types of software licenses, you can associate contract information with software licenses.

For details about how to create contract information, see 11.3.1 Adding contract information.

To associate contract information with a software license:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. In the information area, select the software license information for which you want to set contract information, and then click the **Edit** button.
4. In the displayed dialog box, click the **Change** button on the **Contract Information** tab.
5. In the displayed dialog box, select the contract information, and then click **OK**.
6. Click **OK**.

The contract information is associated with the software license.

Related Topics:

- 11.3.7 Linking software licenses (contract)

11.3 Using contract information

11.3.1 Adding contract information

You can add contract information to the list in the **Contract List** view, which can be selected from **Contract** in the Assets module. Adding contract information allows you to check information about contracts that require a renewal. To check the information, from **Summary**, select the **Dashboard** view and then **Expired Contracts(next 3 months)**.

In addition, linking hardware assets or software licenses, for which a contract is made, with contract information allows you to check the asset management cost in **Hardware Assets Cost** reports or **Software License Cost** reports in the Reports module.

To add contract information:

1. Display the Assets module.
2. In the menu area, select **Contract** and then **Contract List**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, enter the contract information, and then click **OK**.

The contract information is added and displayed in the contract list.

> **Tip**
>
> You can add contract information for multiple items at one time by importing a CSV file. If there is a lot of contract information to be added, we recommend that you create a CSV file and import it.

Related Topics:

- 11.3.2 Editing contract information
- 11.3.3 Deleting contract information
- 11.3.5 Changing the contract status
- 11.4.4 Importing contract information
- 11.5 Exporting asset information

11.3.2 Editing contract information

You can edit contract information. Edit contract information if a contract period or contract status changes, or if you want to change the assets for which a contract is made.

To edit contract information:

1. Display the Assets module.
2. In the menu area, select **Contract** and then **Contract List**.
3. In the information area, select the contract information that you want to edit, and then click the **Edit** button.

To edit contract information for multiple items at one time, select multiple contract information items.

4. In the displayed dialog box, edit the contract information, and then click **OK**.

The selected contract information is updated.

> **Tip**
>
> You can edit contract information by importing a CSV file. If there is a lot of contract information to be edited, we recommend that you export contract information to a CSV file, edit the information, and then import the file.

> **Tip**
>
> To change only **Contract Status**, click the **Change Status** button, and then edit the information in the displayed dialog box.

Related Topics:

- 11.3.1 Adding contract information
- 11.3.3 Deleting contract information
- 11.3.5 Changing the contract status
- 11.4.4 Importing contract information
- 11.5 Exporting asset information

11.3.3 Deleting contract information

You can remove contract information that no longer needs to be managed. Contract information can be removed only when the contract status is **Canceled** or **Expired**.

Note that if you remove contract information, a link with hardware asset information or software license information is also removed.

To remove contract information:

1. Display the Assets module.
2. In the menu area, select **Contract** and then **Contract List**.
3. In the information area, select the contract information that you want to remove, and then select **Remove Contracts** from **Action**.
   To remove multiple items of contract information at one time, select multiple contract information items.
4. In the displayed dialog box, click **OK**.

The selected contract information is removed.

Related Topics:

- 11.3.1 Adding contract information

- 11.3.2 Editing contract information
- 11.3.5 Changing the contract status
- 11.4.4 Importing contract information
- 11.5 Exporting asset information

11.3.4 Adding items to the contract status

You can add any items to **Contract Status**. This allows you to manage the contract status according to your operations.

To add items to the contract status:

1. Display the **Asset Field Definitions** view from the Settings module.
2. In **Custom Fields (Contracts)**, click the **Edit** button for **Contract Status**.
3. In the **Edit Custom Filds** dialog box, click the **Add** button.
4. In the **Add New Item** dialog box, enter an item name, and then click **OK**.
5. In the **Edit Custom Filds** dialog box, click **OK**.

An item for the contract status is added. Note that you can add a maximum of 100 items to the contract status, excluding the default items.

In the **Edit Custom Filds** dialog box, you can edit or remove existing items, or change the sort order of items.

Tip

You cannot edit or remove the default items (Active, Canceled, and Expired). In addition, among the contract status items added by a system administrator, the items saved as filter conditions cannot be removed either.

Tip

You can also add items to the contract status by selecting **(Add New One)** when setting contract information.

11.3.5 Changing the contract status

You can change **Contract Status** in either the **Edit Contract** dialog box or the **Change Contract Status** dialog box.

To change the contract status:

1. Display the Assets module.
2. In the menu area, select **Contract** and then **Contract List**.
3. In the information area, select the contract information for which you want to change **Contract Status**, and then click the **Change Status** button.
   To change the contract status for multiple items at one time, select multiple contract information items.

4. In the displayed dialog box, change the items in **Contract Status**, and then click **OK**.

The items in **Contract Status** for the selected contract information are updated.

> **Tip**
>
> To change other items, click the **Edit** button, and then edit the items in the displayed dialog box.

Related Topics:

- 11.3.1 Adding contract information
- 11.3.2 Editing contract information
- 11.3.3 Deleting contract information
- 11.4.4 Importing contract information
- 11.5 Exporting asset information

11.3.6 Linking hardware assets (contract)

Linking contract information with hardware asset information allows you to manage the hardware assets for which contracts are made. It also allows you to manage the contract cost or contract type of hardware assets.

To link hardware assets:

1. Display the Assets module.
2. In the menu area, select **Contract** and then **Contract List**.
3. In the information area, select the contract information for which you want to specify hardware assets.
4. Select the **Hardware Asset** tab displayed at the bottom of the view.
5. Click the **Change** button in the tab.
6. In the displayed dialog box, select the hardware asset information that you want to link with contract information, and then click **OK**.

The hardware asset information is linked with the selected contract information.

> **Tip**
>
> You can also link hardware asset information in **Associated Information** in the dialog box for adding or editing contract information.

Related Topics:

- 11.1.12 Associating contract information with hardware asset information

11.3.7 Linking software licenses (contract)

Linking contract information with software license information allows you to manage the software licenses for which contracts are made. It also allows you to manage the contract cost or contract type of software licenses.

To link software licenses:

1. Display the Assets module.
2. In the menu area, select **Contract** and then **Contract List**.
3. In the information area, select the contract information for which you want to specify software licenses.
4. Select the **Software License** tab displayed at the bottom of the view.
5. Click the **Change** button in the tab.
6. In the displayed dialog box, select the software license information that you want to link with contract information, and then click **OK**.

The software license information is linked with the selected contract information.

> **Tip**
>
> You can also link software license information in **Associated Information** in the dialog box for adding or editing contract information.

Related Topics:

- 11.2.14 Associating the contract information with a software license

11.4 Importing asset information

11.4.1 Importing hardware asset information

Importing hardware asset information in a CSV file allows you to add or collectively edit hardware asset information.

You can import hardware asset information by using the **Import Assets** wizard.

> **Tip**
>
> You can also import hardware asset information by executing the `ioutils importasset` command. We recommend that you use this command if you need to regularly import hardware asset information from CSV files.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management after the CSV file is uploaded. In addition, the wizard specifies a key (mapping key) that is used to check whether the information to be imported corresponds to any existing information. After import settings are complete, check the settings, and if there are no problems, import the information.

To import hardware asset information:

1. Display the Assets module.
2. In the menu area, from **Hardware Asset Information**, select any group.
3. Select **Import Hardware Asset List** from **Action**, and then start the Import Assets wizard.
4. In the **What is this Wizard?** view, check the import procedure, and then click the **Next** button.
5. In the **Upload CSV file** view, specify a CSV file that you want to import, and then click the **Next** button.
   You can download a sample CSV file from this view. Use it as a reference when creating a CSV file.
6. In the **Map Fields** view, specify **Mapping Key**, **CSV Fields**, **Header Line**, and **Import Starting Line**, and then click the **Next** button.
   You can also select a template that has already been created from **Template Name**.
7. In the **Save Template** dialog box, specify the template name and description, and then click the **Yes** button.
   If you do not want to save the template, click the **No** button.
8. In the **Confirm Settings** view, check the settings, and then click the **Import** button.
   If part of the data fails to be imported, details are displayed in **Check Result Details**. Before importing the data again, we recommend that you first modify the CSV file by checking **Check Result Details**, and then upload the CSV file again by clicking the **Upload and Pre-Check CSV File** button. To output the results of the check, click the **Export** button.
9. In the **Complete** view, check the import results, and then click the **Close** button.

The data in the CSV file is imported. To check the import status, click the **Go to Last Import Log** button.

Check whether the imported information is correctly registered. If an incorrect record exists, modify the CSV file, and then import the information again.

Tip

You can also start the **Import Assets** wizard from the Settings module by selecting **Asset management** and then **Last Import Log**. If you started the wizard from the Settings module, in the **Upload CSV file** view, specify **Hardware Asset Information** for **Asset Type**.

Related Topics:

- 11.5 Exporting asset information
- 17.4 ioutils exportasset (Exporting hardware asset information)
- 17.5 ioutils importasset (Importing hardware asset information)
- 17.8 ioutils exporttemplate (exporting template)
- 17.9 ioutils importtemplate (importing a template)

11.4.2 Importing software license information

Importing software license information in a CSV file allows you to add or collectively edit software license information.

You can import software license information by using the **Import Assets** wizard.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management after the CSV file is uploaded. In addition, the wizard specifies a key (mapping key) that is used to check whether the information to be imported corresponds to any existing information. After import settings are complete, check the settings, and if there are no problems, import the information.

To import software license information:

1. Display the Assets module.
2. In the menu area, select **Software License** and then **Software License List**.
3. Select **Import Software License List** from **Action**, and then start the Import Assets wizard.
4. In the **What is this Wizard?** view, check the import procedure, and then click the **Next** button.
5. In the **Upload CSV file** view, specify a CSV file that you want to import, and then click the **Next** button.
   You can download a sample CSV file from this view. Use it as a reference when creating a CSV file.
6. In the **Map Fields** view, specify **Mapping Key**, **CSV Fields**, **Header Line**, and **Import Starting Line**, and then click the **Next** button.
   You can also select a template that has already been created from **Template Name**.
7. In the **Save Template** dialog box, specify the template name and description, and then click the **Yes** button.
   If you do not want to save the template, click the **No** button.
8. In the **Confirm Settings** view, check the settings, and then click the **Import** button.
   If part of the data fails to be imported, details are displayed in **Check Result Details**. Before importing the data again, we recommend that you first modify the CSV file by checking **Check Result Details**, and then upload the CSV file again by clicking the **Upload and Pre-Check CSV File** button. To output the results of the check, click the **Export** button.

9. In the **Complete** view, check the import results, and then click the **Close** button.

The data in the CSV file is imported. To check the import status, click the **Go to Last Import Log** button.

Check whether the imported information is correctly registered. If an incorrect record exists, modify the CSV file, and then import the information again.

After the information is imported, specify the managed software information that corresponds to software licenses. This allows you to check the status of software licenses.

Tip

You can also start the **Import Assets** wizard from the Settings module by selecting **Asset management** and then **Last Import Log**. If you started the wizard from the Settings module, in the **Upload CSV file** view, specify **Software License Information** for **Asset Type**.

Related Topics:

- 11.5 Exporting asset information
- 17.8 ioutils exporttemplate (exporting template)
- 17.9 ioutils importtemplate (importing a template)

11.4.3 Importing managed software information

Importing managed software information in a CSV file allows you to add or collectively edit managed software information.

You can import managed software information by using the **Import Assets** wizard.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management after the CSV file is uploaded. In addition, the wizard specifies a key (mapping key) that is used to check whether the information to be imported corresponds to any existing information. After import settings are completed, check the settings, and if there are no problems, import the information.

To import managed software information:

1. Display the Assets module.
2. In the menu area, select **Managed Software** and then **Managed Software List**.
3. Select **Import Managed Software List** from **Action**, and then start the Import Assets wizard.
4. In the **What is this Wizard?** view, check the import procedure, and then click the **Next** button.
5. In the **Upload CSV file** view, specify a CSV file that you want to import, and then click the **Next** button.
   You can download a sample CSV file from this view. Use it as a reference when creating a CSV file.
6. In the **Map Fields** view, specify **Mapping Key**, **CSV Fields**, **Header Line**, and **Import Starting Line**, and then click the **Next** button.
   You can also select a template that has already been created from **Template Name**.
7. In the **Save Template** dialog box, specify the template name and description, and then click the **Yes** button.

If you do not want to save the template, click the **No** button.

8. In the **Confirm Settings** view, check the settings, and then click the **Import** button.
   If part of the data fails to be imported, details are displayed in **Check Result Details**. Before importing the data again, we recommend that you first modify the CSV file by checking **Check Result Details**, and then upload the CSV file again by clicking the **Upload and Pre-Check CSV File** button. To output the results of the check, click the **Export** button.

9. In the **Complete** view, check the import results, and then click the **Close** button.

The data in the CSV file is imported. To check the import status, click the **Go to Last Import Log** button.

Check whether the imported information is correctly registered. If an incorrect record exists, modify the CSV file, and then import the information again.

After importing the information, edit the managed software information to specify **Installed Software - Name** and **Target Software Licenses**. This allows you to check the status of software licenses.

Tip

You can also start the **Import Assets** wizard from the Settings module by selecting **Asset management** and then **Last Import Log**. If you started the wizard from the Settings module, in the **Upload CSV file** view, specify **Managed Software Information** for **Asset Type**.

Related Topics:

- 11.5 Exporting asset information
- 17.8 ioutils exporttemplate (exporting template)
- 17.9 ioutils importtemplate (importing a template)

11.4.4 Importing contract information

Importing contract information in a CSV file allows you to add or collectively edit the contract information.

You can import contract information by using the **Import Assets** wizard.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management after the CSV file is uploaded. In addition, the wizard specifies a key (mapping key) that is used to check whether the information to be imported corresponds to any existing information. After import settings are complete, check the settings, and if there are no problems, import the information.

To import contract information:

1. Display the Assets module.

2. In the menu area, select **Contract** and then **Contract List**.

3. Select **Import Contract List** from **Action**, and then start the Import Assets wizard.

4. In the **What is this Wizard?** view, check the import procedure, and then click the **Next** button.

5. In the **Upload CSV file** view, specify a CSV file that you want to import, and then click the **Next** button.

You can download a sample CSV file from this view. Use it as a reference when creating a CSV file.

6. In the **Map Fields** view, specify **Mapping Key**, **CSV Fields**, **Header Line**, and **Import Starting Line**, and then click the **Next** button.
   You can also select a template that has already been created from **Template Name**.
7. In the **Save Template** dialog box, specify the template name and description, and then click the **Yes** button.
   If you do not want to save the template, click the **No** button.
8. In the **Confirm Settings** view, check the settings, and then click the **Import** button.
   If part of the data fails to be imported, details are displayed in **Check Result Details**. Before importing the data again, we recommend that you first modify the CSV file by checking **Check Result Details**, and then upload the CSV file again by clicking the **Upload and Pre-Check CSV File** button. To output the results of the check, click the **Export** button.
9. In the **Complete** view, check the import results, and then click the **Close** button.

The data in the CSV file is imported. To check the import status, click the **Go to Last Import Log** button.

Check whether the imported information is correctly registered. If an incorrect record exists, modify the CSV file, and then import the information again.

Tip

You can also start the **Import Assets** wizard from the Settings module by selecting **Asset management** and then **Last Import Log**. If you started the wizard from the Settings module, in the **Upload CSV file** view, specify **Contact information** for **Asset Type**.

Related Topics:

- 11.5 Exporting asset information
- 17.8 ioutils exporttemplate (exporting template)
- 17.9 ioutils importtemplate (importing a template)

11.4.5 Importing a contract vendor list

Importing a contract vendor list in a CSV file allows you to add contract vendor information or collectively edit the contract vendor list.

You can import a contract vendor list by using the **Import Assets** wizard.

The **Import Assets** wizard relates items in a CSV file to items managed in JP1/IT Desktop Management after the CSV file is uploaded. In addition, the wizard specifies a key (mapping key) that is used to check whether the information to be imported corresponds to any existing information. After import settings are complete, check the settings, and if there are no problems, import the information.

To import a contract vendor list:

1. In the Settings module, select **Asset management** and then **Contract Vendor List**.
2. Select **Import Contract Vender List** from **Action**, and then start the Import Assets wizard.

3. In the **What is this Wizard?** view, check the import procedure, and then click the **Next** button.
4. In the **Upload CSV file** view, specify a CSV file that you want to import, and then click the **Next** button.
   You can download a sample CSV file from this view. Use it as a reference when creating a CSV file.
5. In the **Map Fields** view, specify **Mapping Key**, **CSV Fields**, **Header Line**, and **Import Starting Line**, and then click the **Next** button.
   You can also select a template that has already been created from **Template Name**.
6. In the **Save Template** dialog box, specify the template name and description, and then click the **Yes** button.
   If you do not want to save the template, click the **No** button.
7. In the **Confirm Settings** view, check the settings, and then click the **Import** button.
   If part of the data fails to be imported, details are displayed in **Check Result Details**. Before importing the data again, we recommend that you first modify the CSV file by checking **Check Result Details**, and then upload the CSV file again by clicking the **Upload and Pre-Check CSV File** button. To output the results of the check, click the **Export** button.
8. In the **Complete** view, check the import results, and then click the **Close** button.

The data in the CSV file is imported. To check the import status, click the **Go to Last Import Log** button.

Check whether the imported information is correctly registered. If an incorrect record exists, modify the CSV file, and then import the information again.

Tip

You can also start the **Import Assets** wizard from the Settings module by selecting **Asset management** and then **Last Import Log**. If you started the wizard from the Settings module, in the **Upload CSV file** view, specify **Contact Vendor List** for **Asset Type**.

Related Topics:

- 15.5.12 Exporting contract vendor lists
- 17.8 ioutils exporttemplate (exporting template)
- 17.9 ioutils importtemplate (importing a template)

11.5 Exporting asset information

You can export the asset information displayed in the information area of the Assets module to a CSV file.

To export only specific items of asset information, use filters.

For example, to export only the asset information for the General Affairs Department, use a filter to display asset information for which the **Department** level is set to **General Affairs Department**.

Tip

You can also export hardware asset information by executing the `ioutils exportasset` command. We recommend that you use this command if you need to regularly export asset information.

Tip

If a hyphen (-) is displayed in the information area of the **Hardware Asset** view in the Assets module, when hardware asset information is exported, the hyphen is output as a null character. This enables the exported hardware asset information to be successfully imported when imported without changes.

To export asset information:

1. Display the Assets module.
2. Display the asset information to be exported in the information area.
3. From **Action**, select **Export Hardware Asset List**.
4. In the **Select Export Columns** dialog box, select the items to export, and then click **OK**.
   To specify the character encoding for the exported CSV file, select a character encoding in **Encoding**. The character encoding is set to UTF-8 by default.
5. In the displayed view, click the **Save** button.

The CSV file is saved with the specified name in the location to which files are downloaded.

Related Topics:

- 17.4 ioutils exportasset (Exporting hardware asset information)

12 Software and File Distribution

This chapter describes software installation and uninstallation, as well as file distribution.

12.1 Installing software on the computers

You can use the **Install Software** wizard to distribute and install software on users' computers.

By using the **Install Software** wizard, you can create a package in which the software to be installed is registered and a task to distribute the package. When the wizard is complete, the package is distributed according to the schedule specified in the task.

To install the software on the computers:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, from **Action**, select **Launch Install Wizard** to start the wizard.
4. In the **What is this Wizard?** view, read the instruction, and then click the **Next** button.
5. In the **Select Software** view, select **Create New Package**, specify the files to be registered in the package, and then click the **Next** button.
   If you have created a package already, you can select it in this step.
6. In the **Specify Package** view, set the package information, and then click the **Next** button.
7. In the **Create Package Distribution Task** view, set the schedule to perform distribution and so on, and then click the **Next** button.
   By clicking **Execute Option**, you can specify option settings such as the installation timing, email message to notify the users, and so on.
8. In the **Select Target Computers** view, click the **Change** button.
9. In the **Select Target Computers** dialog box, select the computers on which the software is installed, and then click the **OK** button.
10. Click the **Next** button.
11. In the **Confirm Settings** view, check the settings, and then click the **Complete** button.
12. In the **Distribution Settings Configure**d view, click the **Close** button.

The software is distributed and installed on the specified target computers according to the schedule specified in the task. You can view the execution status of the task in the **Tasks** view of the Distribution module.

> **Tip**
>
> The users can change the schedule to execute the installation later if more urgent or important operation is in progress on their computers.

Related Topics:

- 12.6 Postponing downloads and installation as a user
- 12.5.5 Stopping tasks

12.2 Distributing files to the computers

You can use the **File Distribution** wizard to distribute files to users' computers.

By using the **File Distribution** wizard, you can create a package in which the files to be distributed are registered and a task to distribute the package. When the wizard is complete, the package is distributed according to the schedule specified in the task.

To distribute the files to the computers:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, from **Action**, select **Launch File Distribution Wizard** to start the wizard.
4. In the **What is this Wizard?** view, read the instruction, and then click the **Next** button.
5. In the **Select File** view, select **Create New Package**, specify the files to be registered in the package, and then click the **Next** button.
   If you have created a package already, you can select it in this step.
6. In the **Specify Package** view, set the package information, and then click the **Next** button.
7. In the **Create Package Distribution Task** view, set the schedule to perform distribution and so on, and then click the **Next** button.
   By clicking **Execute Option**, you can specify option settings such as the timing to distribute the files after the package distribution, email message to notify the users, and so on.
8. In the **Select Target Computers** view, click the **Change** button.
9. In the **Select Target Computers** dialog box, select the computers to which the files are distributed, and then click the **OK** button.
10. Click the **Next** button.
11. In the **Confirm Settings** view, check the settings, and then click the **Complete** button.
12. In the **Distribution Settings Configured** view, click the **Close** button.

The files are distributed to the specified target computers according to the schedule specified in the task. You can view the execution status of the task in the **Task List** view of the Distribution module.

> **Tip**
>
> The users can change the schedule to execute the file distribution later if more urgent or important operation is in progress on their computers.

Related Topics:

- 12.6 Postponing downloads and installation as a user
- 12.5.5 Stopping tasks

12.3 Uninstalling software from a computer

You can uninstall software from a user computer by using the **Uninstall Software** wizard.

The **Uninstall Software** wizard creates tasks to uninstall software. After the completion of the wizard, the uninstallation tasks are executed according to the specified schedule.

To uninstall software from a computer:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. To start the wizard, in the information area, select **Launch Uninstall Wizard** from **Action**.
4. In the **What is this Wizard?** view, check the wizard procedure, and then click the **Next** button.
5. In the **Create Uninstallation Task** view, specify information about the software to be uninstalled and the task execution schedule, and then click the **Next** button.
   To specify the time at which to execute the uninstallation or messages to be sent to the user, click **Execute Option**.
6. In the **Select Target Computers** view, click the **Change** button.
7. In the **Select Target Computers** dialog box, specify the computer from which you want to uninstall software, and then click **OK**.
8. Click the **Next** button.
9. In the **Confirm Settings** view, check the settings, and then click the **Complete** button.
10. In the **Complete** view, click the **Close** button.

Software is uninstalled from the specified computer according to the scheduled tasks that were created. You can check the status of task execution in the **Task List** view of the Distribution module.

> **Tip**
>
> You can postpone software uninstallation to avoid executing it during urgent or important jobs. For details, see 12.6 Postponing downloads and installation as a user.

Related Topics:

- 12.5.5 Stopping tasks

12.4 Managing packages

12.4.1 Adding packages

You can add packages in which software or files are registered to the list in the **Packages** view of the Distribution module.

Distributing packages allows you to install software on and distribute files to target computers. To distribute packages, you need to create corresponding tasks. For details about how to create tasks, see 12.5.1 Adding tasks.

To add packages:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, type the package information, and then click **OK**.

Packages are added and displayed in the Package List.

Related Topics:

- 12.4.2 Editing packages
- 12.4.3 Removing packages
- 12.4.4 Exporting package information

12.4.2 Editing packages

You can edit registered packages. You can change package descriptions, expansion folders, or destination folders by editing packages.

To edit packages:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, click the **Edit** button of the package that you want to edit.
4. In the displayed dialog box, edit the package information, and then click **OK**.

The selected package is updated.

Related Topics:

- 12.4.1 Adding packages
- 12.4.3 Removing packages
- 12.4.4 Exporting package information

12.4.3 Removing packages

You can remove unused packages.

> **Important note**
>
> Packages that are specified for tasks cannot be removed. To remove packages specified for tasks, in the **Tasks** tab in the **Package list** view, stop all related tasks, remove those tasks in the **Task List** view, and then remove the packages.

To remove packages:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. In the information area, select the packages that you want to remove, and then select the **Remove** button.
   To remove multiple packages at one time, select multiple packages.
4. In the displayed dialog box, click **OK**.

The selected packages are removed.

Related Topics:

- 12.4.1 Adding packages
- 12.4.2 Editing packages
- 12.4.4 Exporting package information

12.4.4 Exporting package information

You can export (batch output) the package information displayed in the information area of the Distribution module to a CSV file.

To export only specific items of package information, use a filter.

For example, to export only the file distribution package information, use a filter to display only the package information for which **Package Type** is set to **File Distribution**.

To export package information:

1. Display the Distribution module.
2. In the menu area, select **Packages** and then **Package List**.
3. Display the package information to be exported in the information area.
4. Select **Export Package List** from **Action**.
5. In the displayed dialog box, select the items that you want to export, and then click **OK**.
   To specify the character encoding for the exported CSV file, select a character encoding in **Encoding**. The character encoding is set to UTF-8 by default.

6. In the displayed view, click the **Save** button.

The CSV file is saved with the specified name in the location to which files are downloaded.

Related Topics:

- 12.4.1 Adding packages
- 12.4.2 Editing packages
- 12.4.3 Removing packages

12.5 Managing tasks

12.5.1 Adding tasks

You can add tasks to the list in the **Tasks** view in the Distribution module. Adding tasks allows you to install software on, distribute files to, or uninstall software from target computers.

Note that to create package distribution tasks, you need to create in advance packages in which software or files to be distributed are registered. For details about how to create packages, see 12.4.1 Adding packages.

To add tasks:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, click the **Add Package Distribution Task** or **Add Uninstallation Task** button.
4. In the displayed dialog box, type the task information, and then click **OK**.

Tasks are added and displayed in the Package List.

Tip

Tasks executed by Auto Enforce are created when Auto Enforce for Windows Update, mandatory software, or prohibited software are set in the Security Policy.

Tip

Uninstallation tasks can also be created by setting prohibited software in the **Software Details** view in the Device module.

Tip

To add a task based on a task that is already registered, copy the registered task.

Related Topics:

- 6.20 Setting unauthorized software
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.4 Removing tasks
- 12.5.6 Re-executing tasks
- 12.5.5 Stopping tasks
- 12.5.7 Exporting task information

12.5.2 Editing tasks

You can edit registered tasks. You can change the execution schedule or add target computers by editing tasks.

To edit tasks:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, click the **Edit** button of the task that you want to edit.
4. In the displayed dialog box, edit the task information, and then click **OK**.

The selected task is updated.

> **Tip**
>
> To add a task based on a task that is already registered, copy the registered task.

Note that tasks that are executed by Auto Enforce cannot be edited.

Related Topics:

- 12.5.1 Adding tasks
- 12.5.3 Copying tasks
- 12.5.4 Removing tasks
- 12.5.6 Re-executing tasks
- 12.5.5 Stopping tasks
- 12.5.7 Exporting task information

12.5.3 Copying tasks

You can copy and edit the registered tasks. To add a task based on a task that is already registered, copy the registered task.

For example, when distributing packages over a period of several days because there are many target computers, you can edit the execution schedule and target computers for the registered tasks to add new tasks.

To copy tasks:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, click the **Copy** button of the task that you want to copy.
4. In the displayed dialog box, edit the task information, and then click **OK**.

New tasks are added and displayed in the Package List.

Note that tasks that are executed by Auto Enforce cannot be copied.

Related Topics:

- 12.5.1 Adding tasks
- 12.5.2 Editing tasks
- 12.5.4 Removing tasks
- 12.5.6 Re-executing tasks
- 12.5.5 Stopping tasks
- 12.5.7 Exporting task information

12.5.4 Removing tasks

You can remove unnecessary tasks.

To remove tasks in progress, stop the tasks first, and then remove them. Note that tasks cannot be removed in the following cases, because the tasks cannot be stopped: Packages are distributed to a user computer, and processing for software installation, file distribution, or software uninstallation has started.

Important note

To delete tasks that are executed by Auto Enforce, cancel the Auto Enforce settings specified in **Software Use** for the Security Policy, and remove prohibited software or mandatory software. Tasks are automatically removed according to the Security Policy settings.

To remove tasks:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, select the tasks that you want to remove, and then from **Action**, select **Remove**.
   To remove multiple tasks at one time, select multiple tasks.
4. In the displayed dialog box, click **OK**.

The selected tasks are removed.

Related Topics:

- 12.5.1 Adding tasks
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.6 Re-executing tasks
- 12.5.5 Stopping tasks
- 12.5.7 Exporting task information

12.5.5 Stopping tasks

You can stop tasks for which the task status is not **Successful**, **Failed**, or **Cancel**.

> **Important note**
>
> Note that tasks cannot be stopped in the following cases: Packages are distributed to a user computer, and processing for software installation, file distribution, or software uninstallation has started.

To stop tasks:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, select the tasks that you want to stop, and then from **Action**, select **Stop**.
   To stop tasks multiple tasks at one time, select multiple tasks.
4. In the displayed dialog box, click **OK**.

Tasks are stopped.

To stop tasks by specifying a computer:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, select the tasks that you want to stop, and then display the **Task Status** tab.
4. In the tab, select a computer for which you want to stop tasks.
   To stop tasks for multiple computers at one time, select multiple computers.
5. Click the **Stop** button in the tab.
6. In the displayed dialog box, click **OK**.

Tasks are stopped.

Related Topics:

- 12.5.1 Adding tasks
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.4 Removing tasks
- 12.5.6 Re-executing tasks
- 12.5.7 Exporting task information

12.5.6 Re-executing tasks

If an attempt to execute or stop a task fails, the task can be re-executed.

You can re-execute tasks for a computer for which **Task Status** in the **Task Status** tab is either **Failed** or **Cancel**.

To re-execute tasks:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, select the tasks that you want to re-execute, and then from **Action**, select **Retry**.
   To re-execute multiple tasks at one time, select multiple tasks.
4. In the displayed dialog box, click **OK**.

Tasks are re-executed immediately.

To re-execute tasks by specifying a computer:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. In the information area, select the tasks that you want to re-execute, and display the **Task Status** tab.
4. In the tab, select a computer for which you want to re-execute tasks.
   To re-execute tasks in a batch for multiple computers, select multiple computers.
5. Click the **Retry** button in the tab.
6. In the displayed dialog box, click **OK**.

Tasks are re-executed immediately.

> **Important note**
>
> Tasks are immediately re-executed regardless of the execution schedule specified for them. If you want to re-execute tasks according to the specified execution schedule, edit or copy the tasks.

Related Topics:

- 12.5.1 Adding tasks
- 12.5.2 Editing tasks
- 12.5.3 Copying tasks
- 12.5.4 Removing tasks
- 12.5.5 Stopping tasks
- 12.5.7 Exporting task information

12.5.7 Exporting task information

You can export (batch output) the task information displayed in the information area of the Assets module to a CSV file.

To export only specific items of task information, use a filter.

For example, to export only the information about tasks created by an administrator, you can use a filter to display only the tasks for which **Task Type** is set to **On Demand Task**.

To export task information:

1. Display the Distribution module.
2. In the menu area, select **Tasks** and then **Task List**.
3. Display the task information to be exported in the information area.
4. Select **Export Task List** from **Action**.
5. In the displayed dialog box, select the items that you want to export, and then click **OK**.
   To specify the character encoding for the exported CSV file, select a character encoding in **Encoding**. The character encoding is set to UTF-8 by default.
6. In the displayed view, click the **Save** button.

The CSV file is saved with the specified name in the location to which files are downloaded.

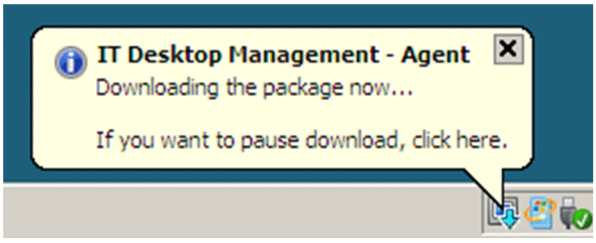
12.6 Postponing downloads and installation as a user

After packages are distributed to a computer, a user can choose to postpone package downloads or software installation. Postponing downloads or installation allows the user to avoid interrupting urgent or important jobs.

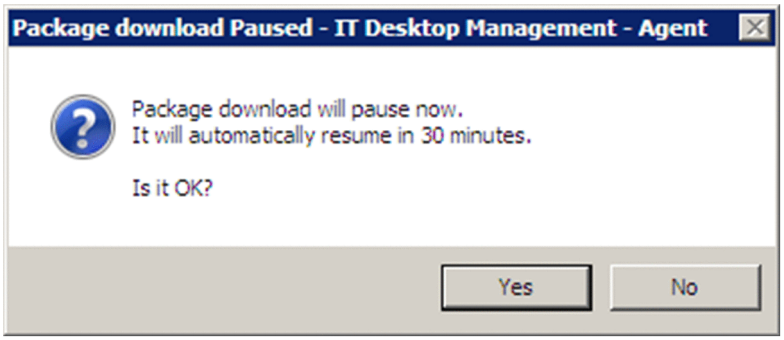
> **Tip**
>
> File distribution or uninstallation can also be postponed.

To postpone downloading:

When downloading of the distributed package starts, the icon and balloon hint shown below appear on the task bar of the user computer. However, the display of the balloon hint depends on the settings in the **Agent Basic Settings** view during agent setup.



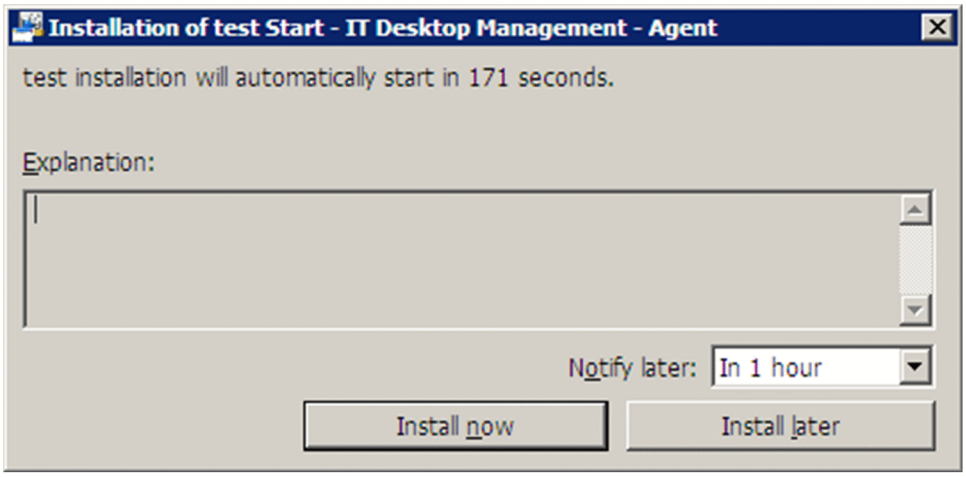
If you click the icon, a dialog box prompting you to temporarily stop package downloads appears.



To temporarily stop downloading, click the **Yes** button in the dialog box. Downloading resumes after a certain period of time elapses.

To postpone installation:

If you set the **Pre-execution Message** to appear when tasks are created, before installation starts, a dialog box appears on the user computer notifying the user of the start of installation.



To postpone software installation, click the **Install later** button in the dialog box. If you decide to postpone installation, the dialog box reappears after the time specified in the pull-down menu for **Notify later** elapses. You can select **In 10 minutes**, **In 30 minutes**, or **In 1 hour** as the time after which the dialog box reappears.

13 Event Reference

This section describes how to reference events that are output by JP1/IT Desktop Management.

13.1 Viewing event details

Viewing event details allows you to check event descriptions or make use of event information by, for example, copying it to the clipboard.

To display event details:

1. Display the Events module.
2. From **Events** in the menu area, select a group that contains the events that you want to display.
3. In the information area, select events for which you want to display details.
4. Select **Show Details** from **Action**.

Details of the events you have selected are displayed in the **Event Detail** dialog box.

Tip

Event details can be displayed by clicking **Description** for an event in the information area.

Tip

To copy event details, click the **Copy to Clipboard** button in the **Event Detail** dialog box. This is useful when reporting event descriptions.

Note that a summary of events can be viewed on the **Not Ack Event Summary** panel in the Home module or the **Summary Reports** view in the Reports module.

13.2 Exporting event information

You can export (batch output) the event information displayed in the information area of the Events module to a CSV file.

To export only specific items of event information, use a filter.

For example, to export only events for which action is required immediately, you can use a filter to display only events for which **Severity** is **Critical** and **Verification Status** is **Unconfirmed**.

To export event information:

1. Display the Events module.
2. Display the event information to be exported in the information area.
3. Select **Export Event List** from **Action**.
4. In the displayed dialog box, select the items that you want to export, and then click **OK**.
   To specify the character encoding for the exported CSV file, select a character encoding in **Encoding**. The character encoding is set to UTF-8 by default.
5. In the displayed view, click the **Save** button.

The CSV file is saved with the specified name in the location to which files are downloaded.

14 Report Reference

This section describes how to display reports to check the status of security control or asset management in your organization.

14.1 Displaying reports

JP1/IT Desktop Management can display 20 types of reports, which vary according to the purpose for which they will be used.

To display reports:

1. Display the Reports module.
2. In the menu area, click the reports you want to display.

The reports are displayed in the information area.

Note that if there is no data to be calculated for a report, in cases such as when software has just been installed or a function has not been used, no report details are displayed. In this case, operate JP1/IT Desktop Management so that the data to be calculated is stored in the database.

Tip

Reports can be displayed in a new window and not in the operation window. This is useful when you want to display multiple reports side by side. To display reports in a new window, in the information area, click the **Open new window** button in the upper-right corner.

14.2 Displaying reports with the latest data

Some reports display the results of calculations that are performed regularly. These calculations therefore need to be performed so that the reports display the latest data.

To display a report with the latest data:

1. Display the Reports module.
2. In the menu area, click a report that you want to display.
3. In the information area, click the **Calculate** button in the upper-right corner.
4. In the displayed dialog box, click **OK**.

Calculations are performed, and the report displays the latest data.

Tip

The **Calculate** button is displayed for the following reports:

- **Current Diagnosis** report
- **Percentage by violation level** report
- **Windows Update Installation Status** report
- **Antivirus Software Status** report
- **Mandatory Software Installation Status** report
- **Unauthorized Software Installation Status** report
- **Status of each security setting** report
- **Device Management Status** report
- **Green IT(Power Saving Settings)** report
- **Hardware Asset** report

Tip

For the **Software(License Violation)** and **Software(Surplus License)** reports, calculations are performed to obtain the latest data whenever the reports are displayed.

14.3 Printing reports

You can print reports. Printing can be used to create hard copies of reports.

To print a report:

1. Display the Reports module.
2. In the menu area, click a report that you want to display.
3. In the information area, click the **Print** button in the upper-right corner.
4. In the displayed dialog box, select the printer driver, and then click the **Print** button.

The report is printed.

14.4 Saving reports in PDF format

Saving reports in PDF format allows you to store past reports as electronic data. You can also distribute reports throughout your organization by attaching them to an email message.

> **Important note**
>
> A printer driver capable of PDF output is required to save reports in PDF format.

To save a report in PDF format:

1. Display the Reports module.
2. In the menu area, click a report that you want to display.
3. In the information area, click the **Print** button in the upper-right corner.
4. In the displayed dialog box, select the printer driver for PDF output, and then click the **Print** button.

The report is saved in PDF format.

15 Customizing Settings

This chapter describes items that can be customized in the Settings module and setup.

15.1 Managing server configurations

There are two types of servers for JP1/IT Desktop Management server: a management server and a site server. A site server is used for relaying package distribution and storing operation logs to balance the load on management servers and the network. To use a site server, define a site server group in the **Server Configuration Settings** view in the Settings module, and specify the group as a relay point for package distribution in each network segment or as an operation log backup location.

The following sections describe how to specify server configurations and how to manage site server groups.

15.1.1 Specifying server configurations

Specify a package distribution relay point and operation log backup location for each network segment. Management servers are specified for all network segments by default.

> **Tip**
>
> A package distribution relay point and operation log backup location are specified for each site server group. Therefore, adding the necessary site server groups before specifying server configurations makes operation easy.

To specify settings for server configurations:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.
3. In the information area, select **Server Configuration Settings**, and then click the **Edit** button of the network segment for which you want to specify server configurations.
4. In the displayed dialog box, select the corresponding site server group (or management server) for each item, and then click **OK**.

Package distribution relay points and operation log backup locations for the selected network segments are specified and displayed in the list.

15.1.2 Adding site server groups

Select multiple site servers in the system, and define them as a group.

Specify a package distribution relay point or operation log backup location for each site server group. You can either define a single site server as a group or group multiple site servers into one group. You can set connection priorities for each site server in a group.

Tip

If you use a site server as an operation log backup location, we recommend that you specify a single site server for the site server group specified for each network segment. This makes it easy to manage operation logs because the operation logs of a single computer are collected in a single site server.

To add site server groups:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.
3. In the information area, select **Site Server Group Settings**, and then click the **Add** button.
4. In the displayed dialog box, type information about site server groups, and then click **OK**.

Site server groups are added and displayed in the list.

15.1.3 Editing site server group information

You can edit the registered site server group information.

To edit the site server group information:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.
3. In the information area, select **Site Server Group Settings**, and then click the **Edit** button of the site server group you want to edit.
4. In the displayed dialog box, edit the site server group information, and then click **OK**.

The site server group information is updated.

15.1.4 Removing site server groups

You can remove the unnecessary site server groups.

Tip

You cannot remove a site server group specified as a package distribution relay point or operation log backup location for each network segment.

To remove site server groups:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.

3. In the information area, select **Site Server Group Settings**, and then click the **Remove** button of the site server groups you want to remove.

The site server groups are removed.

15.2 Specifying settings for discovery

You can customize settings to search for devices in Active Directory or networks. The customized settings can be immediately used for searching.

For details about the search conditions for Active Directory, see 15.2.2 Specifying search conditions (searching Active Directory).

For details about the search conditions for networks, see 15.2.1 Specifying search conditions (discovery from IP address).

15.2.1 Specifying search conditions (discovery from IP address)

You can specify search conditions for discovering network devices.

To specify search conditions:

1. Display the Settings module.
2. In the menu area, select **Discovery**, **Configurations**, and then **IP Address Range**.
3. In **Search Node Locations**, specify a discovery range.
   The discovery range named Management Server Segment is set by default. The management server segment is a segment that contains a management server.
4. In **Credentials Used**, specify credentials.
   Specify credentials if you want to perform a search by using credentials. After registering the credentials, in **Search Node Locations**, assign credentials to each discovery range.
5. Edit **Auto Discovery Schedule**.
   Specify the schedule if you want to regularly perform searches according to the determined schedule.
6. Edit **Edit Discovery Option**.
   Specify operations for cases in which a new device is discovered after the device search.
7. Edit **Notification of Discovery Completion**.
   To send a notification email to administrators of JP1/IT Desktop Management after the completion of device discovery, specify the recipients.
   If you have not set information for the mail server (SMTP server) to be used, in the view that is displayed by clicking the link **SMTP Server**, set the mail server information.

The settings for the search conditions are completed.

If you want to immediately start searching with the specified search conditions, click the **Start Discovery** button. If you do not perform an immediate search, the search is performed according to the **Auto Discovery Schedule**.

To check the search execution status and results, in the Settings module, select **Last Discovery Log**, and then the **IP Address Range** view.

Related Topics:

- 15.2.4 Checking the device discovery status

- 15.2.3 Credentials used in discovery from IP address

15.2.2 Specifying search conditions (searching Active Directory)

You can specify search conditions for discovering devices registered on Active Directory.

To specify search conditions:

1. Display the Settings module.
2. In the menu area, select **Discovery**, **Configurations**, and then **Active Directory**.
3. Edit **Auto Discovery Schedule**.
   Specify the schedule if you want to regularly perform searches according to the determined schedule.
4. Edit **Edit Discovery Option**.
   Specify what operations will be performed if a new device is discovered after the device search.
5. Edit **Notification of Discovery Completion**.
   To send a notification email to administrators of JP1/IT Desktop Management after the completion of device discovery, specify the recipients.
   If you have not set the mail server (SMTP server) information to be used by JP1/IT Desktop Management, click the **SMTP Server** link and set the mail server information in the window that appears.

> **Important note**
>
> The search cannot be performed if the Active Directory domain to be connected to is not specified. In the **Active Directory** view, specify a domain for Active Directory.

Settings for the search conditions are completed.

If you want to immediately start searching with the specified search conditions, click the **Start Discovery** button. If you do not perform an immediate search, the search is performed according to the **Auto Discovery Schedule**.

To check the search execution status and results, in the Settings module, select **Last Discovery Log**, and then the **Active Directory** view.

Related Topics:

- 15.2.4 Checking the device discovery status

15.2.3 Credentials used in discovery from IP address

When searching with IP addresses, devices are discovered with the use of ARP and ICMP, but detailed information about the devices is not collected. To collect the detailed device information during the search, you need to specify credentials for the discovered devices so that the devices can be connected by using SNMP or a Windows administrative share.

SNMP credentials
   Community name

Credentials for Windows administrative share

- User ID with administrator permissions
- Password

For a device for which SNMP can be used, if community authentication is possible, the device type as well as part of the device information can be collected when it is discovered.

For a computer for which Windows administrative shares are enabled, if logon authentication with administrator permissions is possible, the device type as well as most of the device information can be collected when it is discovered. In addition, the agent can be delivered and installed.

Important note

The device type of a computer with the following OSs: Windows Me, Windows 98, Windows 95, and Windows NT 4.0, might be classified as Unknown after discovery.

Important note

If multiple network cards are used for a single device, when a search is performed using ICMP, the device is discovered as multiple devices.

Tip

Specify a user ID to be used in authentication for Windows administrative shares in the following format if the ID is to be authenticated as a domain user: *User ID@FQDN (fully qualified domain name)*, or *domain name \user ID*. The fully qualified domain name is a format in which no host name or domain name are omitted. For example, specify an ID in the following format: User001@PC001.hitachi.com.

Tip

If Windows administrative share authentication is used, administrative share setting of a computer must be enabled in advance.

A search is performed by combining credentials for each discovery range. By default, all the specified credentials are used for discovery. If, however, SNMP community names differ among departments, or the Windows credentials differ among computers, you can perform a search by selecting the credentials necessary for each discovery range.

Note that the credentials used in discovery from IP addresses are also used when the agent is delivered. To deliver the agent after discovery, in the Settings module, select **Discovery** and then **Configurations**, and in the **IP Address Range** view, specify Windows administrative share credentials for the discovery range that includes the computer to which the agent is to be delivered.

15.2.4 Checking the device discovery status

In JP1/IT Desktop Management, after discovering devices in an organization, you can check the discovery history or the status of the discovered devices in the **Discovery** view of the Settings module. In this way, you can determine the current status of an organization's devices.

There are the following two types of device discovery history. Check the discovery history appropriate for the discovery method you used.

- Active Directory discovery history
- IP discovery history

There are the following three device management statuses. If necessary, either include or exclude a discovered device as a managed device.

Discovered

A discovered device is managed and displayed in the **Discovered Nodes** view that opens when you select **Discovery** in the Settings module. You can manage discovered devices or exclude them from the management target.

Managed

Specify this management status for the devices you want to manage in JP1/IT Desktop Management. The devices are displayed in the **Managed Nodes** view that opens when you select **Discovery** in the Settings module. You can also exclude these devices from management. Note that specifying this status for a device you want to manage consumes a product license.

Ignored

Specify this management status for devices that do not need to be managed in JP1/IT Desktop Management. These devices are displayed in the **Ignored Nodes** view that opens when you select **Discovery** in the Settings module. You can also change the status to *Managed* or delete these devices. When *Ignored* has been set for a device, the device is not displayed in the **Discovered Nodes** view even if you run a discovery again.

Related Topics:

- 15.2.5 Checking the latest discovery status
- 15.2.6 Checking the discovered devices
- 15.2.7 Checking the managed devices
- 15.2.8 Checking the excluded devices

15.2.5 Checking the latest discovery status

You can check the latest discovery execution status and results in a list.

To check the latest discovery status:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Last Discovery Log**.
3. In the information area, select **Active Directory** or **IP Address Range**.

The **Active Directory** view or the **IP Address Range** view appears. The discovery log is updated according to the progress of search.

Tip

You can also stop or start a search from the **Active Directory** view or the **IP Address Range** view. If a discovery error occurs frequently, we recommend that you stop the search and correct the search condition settings. After correcting the settings, perform a search again.

15.2.6 Checking the discovered devices

You can check the devices discovered during the Active Directory or network search in a list. In addition, you can change the status of the discovered devices to **Managed** (management targets) or **Ignored** (exclusion targets), or remove them from the list.

To check the discovered devices:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Discovered Nodes**.

The **Discovered Nodes** view appears. In this view, you can check the number of discovered devices, number of devices that can be managed, and the number of managed devices.

To change the status of a device to **Managed**, select a device in the information area, and then click the **Manage** button. To change the status of the device to **Ignored**, click the **Ignore** button. To remove the device from the list, from **Action**, select **Remove**. You can also select multiple devices at a time and change their status to **Managed** or **Ignored**, or remove them from the list.

Note that devices with the **Ignored** status are not displayed in the **Discovered Nodes** view. If you want to manage these devices again, access the **Ignored Nodes** view, and then change their status to **Managed**. If you want to manage the devices that you have previously removed, perform a search again.

Related Topics:

- 15.2.7 Checking the managed devices
- 15.2.8 Checking the excluded devices

15.2.7 Checking the managed devices

You can check the devices managed by JP1/IT Desktop Management in a list. In addition, you can change the status of the managed devices to **Ignored** (exclusion targets), or remove them from the list.

To check the managed devices:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Managed Nodes**.

The **Managed Nodes** view appears. In this view, you can check the number of managed devices and the remaining number of devices that can be managed.

To change the status of a device to **Ignored**, select a device in the information area, and then click the **Ignore** button. To remove the device from the list, from **Action**, select **Remove**. You can also select multiple devices at a time and change their status to **Ignored** or remove them from the list.

Note that devices with the **Ignored** status are not displayed in the **Managed Nodes** view. If you want to manage these devices again, access the **Ignored Nodes** view, and then change their status to **Managed**.

Tip

If you remove a device from the list and then perform a search again, the removed device is displayed in the **Discovered Nodes** view. To display the **Discovered Nodes** view, in the Settings module, select **Discovery** and then **Discovered Nodes**.

Related Topics:

- 15.2.8 Checking the excluded devices

15.2.8 Checking the excluded devices

You can check the devices that are excluded from being managed by JP1/IT Desktop Management in a list. In addition, you can change the status of the excluded devices to **Managed** (management targets).

To check the excluded devices:

1. Display the Settings module.
2. In the menu area, select **Discovery** and then **Ignored Nodes**.

The **Ignored Nodes** view appears. In this view, you can check the number of excluded devices and the remaining number of devices that can be managed.

To change the status of a device to **Managed**, select a device in the information area, and then click the **Manage** button. To remove the device from the list, from **Action**, select **Remove**. You can also select multiple devices at a time and change their status to **Managed** or remove them from the list.

Tip

If you remove a device from the list and then perform a search again, the removed device is displayed in the Discovered Nodes view. To display the Discovered Nodes view, in the Settings module, select **Discovery** and then **Discovered Nodes**.

Related Topics:

- 15.2.7 Checking the managed devices

15.3 Setting agents

Creating agent configurations and assigning them to computers on which the agent is installed allows you to remotely manage the agent setup.

For devices with agentless management, you can set intervals for collecting the device information.

Related Topics:

- 15.3.1 Managing agent configurations
- 15.3.7 Regularly updating agentless device information

15.3.1 Managing agent configurations

Agent configurations are assigned to the agent installed on a computer. You can specify the following agent configurations for a target computer: a monitoring interval, password protection for setup and uninstallation, or a behavior when remotely controlled. Managing the agent configurations allows you to remotely control the setup details of each agent.

If no particular agent configurations are assigned, the default agent configuration is assigned. If you do not need to use multiple agent configurations, editing the default agent configuration allows you to collectively change all of the agent settings.

Create agent configurations if you want to set different monitoring intervals for each computer or use flow control on only some of the computers. For details about how to create agent configurations, see 15.3.2 Adding agent configurations.

If the operation status changes, edit the agent configurations. For details about how to edit agent configurations, see 15.3.3 Editing agent configurations. For details about how to edit agent configurations to enable a site server and network monitoring, see 15.3.4 Editing agent configurations that enable site server and network monitoring.

If the agent configurations are no longer required due to a change in the operation status, remove the agent configurations. For details about how to remove agent configurations, see 15.3.5 Removing agent configurations.

Note that agent configurations must be assigned to each agent after they are created. For details about how to assign agent configurations to each agent, see 15.3.6 Assigning agent configurations.

Tip

If you cancel the assignment of agent configurations, the default agent configuration is automatically assigned to a computer.

Related Topics:

- 6.1 Starting to manage devices

15.3.2 Adding agent configurations

To set different monitoring intervals for computers, or use flow control on only selected computers, add agent configurations.

To add agent configurations:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Agent Configurations**.
3. In the information area, click **Add Agent Configuration**.
4. In the displayed dialog box, type the agent configuration information, and then click **OK**.

The agent configuration is added and displayed in the list of agent configurations.

The added agent configuration can be applied to computers with the agent already installed by assigning the agent configuration in the **Assign Agent Configuration** view.

15.3.3 Editing agent configurations

To change monitoring intervals or password protection settings for the agent, edit the agent configurations.

To edit agent configurations:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Agent Configurations**.
3. In the information area, click the **Edit** button of the agent configuration you want to edit.
4. In the displayed dialog box, edit the agent configuration information, and then click **OK**.

The agent configuration is updated. In addition, the settings of computers to which the agent configuration is assigned are automatically updated.

When editing the default agent configuration, you can specify an installation folder to which the agent can be delivered and installed. The default installation folder is %ProgramFiles%\Hitachi\jp1itdma.

Related Topics:

- 15.3.2 Adding agent configurations
- 15.3.5 Removing agent configurations
- 15.3.6 Assigning agent configurations

15.3.4 Editing agent configurations that enable site server and network monitoring

The following agent configurations must be specified for computers for which site server and network monitoring are to be enabled.

To edit agent configurations:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Agent Configurations**.

3. In the information area, click the **Edit** button of the agent configuration you want to edit.

4. In the displayed dialog box, select the check box of the following items, and then click **OK**.
   - **Connect to the management server**
   - **Regularly send information collected from a computer to the management server**
   - **Regularly collect information from the management server**

The agent configuration is updated. In addition, the settings of computers to which the agent configuration is assigned are automatically updated.

15.3.5 Removing agent configurations

You can remove unused agent configurations.

The agent configurations that are already assigned to a group or computer cannot be removed. To remove the agent configurations, cancel assignment of the agent configurations in advance.

For details about how to cancel agent configurations, see 15.3.6 Assigning agent configurations.

You cannot remove the default agent configuration.

To remove agent configurations:

1. Display the Settings module.

2. In the menu area, select **Agent**, and then **Agent Configurations**.

3. In the information area, click the **Remove** button of the agent configuration you want to remove.
   To remove agent configurations in a batch, select multiple agent configurations.

4. In the displayed dialog box, click **OK**.

The selected agent configurations are removed.

Related Topics:

- 15.3.2 Adding agent configurations
- 15.3.3 Editing agent configurations

15.3.6 Assigning agent configurations

You can assign agent configurations to each group or computer. You can also cancel the assigned agent configurations.

By default, the default agent configuration is assigned. If agent configurations other than the default agent configuration assigned to a group or computer are canceled, the default agent configuration is instead assigned to them.

To assign agent configurations:

1. Display the Settings module.

2. In the menu area, select **Agent**, and then **Agent Configurations Assignment**.

3. To assign agent configurations to each group, select the target group at the top of the view, and then click the **Assignment** button. To change a group configuration, click the **Change Target Group Type** button.

   To assign agent configurations to each computer, select the target computer at the bottom of the view, and then click the **Assignment** button.

4. In the displayed dialog box, select the agent configuration you want to assign, and then click **OK**.

5. In the displayed dialog box, click **OK**.

Agent configuration is assigned to the selected group or computer.

To cancel assignment of agent configurations:

1. Display the Settings module.

2. In the menu area, select **Agent**, and then **Agent Configurations Assignment**.

3. To cancel agent configurations assigned to a group, select the target group at the top of the view, and then click the **Assign Cancel** button. To change a group, click the **Change Target Group Type** button.

   To cancel agent configurations assigned to a computer, select the target computer at the bottom of the view, and then click the **Assign Cancel** button.

4. In the displayed dialog box, click **OK**.

   When canceling agent configuration assigned to a group, you can also choose to cancel the agent configuration for groups included in the selected group.

The agent configuration assigned to the group or computer is canceled. If you cancel assignment of agent configuration, the default agent configuration is assigned to the group or computer. Note that you cannot cancel the default agent configuration.

> **Tip**
>
> There are two types of agent configurations assignment: **Direct** or **Indirect**. If you assign agent configurations by selecting a group, the assignment is performed as **Direct**. For the groups and computers that are lower than the selected group, the assignment is performed as **Indirect**. If, however, agent configurations are already assigned as **Direct** to the lower groups or computers, **Indirect** assignment is not performed because **Direct** takes precedence.

Related Topics:

- 15.3.2 Adding agent configurations
- 15.3.3 Editing agent configurations
- 15.3.5 Removing agent configurations

15.3.7 Regularly updating agentless device information

For devices with no agent installed (agentless), you can set up an update, which regularly collects information from the devices, and you can set up update intervals.

To regularly update information about agentless devices:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Agentless Management**.
3. In the information area, select **Auto Monitoring Schedule**.
4. Specify an update interval for **Update Interval**.

   Tip

   To efficiently collect and update information, specify an hour interval for every 1,000 agentless devices. For example, if there are 800 agentless devices, specify settings so that the information can be updated every hour.

5. Click the **Apply** button.

Information about agentless devices is collected and updated at the specified update interval.

If you deselect **Auto Monitoring Schedule**, information about agentless devices is not collected.

Tip

JP1/IT Desktop Management recommends that you install the agent on managed computers for better security management.

15.4 Specifying settings for security management

You can change the schedule for judging the security status of a managed computer.

Related Topics:

- 15.4.1 Changing the schedule for security judgment

15.4.1 Changing the schedule for security judgment

You can change the time and intervals for judging the security status of a computer. The information on the Security module and reports are updated according to the schedule specified here.

To change the schedule for security judgement:

1. Display the Settings module.
2. In the menu area, select **Security management** and then **Security Schedule**.
3. In the information area, specify **Judgment Time** and **Judgment Interval (days)**.
4. Click the **Apply** button.

The security status of the managed computers is judged according to the specified schedule.

> **Tip**
>
> If the setting to automatically download the latest update program from the support service site is enabled, we recommend that you first update the information from the support service, and then specify the schedule so that the security status can be judged by using the latest information.

Related Topics:

- 15.9.3 Setting information for connecting to the support service

15.5 Specifying settings for asset management

You can add management items to be used in asset management, or change the data source of information for each item.

You can also specify a contract vendor list used to manage contract information.

Related Topics:

- 15.5.1 Adding asset management items
- 15.5.8 Managing contract vendor information

15.5.1 Adding asset management items

If you have a ledger for device management, you can add items that are not provided by JP1/IT Desktop Management as user-defined asset management items.

To add asset management items:

1. Display the **Asset Field Definitions** view from the Settings module.
2. Click the **Add Fields** button of a category to which you want to add items.
3. In the displayed dialog box, specify an item name or an information data source.

The specified asset management items are added. You can display the added items in the Assets module.

15.5.2 Changing the data source or data type of asset management items

You can change the data source of asset management items.

For example, if you configure the settings so that a user has to input some information, an administrator does not have to spend time maintaining the information.

To change the data source of asset management items:

1. Display the **Asset Field Definitions** view from the Settings module.
2. Click the **Edit** button of the item for which you want to change the data source.
   You can specify the data source or data type when adding new items.
3. In the displayed dialog box, edit the data source.

The data source is changed.

Tip

If the data type of **Department** or **Location** has been changed to a hierarchical structure, you can edit the hierarchical structure. The hierarchical structure edited here is reflected in the menu area of the Assets module or Device module.

Tip

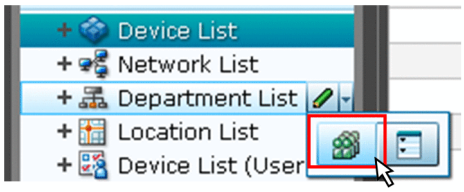
The data type of **Department** or **Location** can be changed. The added asset management items other than those two items cannot be changed to other data types once it has been specified.

15.5.3 Adding the definition for a department or location

If the departments or locations to manage increase, you can add a definition for a new department or location. After the definition is added, the new department or location is displayed in the menu area of the Assets module and the Device module.

To add the definition for a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



Tip

Alternatively, you can perform the following: In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the window that appears, click either **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

3. In the displayed dialog box, click the **Edit** button in **Type**.
4. In the displayed dialog box, add the department or location.
5. Click **OK**.
6. Click **OK**.

The the definition for the department or location is added, and the added group is displayed in the menu area of the Assets module and Device module.

Related Topics:

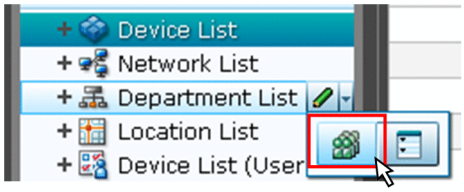
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location

15.5.4 Editing the definition for a department or location

If the organizational structure of the departments you are managing or the name of a location was changed, you can edit the definition for the department or location. After the definition is edited, the edited department or location is displayed in the menu area of the Assets module and the Device module.

To edit the definition of a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



> **Tip**
>
> Alternatively, you can perform the following: In the Settings module, select **Asset Management** and then **Asset Field Definitions**. In the window that appears, either click **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

3. In the displayed dialog box, click the **Edit** button in **Type**.
4. In the displayed dialog box, edit the name of the department or location, or hierarchical structure.
5. Click **OK**.
6. Click **OK**.

The definition for the department or location is edited, and the edited group is displayed in the menu area of the Assets module and Device module.

The user information (actual status) of each device is unchanged even if you changed a definition. Therefore, the definition that is different from the actual status is added to the menu area of the Assets module and Device module. To ensure the actual status is consistent with the definition, update the user information according to the definition after you edited the definition for a department or location. After you update the user information, delete only the hierarchies that exist in the old organizational system, so that the menu area display is consistent with the definition. For details about how to delete only the hierarchies that were used in the old system, see 6.31 Removing only hierarchies that were used in the old organizational system.

> **Tip**
>
> After you change the department definition, the department information displayed in the following views in the Assets module also changes: **Software License List** in **Software Licenses**, **Software License Status List** in **Software License Status**, and **Contract List** in **Contracts**.

Related Topics:

- 6.28 Adding the definition for a department or location

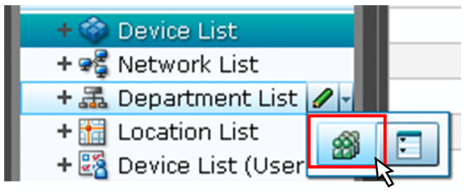
- 6.30 Removing the definition for a department or location

15.5.5 Removing the definition for a department or location

If you no longer manage a department or location, you can remove the definition for the department or location. After the definition is removed, the removed department or location no longer appears in the menu area of the Assets module and the Device module.

To remove the definition for a department or location:

1. Display the Assets module.
2. From **Hardware Assets** in the menu area, select **Department List** or **Location List**, and then click the displayed icon.



3. In the displayed dialog, click the **Edit** button in **Type**.
4. In the display the window, remove the definition for the department or location.
5. Click **OK**.
6. Click **OK**.

The definition for the department or location is removed.

The user information (actual status) of each device is unchanged even if you remove a definition. Therefore, the removed hierarchy is still displayed in the menu area of the Assets module and the Device module. To ensure the actual status is consistent with the definition, update the user information according to the definition after you edited the definition for a department or location. After you update the user information, delete only the hierarchies that exist in the old organizational system, so that the menu area display is consistent with the definition. For details about how to delete only the hierarchies that were used in the old system, see 6.31 Removing only hierarchies that were used in the old organizational system.

Tip

After you delete the department definition, in the following views of the Assets module, Unknown appears for the department:

- The **Software License List** view in **Software Licenses**
- The **Software License Status List** view in **Software License Status**
- The **Contract List** view in **Contracts**

Related Topics:

- 6.28 Adding the definition for a department or location

- 6.29 Editing the definition for a department or location

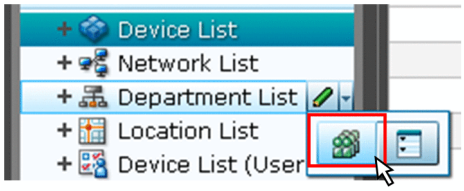
15.5.6 Setting the display names of departments and locations for each language

You can set the display names of departments and locations to the language of the computer a user is using. This is useful in managing departments and locations in an environment where an OS with multiple languages is used.

Note that, to set the display names of departments and locations for each language, the data source of departments and locations must be set to **End User**.

To set display names of departments and locations for each language:

1. Display the Assets module.
2. In the menu area, from **Hardware Assets**, select **Department List** or **Location List**, and click the displayed icon.



3. In the displayed dialog box, click the **Edit** button of **Type**.
4. Click the link **Other Language Settings**.
5. In the displayed dialog box, set the display names for each language.
6. Click **OK**.
7. Click **OK**.

The display names of departments and locations for other language environments are set.

Related Topics:

- 6.28 Adding the definition for a department or location
- 6.29 Editing the definition for a department or location
- 6.30 Removing the definition for a department or location
- 6.32 Changing the name of a department or location
- 6.33 Deleting a department or location

15.5.7 Removing only hierarchies that were used in the old organizational system

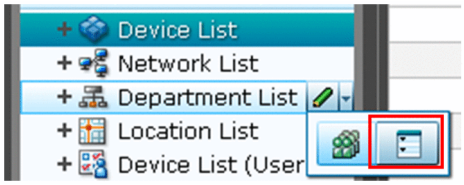
Even if you remove the hierarchies (definitions) for the departments or locations in the Settings module in association with an organizational change, the removed hierarchies will still appear in the menu area of the Assets or Device module. To ensure that the display in the menu area is consistent with the definitions, you need to remove only the hierarchies

that were used in the old organizational system. You can do so in the dialog box that you display from the menu area of the Assets module, the Device module, or the Security module.

The example below explains how to remove such hierarchies from the Assets module.

To remove only hierarchies that were used in the old organizational system:

1. Display the Assets module.
2. In the menu area, select **Hardware Asset**, select **Department List** or **Location List**, and then click the icon that appears.



3. In the dialog box that appears, select the hierarchies that you want to remove.
4. Click the **Remove** button.
5. In the dialog box that appears, click **OK**.
6. Click the **Close** button.

Only the hierarchies that were used in the old organizational system are removed, and the display of the menu area in the Assets module or the Device module is now consistent with the definitions.

15.5.8 Managing contract vendor information

If the contract information for an organization is managed by JP1/IT Desktop Management, you can register the information about vendors with which a contract, such as a maintenance contract, is made. A list of contract vendor information is called a contract vendor list. The contract vendor list is managed in **Contract Vendor List**, which you can select from **Asset management** in the Settings module.

Managing the contract vendor information allows you to specify the contract vendor information for contract information, so that you can quickly find out from the contract information a company location, contact person, or contact details. In addition, if you link the contract information with hardware asset information or software license information, you can check the corresponding contract vendor information on the **Contract Information** tab in the Assets module.

For details about how to add contract vendor information to a contract vendor list, see 15.5.9 Adding contract vendor information.

To update contract vendor information due to a change of a location or contact person, edit the contract vendor information. For details about how to edit contract vendor information, see 15.5.10 Editing contract vendor information.

To edit multiple contract vendor information items, export a contract vendor list first, edit the information, and then import the list to collectively update the information. For details about how to export a contract vendor list, see 15.5.12 Exporting contract vendor lists. For details about how to import a contract vendor list, see 11.4.5 Importing a contract vendor list.

To cancel contracts, remove the contract vendor information no longer required. For details about how to remove contract vendor information, see 15.5.11 Removing contract vendor information.

Related Topics:

- 1.11 General procedure for managing asset contract information

15.5.9 Adding contract vendor information

You can add contract vendor information to a contract vendor list in the **Contract Vendor List** view, which can be selected from **Asset management** in the Settings module. Adding the contract vendor information allows you to specify a contract vendor name for contract information in the Contract view of the Assets module. The contract information is then linked with the contract vendor information, allowing you to quickly find out the vendor location, contact person, or contact details.

To add contract vendor information:

1. Display the Settings module.
2. In the menu area, select **Asset management**, and then **Contract Vendor List**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, type the contract vendor information, and then click **OK**.

The contract vendor information is added and displayed in the contract vendor list.

Related Topics:

- 15.5.10 Editing contract vendor information
- 15.5.11 Removing contract vendor information
- 11.4.5 Importing a contract vendor list
- 15.5.12 Exporting contract vendor lists

15.5.10 Editing contract vendor information

You can edit the contract vendor information to change a location, contact person, or contact details of a contract vendor.

To edit contract vendor information:

1. Display the Settings module.
2. In the menu area, select **Asset management**, and then **Contract Vendor List**.
3. In the information area, click the **Edit** button of the contract vendor information you want to edit.
4. In the displayed dialog box, edit the contract vendor information, and then click **OK**.

The contract vendor information is updated.

Tip

To edit multiple contract vendor information items, export a contract vendor list first, edit the information, and then import the list to batch-update the information.

Related Topics:

- 15.5.9 Adding contract vendor information
- 15.5.11 Removing contract vendor information
- 11.4.5 Importing a contract vendor list
- 15.5.12 Exporting contract vendor lists

15.5.11 Removing contract vendor information

You can remove the canceled contract vendor information no longer used.

You cannot remove contract vendor information if it is specified for contract information. In this case, edit the contract information in advance so that the contract vendor information you want to remove is not specified for a contract vendor name. For details about how to edit contract information, see 11.3.2 Editing contract information.

To remove contract vendor information:

1. Display the Settings module.
2. In the menu area, select **Asset management**, and then **Contract Vendor List**.
3. In the information area, select the contract vendor information you want to remove, and then click the **Remove** button.
   To remove contract vendor information in a batch, select multiple contract vendor information items.
4. In the displayed dialog box, click **OK**.

The selected contract vendor information is removed.

Related Topics:

- 15.5.9 Adding contract vendor information
- 15.5.10 Editing contract vendor information
- 11.4.5 Importing a contract vendor list
- 15.5.12 Exporting contract vendor lists

15.5.12 Exporting contract vendor lists

You can export (batch output) a contract vendor list to a CSV file.

To export a contract vendor list:

1. Display the Settings module.

2. In the menu area, select **Asset management**, and then **Contract Vendor List**.
3. Select **Export Contract List** from **Action**.
4. In the **Export Item Selection** dialog box, select the items to export, and then click **OK**.
   To specify the character code for the exported CSV file, select a character code in **Encoding**. The character code is set to UTF-8 by default.
5. In the displayed view, click the **Save** button.

The CSV file is saved with the specified name in the location where the file is downloaded.

Related Topics:

- 15.5.9 Adding contract vendor information
- 15.5.10 Editing contract vendor information
- 15.5.11 Removing contract vendor information

15.6 Specifying settings for device management

You can set software search conditions to collect software information not registered on Windows **Programs and Functions**.

You can also configure AMT settings to control computer power sources.

Related Topics:

- 15.6.6 Setting AMT credentials

15.6.1 Adding software search conditions

You can add software search conditions to the list in the **Software Search Conditions** view, which can be selected from **Inventory** in the Settings module. Adding software search conditions allows you to obtain the software information that satisfies the search conditions from the managed computers as the installed software information. Specifying the obtained installed software information as mandatory software or prohibited software for the security policy enables monitoring of the installation status.

To add software search conditions:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Software Search Conditions**.
3. In the information area, click **Add Software Search Condition**.
4. In the displayed dialog box, type search conditions, and then click **OK**.
5. Click the **Apply** button.

The software search conditions are added.

Related Topics:

- 15.6.2 Editing software search conditions
- 15.6.3 Removing software search conditions
- 15.6.4 Importing software search conditions
- 15.6.5 Exporting software search conditions

15.6.2 Editing software search conditions

You can edit software search conditions. If you want to change software names or file names used for search, edit the software search conditions.

To edit software search conditions:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Setting Software Search Conditions**.

3. In the information area, click the **Edit** button of the software search conditions you want to edit.
4. In the displayed dialog box, edit the software search conditions, and then click **OK**.

The selected software search conditions are changed.

Related Topics:

- 15.6.1 Adding software search conditions
- 15.6.3 Removing software search conditions
- 15.6.4 Importing software search conditions
- 15.6.5 Exporting software search conditions

15.6.3 Removing software search conditions

You can remove unused software search conditions.

To remove software search conditions:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Software Search Conditions**.
3. In the information area, select the software search conditions you want to remove, and then click the **Remove** button.
   To remove software search conditions in a batch, select multiple software search conditions.
4. In the displayed dialog box, click **OK**.

The selected software search conditions are removed.

Related Topics:

- 15.6.1 Adding software search conditions
- 15.6.2 Editing software search conditions
- 15.6.4 Importing software search conditions
- 15.6.5 Exporting software search conditions

15.6.4 Importing software search conditions

You can collectively add software search conditions by importing software search conditions in a CSV file.

To import software search conditions:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Software Search Conditions**.
3. In the information area, from **Action** select **Import Software Search Conditions**.
4. In the **Import Software Search Conditions** dialog box, specify a CSV file you want to import.

To specify the character encoding for the imported CSV file, select a character encoding in **Encoding**. The character encoding is set to UTF-8 by default.

You can download a CSV sample file from this view. Use it as a reference when creating a CSV file.

5. Click **OK**.

CSV file data is imported. Check whether the imported information is correctly registered. If an incorrect record exists, change the CSV file, and then import the information again.

Related Topics:

- 15.6.1 Adding software search conditions
- 15.6.2 Editing software search conditions
- 15.6.3 Removing software search conditions
- 15.6.5 Exporting software search conditions

15.6.5 Exporting software search conditions

You can export (batch output) software search conditions to a CSV file.

To export software search conditions:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Software Search Conditions**.
3. Select **Export Software Search Conditions** from **Action**.
4. In the **Select Export Columns** dialog box, check the items to export, and then click **OK**.

   To specify the character encoding for the exported CSV file, select a character encoding in **Encoding**. The character encoding is set to UTF-8 by default.
5. In the displayed view, click the **Save** button.

The CSV file is saved with the specified name in the location where the file is downloaded.

Related Topics:

- 15.6.1 Adding software search conditions
- 15.6.2 Editing software search conditions
- 15.6.3 Removing software search conditions
- 15.6.4 Importing software search conditions

15.6.6 Setting AMT credentials

To control computer power sources by using AMT or obtain information about AMT firmware versions, you must set AMT credentials in advance.

In addition, to set AMT for a computer via agent configurations, a password with administrator privileges must be set to automatically enable AMT.

To set AMT credentials:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **AMT**.
3. Set AMT credentials.

   To control computer power source by using AMT and to obtain information about AMT firmware version, in the information area, type **User ID**, **Password**, and **Retype Password**.

   To automatically enable AMT for a computer, type a password with AMT administrator privileges in **Password** and **Retype Password** of **Password for administrative privileges**.
4. Click the **Apply** button.

Power source control with the use of AMT is enabled for a user computer.

Note that to use AMT, in addition to the settings specified for JP1/IT Desktop Management, you must specify AMT settings for a management server and a user computer.

Important note

The user name and password for the AMT user information (AMT management user) specified for **Credentials Used** must be consistent between the management server settings and a managed computer.

Tip

For computers with the agent already installed, you can specify AMT settings from the agent configurations. This reduces the time to operate the BIOS on each computer.

Tip

If a password with administrator privileges is not specified for a computer's AMT, the password specified for **Password for administrative privileges** is registered on AMT. If a password with administrator privileges is already registered, you cannot set the password. Specify the already registered password. In addition, if a password with administrator privileges is already specified and AMT is disabled, you must enable the computer's AMT in advance.

Related Topics:

- 6.23 Controlling the computer power

15.6.7 Setting acquisition of the Revision History of the device

If the device information has changed, you can specify a setting to acquire the Revision History of the changes.

To set acquisition of the Revision History:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Revision History Settings**.

3. Select **Collect revision history**.

4. From **Revision History Collection Targets**, select the device information for which you want to acquire the Revision History.

   Only the Revision History of the device information that you select here is acquired.

5. Click **Apply**.

You can now acquire the Revision History. You can view the Revision History in the **Revision History** view of the Device module. If, during setup, you set output of the revision history archive, you can output the acquired revision history archive to a file.

15.7 Specifying settings for reports

You can change the period to store reports and the month or the day of the week that is regarded as a starting point of calculations for reports.

You can also specify recipients of daily, weekly, and monthly summary reports.

Related Topics:

- 15.7.1 Changing the storage period and start date for reports
- 15.7.2 Setting recipients of summary reports

15.7.1 Changing the storage period and start date for reports

You can change the period to store reports and the start date that is regarded as a starting point of calculations for reports.

Storing reports allows you to reference past reports. Note that after the storage period is over, the calculated data is automatically removed, and you can no longer reference reports.

To change the storage period and start date for reports:

1. Display the Settings module.
2. In the menu area, select **Reports** and then **Duration and Start Date**.
3. In the information area, select the period for which you want to store reports.
4. Select the day of the week, date, and month that is regarded as a starting point of calculations for reports.
5. Click the **Apply** button.

The storage period and start date for reports are changed.

Tip

By default, the storage period for reports is **5 years**, the start of the week is **Monday**, the start of the month is **1**, and start of the year is **April**.

15.7.2 Setting recipients of summary reports

You can specify recipients of daily, weekly, and monthly summary reports.

The contents of reports are sent to the specified email addresses when summary reports are created. The email content allows you to know the management status without using JP1/IT Desktop Management.

To specify recipients of summary reports:

1. Display the Settings module.
2. In the menu area, select **Reports** and then **Summary Report Notifications**.

3. In the information area, select user IDs to which summary reports are sent.

4. Click the **Apply** button.

The recipients of summary reports are specified.

> **Tip**
>
> To edit email addresses, select user IDs. If email addresses are not specified, you can type email addresses. Note that the email addresses specified here are reflected on the user accounts that are displayed in the **Account Management** view, which you can select from **User Management** in the Settings module.

> **Tip**
>
> All the user IDs specified as recipients receive the same summary reports regardless of work responsibilities specified for each user ID.

Related Topics:

- 15.9.1 Setting up mail servers
- 4. Managing User Accounts

15.8 Setting events

Related Topics:

- 15.8.1 Specifying settings for event notification

15.8.1 Specifying settings for event notification

You can specify settings for mail notification so that when a specific event occurs, you can be notified of the event occurrence via email.

To specify settings for event notification:

1. Display the Settings module.
2. In the menu area, select **Events** and then **Event Notification Settings**.
3. In **Select category and severity of events**, select categories of events of which you want to be notified via email.
4. In **Select recipients**, select user IDs to which an event notification is sent.
   To edit an email address, select a relevant user ID.

The events for which a notification is to be sent and recipients of the notification are specified.

To exclude specific events from those for which a notification is sent, in **Specify the event notifications to be ignored**, click the **Add** button. In the **Add Ignored Events** dialog box, you can specify events for which a notification email is not sent.

Tip

To edit email addresses, select user IDs. If email addresses are not specified, you can type email addresses. Note that the email addresses specified here are reflected on the user accounts that are displayed in the **Account Management** view, which you can select from **User Management** in the Settings module.

Tip

All the user IDs specified as recipients receive all notifications about the specified events regardless of work responsibilities specified for each user ID. However, the URL in the event notification email can be accessed only when the user ID of the recipient is specified to have work responsibilities for the linked URL. If a user with the user ID for which work responsibilities for the linked URL are not specified clicks the link, the user is automatically returned to the Home module.

Related Topics:

- 15.9.1 Setting up mail servers
- 4. Managing User Accounts

15.9 Setting information about connecting to other systems

You can set the following information necessary for JP1/IT Desktop Management to connect to other systems.

- Mail server information used by JP1/IT Desktop Management to send email notifications
- Domain information of Active Directory to be searched
- Information for connecting to the support service site from which the latest Windows update details can be obtained
- Information for connecting to MDM systems that are required for the smart device management

Related Topics:

- 15.9.1 Setting up mail servers
- 15.9.2 Setting information for connecting to Active Directory
- 15.9.3 Setting information for connecting to the support service
- 15.9.4 Specifying settings to link with an MDM system

15.9.1 Setting up mail servers

To receive notification emails about the completion of discovery, creation of summary reports, or an event occurrence, you must specify the information about the mail server used by JP1/IT Desktop Management to send email notifications.

To set up a mail server:

1. Display the Settings module.
2. In the menu area, select **General** and then **SMTP Server**.
3. In the information area, specify the mail server information.
   To send a test mail by using the specified mail server, click the **Send Test E-mail** button. Check if the test mail is sent properly. Note that the test mail is sent to email addresses specified for the user accounts of login users.
4. Click the **Apply** button.

Emails can be sent by using the specified user.

Tip

Using email notification allows you to know the management status without frequently checking the operation window in JP1/IT Desktop Management. You can use email notification for the following functions.

- Notification of discovery results
- Notification of summary reports
- Notification of event occurrences

Related Topics:

- 15.2.1 Specifying search conditions (discovery from IP address)
- 15.2.2 Specifying search conditions (searching Active Directory)

- 15.7.2 Setting recipients of summary reports
- 15.8.1 Specifying settings for event notification

15.9.2 Setting information for connecting to Active Directory

To specify devices registered on Active Directory as a management target of JP1/IT Desktop Management or import department hierarchy information, you must set the domain information of Active Directory to be searched.

To set information for connecting to Active directory:

1. Display the Settings module.
2. In the menu area, select **General** and then **Active Directory**.
3. To obtain group hierarchy information from Active Directory, in the information area, select **Get Department Hierarchy Information**.
4. Specify the information about Active Directory to be connected
   To set multiple Active Directory information items, click the **Add** button, and then add information.
5. Click the **Test** button to check if a connection to Active Directory can be established.
6. If no problems have been found in the connection, click the **Apply** button.

When the search for Active Directory is started, the Active Directory information specified here is collected.

If the agent is simultaneously delivered while Active Directory is being searched, the credentials specified in this view are used.

Related Topics:

- 15.2.2 Specifying search conditions (searching Active Directory)

15.9.3 Setting information for connecting to the support service

To judge whether the Windows update program is up to date, you must regularly download the latest information about update programs from the support service site. To do this, you must set information for connecting to the support service site.

Connecting to the support service site automatically updates the information about update programs to the latest.

Obtaining the latest information from the support service site allows the security policy to judge whether the latest update program is applied to the managed computers.

Important note

To connect to the support service site, you must have a contract for the support service.

To set information for connecting to the support service:

1. Display the Settings module.

2. In the menu area, select **General** and then **Product Update**.

3. In the information area, specify information about the support service to be connected.

   For details about the information of the support service to be connected, check the Release Notes. Click the **Test** button to check if a connection to the specified support service site can be established.

   In **Edit Import Schedule**, you can specify schedule to obtain the latest information about update programs from the support service site.

   In addition, in **Specify users to receive Product Update notification e-mails**, you can specify recipients of a notification mail that informs users that the update program list on the Security module has been updated.

4. Click the **Apply** button.

The latest support information is downloaded from the support service site according to the schedule specified in **Edit Import Schedule**. In addition, when the update programs list is updated after downloading, a notification mail is sent to the specified addresses.

Tip

If a management server cannot connect to the external network, use computers that can connect to the external network to download the support information from the support service site. You can register the downloaded support information on the management server by using the `updatesupportinfo` command.

Tip

When the security policy is updated after the information is obtained from the support service site, the security status of a device is judged.

Related Topics:

- 17.22 updatesupportinfo (uploading support service information)

15.9.4 Specifying settings to link with an MDM system

To obtain smart device information from an MDM system and manage it in JP1/IT Desktop Management, you must specify information for connecting to the MDM system and the schedule for obtaining the smart device information.

Important note

Only a single MDM linkage setting can be specified for each MDM server. If more than one setting is specified for a single MDM server, JP1/IT Desktop Management might fail to control smart devices.

To set information for linking with an MDM system:

1. Obtain a server certificate for an MDM product.
   1. In the Web browser, access the portal of MDM products.
   2. Export the server certificate to a file.

For Internet Explorer:

(i) Right click on the window, and select **Properties**, **Certificates**, **Details**, and then **Copy to File**.

(ii) Use the certificate export wizard to export the certificate in the DER encoded binary X.509 format.

For Firefox:

(i) Right click on the window, and select **View Page Info**, **Security**, **View Certificate**, **Details**, and then **Export**.

(ii) In the dialog box for saving certificates, save the certificate in the X.509 Certificate (DER) format.

2. Copy the server certificate obtained in step 1 to a management server.

3. Import the server certificate to the management server.

   Execute the following command in the command prompt of the management server:

   JP1/IT Desktop Management - Manager installation folder\mgr\uCPSB\jdk\jre\bin\keytool.exe -import -keystore *JP1/IT Desktop Management - Manager installation folder*\mgr\uCPSB\jdk\jre\lib\security\cacerts -file *server certificate path*\ -alias *server certificate alias*\#

   #: The string *server certificate path* indicates the path of the server certificate copied in step 2. The string *server certificate alias* indicates another name of the server certificate to be imported. You can specify any name for the alias.

   When the command is executed, you are asked to type a password to import the server certificate. Type the password. The default password is change it.

4. Display the Settings module of JP1/IT Desktop Management.

5. In the menu area, select **General** and then **MDM Linkage Settings**.

6. In the information area, click the **Add** button in the **MDM Linkage Settings**.

7. In the displayed dialog box, specify information about the MDM system to be connected to.

8. Click the **Test** button to check if a connection to the specified MDM system can be established.

9. Edit **Collection Schedule**.

   Specify the schedule if you want to regularly update the smart device information according to a determined schedule.

10. Click **OK**.

11. In the information area, click the **Edit** button in **Edit Discovery Option**.

12. In the displayed dialog box, specify whether the discovered smart device is to be automatically managed.

The smart device information is obtained from the MDM system according to the schedule specified in **MDM Linkage Settings**.

To link with MobileIron, you must assign API permission in MobileIron to the user ID specified in **MDM Linkage Settings**.

Tip

Discovered smart devices are to be managed according to the settings specified in **Edit Discovery Option**. If the discovered devices are not specified as a device to be automatically managed, to manage the smart devices, you must specify the smart devices as management target in the **Discovered Nodes** view of the Settings module.

Tip

After importing the server certificate that you obtained from the MDM system to the management server, if you change the server certificate, you need to obtain the changed server certificate, and then re-import it to the management server.

Related Topics:

- 15.2.6 Checking the discovered devices
- 15.2.7 Checking the managed devices

16 Database Management

This chapter describes how to manage a database by using a database manager.

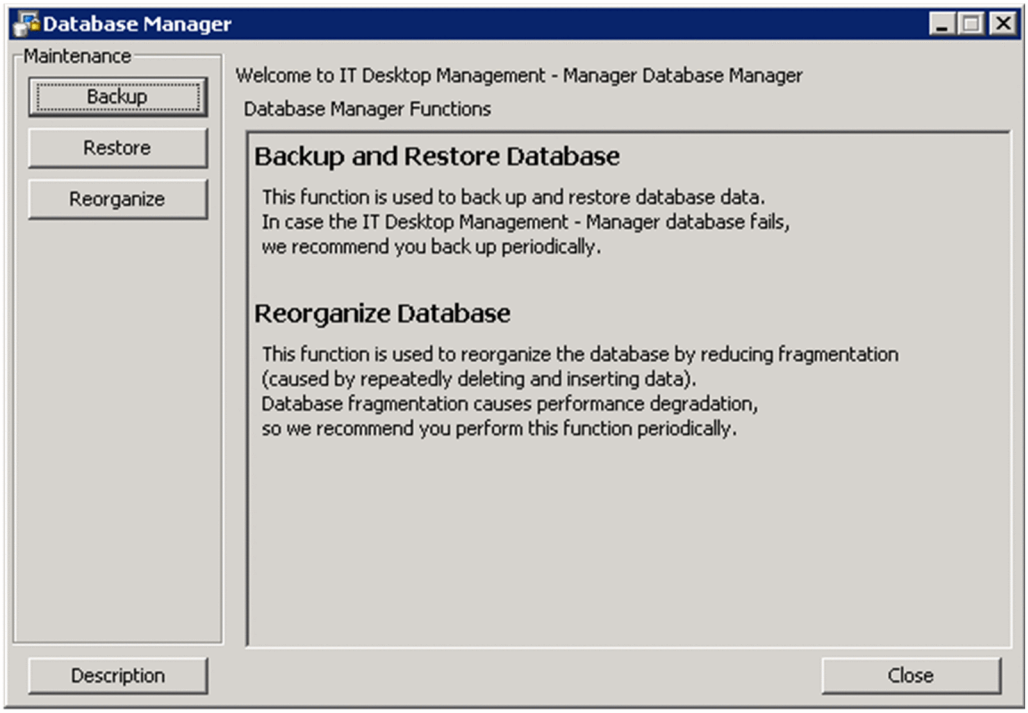
16.1 Starting a database manager

For a system in a single-server configuration, a database manager can be started from a management server. For a system in a multi-server configuration, a database manager can be started from a database server.

Note that a database manager can be used only when the services for JP1_ITDM_DB Service are running.

To start a database manager:

1. Log in to the OS as a user with administrator permissions.
2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Manager**, **Tools**, and then **Database Manager**.
   The database manager starts, and a view for describing functionality appears.



3. In **Maintenance** on the left side of the dialog box, click the button for the function that you want to execute.
   The view for the selected function is displayed.

To return to the initial view of the database manager, click the **Description** button.

> **Important note**
>
> When the initial view is displayed after you click the **Description** button, whatever you have specified so far is cleared.

To close the database manager, click the **Close** button.

Related Topics:

- 16.2 Backing up databases
- 16.3 Restoring databases

16.2 Backing up databases

This chapter describes how to back up a database by using a database manager.

Tip

To back up a database, you must stop the management server. Therefore, choose a day or time of day for the backup that is during a time when the management server is not used.

Tip

The time required for a backup depends on the disc capacity. In addition, if operation logs are specified in setup to be automatically stored, operation logs for which backup operations are not performed are also backed up. The dialog box that indicates that a backup is being processed displays the elapsed time, which you can use to measure the progress status.

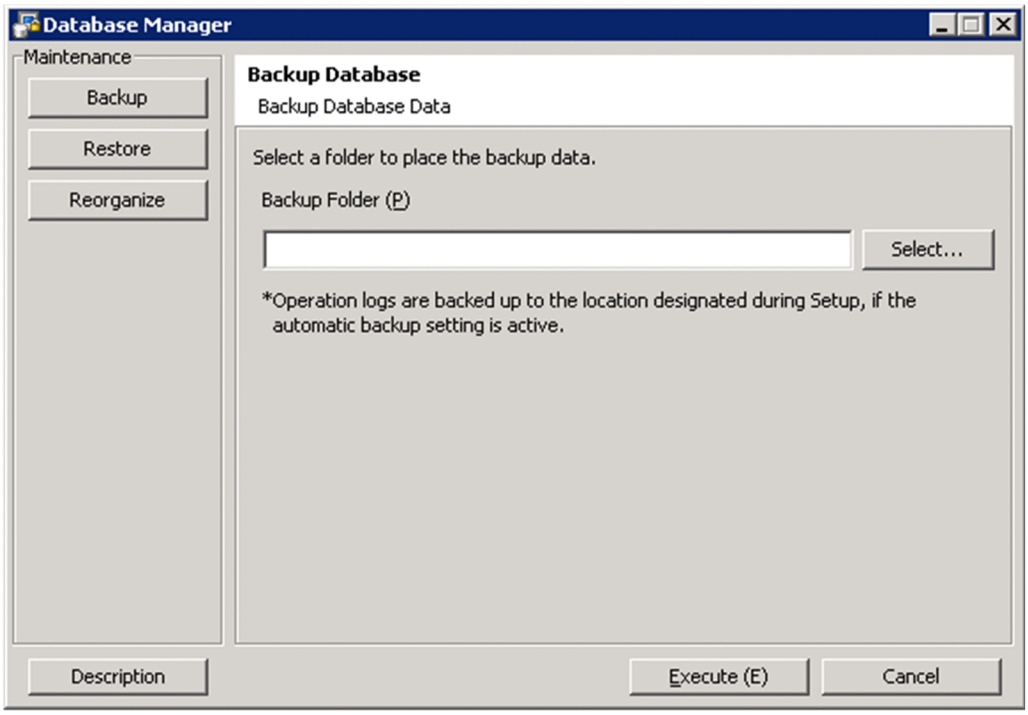
Important note

If you are using a computer that is running Windows 8, do not specify the following folders for **Backup Folder**:

- *system-drive*:\Program Files\folders-in-WindowsApps
- Storage folders created by using thin provisioning

1. In the Database Manager view, from **Maintenance**, click the **Backup** button.
2. In the **Database Backup** view, specify a folder in which to store the backup file.

   Specify for **Backup Folder** the location in which to store the backup file. Specify a folder on a local drive. The size of the backup file depends on what operations have been performed and how long JP1/IT Desktop Management has been used. Make sure that the drive has an amount of free space equal to at least the total amount of disk space occupied by the database folder and data folder.



Important note

If you specify a folder on a network drive for **Backup Folder**, the backup will fail.

If you have backed up a database before, the location specified for storing the backup file the previous time is displayed. Note that if a backup file with the same name exists in the specified location, the file is overwritten. If overwriting fails, the file backed up the previous time remains without change.

If specifying a backup folder directly, use a character string not exceeding 150 single-byte characters, which can consist of alphanumeric characters, spaces, and the following symbols:

( ) . @ \

3. Click the **Execute** button.

   A dialog box that shows the processing status is displayed until the backup is complete.

After the backup is complete, the following files are output:

- jdnexport.info
- jdnexportdata.bak
- table.*table name*.exp.bin

Related Topics:

- 16.1 Starting a database manager

16.3 Restoring databases

This chapter describes how to restore a database by using a database manager.

Tip

To restore a database, you must stop the management server. Therefore, choose a day or time of day for the reorganization that is during a time when the management server is not used.

Tip

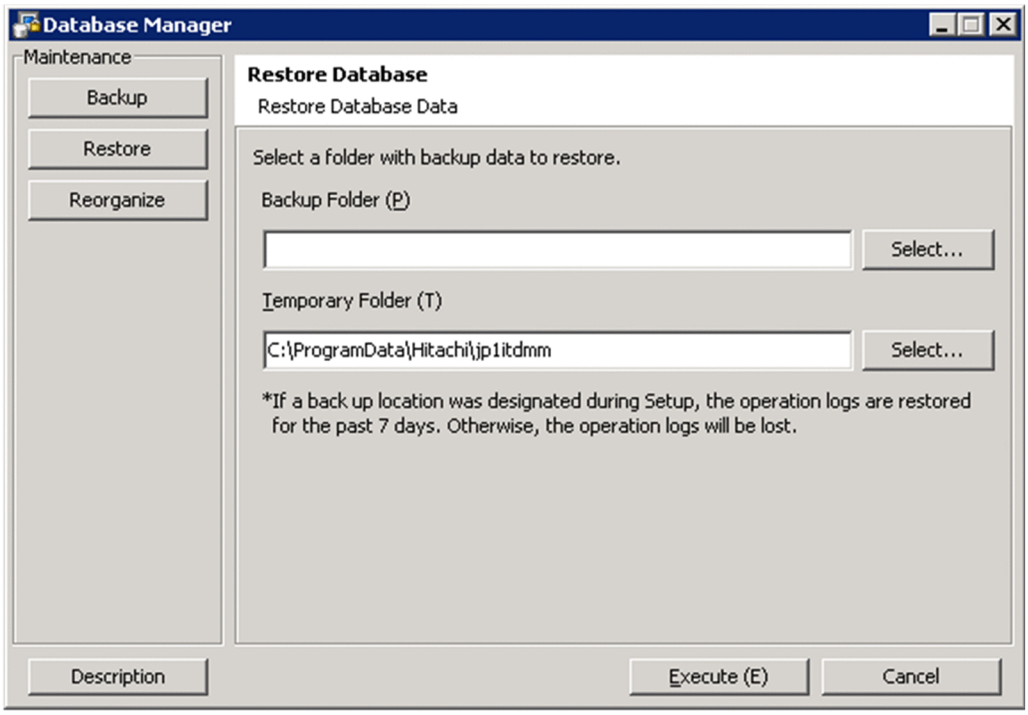
The time required for restoration depends on the disc capacity. In addition, if operation logs are specified in setup to be automatically stored, the time required for restoration changes depending on the size of the operation logs. The dialog box that indicates that a restoration is being processed displays the elapsed time, which you can use to measure the progress status.

Important note

If you are using a computer that is running Windows 8, do not specify any of the following folders for **Backup Folder**:

- *system-drive*:\program files\folders-in-WindowsApps
- Storage folders created by using thin provisioning

1. In the Database Manager view, from **Maintenance**, click the **Restore** button.
2. In the **Restore Database** view, specify a folder in which a backup file is stored.
   Specify for **Backup Folder** the location in which a backup file is stored.



Important note

If you specify a folder on a network drive for **Backup Folder**, restoration will fail.

If you have backed up a database before, the location specified for storing the backup file the previous time is displayed.

If specifying a data storage folder directly, use a character string not exceeding 150 single-byte characters, which can consist of alphanumeric characters, spaces, and the following symbols:

( ) . @ \

3. Specify a work folder.

   Specify for **Temporary Folder** a work folder to be used for restoration.

   Important note

   For **Temporary Folder**, if 10,000 devices are managed, specify a folder on a local drive that has at least 10 GB of free space. If you specify a folder on a network drive, restoration will fail.

   If you have restored the database before, the work folder specified for the previous time is displayed.

   If specifying a work folder directly, use a character string not exceeding 150 single-byte characters, which can consist of alphanumeric characters, spaces, and the following symbols:

   # ( ) . @ \

   By default, the following folder is specified:

   All User profile application data folder \Hitachi\jp1itdmm

4. Click the **Execute** button.

   A dialog box that shows the processing status is displayed until restoration is complete.

Restoration is complete.

Related Topics:

- 16.1 Starting a database manager

16.4 Reorganizing databases

This chapter describes how to reorganize a database by using a database manager.

Tip

To reorganize a database, you must stop the management server. Therefore, choose a day or time of day for the reorganization that is during a time when the management server is not used.

Tip

The time required for reorganization depends on the disc capacity. The dialog box that indicates that reorganization is being processed displays the elapsed time, which you can use to measure the progress status.

Important note

If you are using a Windows 8 computer, do not specify the following folders when setting the folders:

- *system-drive*:\program files\folders-in-WindowsApps
- Storage folders created by using thin provisioning

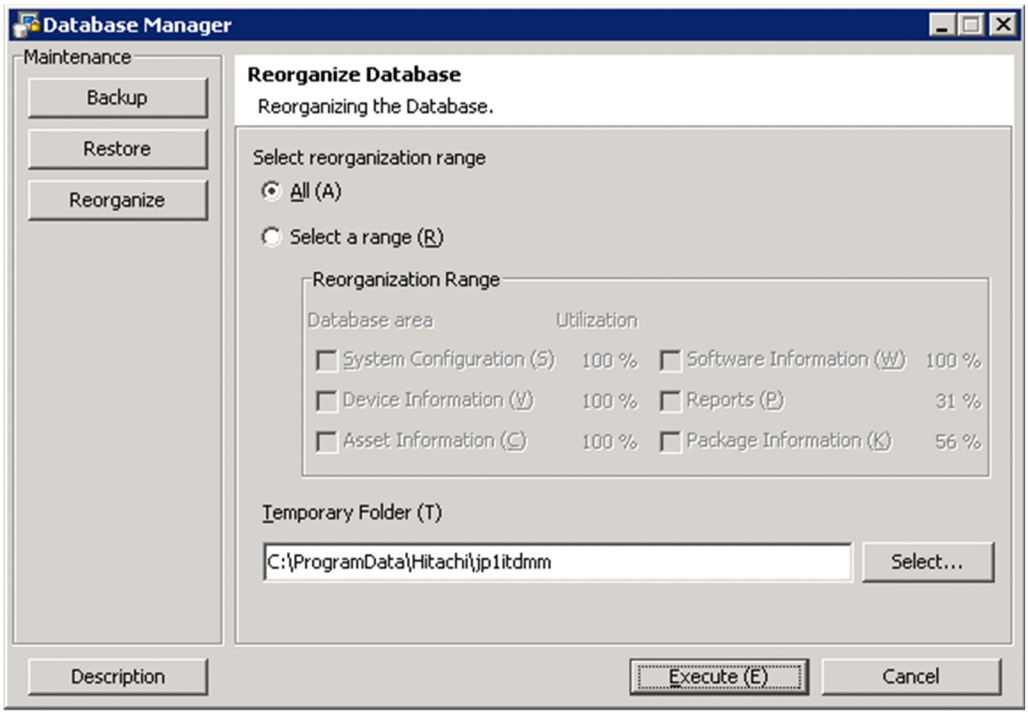
1. In the Database Manager view, from **Maintenance**, click the **Reorganize** button.
2. In the **Database Reorganization** view, select a range that you want to reorganize.

   If **All** is selected:

   All data in the database will be reorganized.

   If **Select a range** is selected:

   Select the items that you want to reorganize. Database usage is displayed for each item. Items with 80% or more database usage are automatically selected.



3. Specify a work folder.
   Specify for **Temporary Folder** a work folder to be used during reorganization.

   Important note

   For **Temporary Folder**, if 10,000 devices are managed, specify a folder on a local drive that has at least 30 GB of free space. If you specify a folder on a network drive, the reorganization will fail. If you are using a cluster configuration, specify a folder on a shared disk.

   If you have reorganized the database before, the work folder specified for the previous time is displayed.
   If specifying a work folder directly, use a character string not exceeding 150 single-byte characters, which can consist of alphanumeric characters, spaces, and the following symbols:
   Sharp signs (#), brackets ((and)), periods (.), @, backslashes (\)
   # ( ) . @ \
   By default, the following folder is specified:
   All User profile application data folder\Hitachi\jp1itdmm

4. Click the **Execute** button.
   A dialog box that shows the processing status is displayed until reorganization is complete.

The reorganization is complete.

Tip

You can also reorganize a database by using the `reorgdb` command. For details about the `reorgdb` command, see 17.25 reorgdb (reorganizing the database).

Related Topics:

- 16.1 Starting a database manager

17 Commands

This section describes JP1/IT Desktop Management commands.

17.1 Executing commands

To execute JP1/IT Desktop Management commands, you can use either the dedicated command prompt (**JP1ITDM Utility Console**) or the Windows command prompt.

JP1ITDM Utility Console is useful when you execute commands on the management server or database server. **JP1ITDM Utility Console** allows you to skip specification of a storage folder for the command execution file when entering a command. By default, when **JP1ITDM Utility Console** starts, the storage folder used by the command is set to the current folder. You can also use the Windows command prompt to execute commands.

Execute commands other than the `getinv.vbs` command as a user who has administrator permissions. In Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, if User Account Control (UAC) is enabled, use a right-click to open **JP1ITDM Utility Console** or the Windows command prompt, and then select **Run as administrator**. Execute the `getinv.vbs` command as a user who has full control permissions over the folder in which the `getinv.vbs` command is stored.

To execute commands on the site server or an agent, use the Windows command prompt.

To execute commands on the management server or database server:

1. From the Windows **Start** menu, select **All programs**, **JP1_IT Desktop Management - Manager**, and then **Command**.
2. In the window that appears, enter the command that you want to execute.

The command is executed.

To execute commands on the site server or an agent:

1. Open the Windows command prompt.
2. In the window that appears, enter the command that you want to execute.

The command is executed.

> **Tip**
>
> JP1/IT Desktop Management commands can be run as a scheduled task by registering them as a Windows task.
>
> When backing up, restoring, and reorganizing the database with commands, services on the management server and database server must be stopped. Make sure to check which day of the week or time of the day JP1/IT Desktop Management is not running when you register these commands as a Windows scheduled task.

Note

Do not perform the operations listed below on a management server, site server, or database server on which a command is executing. If you perform one of these operations while a command is executing, the command is forcibly terminated. Depending on the timing, the database and important data might be corrupted, the agent control service might be suspended, and the command might output incorrect return values.

- Pressing the **Ctrl** + **C** keys
- Closing either **JP1ITDM Utility Console** or the Windows command prompt
- Logging out of Windows

- Shutting down Windows

If you perform one of these operations while a command is executing, check the messages in the log file. If a message indicating that the command finished successfully does not appear, re-execute the command as necessary. If a message indicating that the agent control service was suspended appears, restart the agent control service.

Note that the above notes do not apply to the following commands:

- `stopservice`
- `startservice`
- `getlogs`
- `getinstlogs`
- `addfwlist.bat`
- `resetnid.vbs`
- `getinv.vbs`

17.2 Command description format

Commands are described in subsections such as functionality, format, and arguments. The following table shows how the commands are described.

No.	Item	Description
1	Functionality	This subsection describes the command functionality.
2	Format	This subsection describes the format of the command.
3	Arguments	This subsection describes the arguments for the command.
4	Storage location	This subsection describes the storage location for the command.
5	Notes	This subsection provides notes on execution of the command.
6	Return values	This subsection describes the return values of the command.
7	Example	This subsection provides an example of usage of the command.

17.3 Command List

The following table shows the list of available commands in JP1/IT Desktop Management.

In a single-server configuration:

Command name	Functionality	Systems for the command to be executed in
`ioutils exportasset`	Exports hardware asset information.	Management server
`ioutils importasset`	Imports hardware asset information.	Management server
`ioutils exportfield`	Exports custom field settings.	Management server
`ioutils importfield`	Imports custom field settings.	Management server
`ioutils exporttemplate`	Exports templates that defines field mappings used when importing asset information.	Management server
`ioutils importtemplate`	Imports templates that defines field mappings used when importing asset information.	Management server
`ioutils exportdevice`	Exports device information.	Management server
`ioutils exportdevicedetail`	Exports device information details.	Management server
`ioutils exportpolicy`	Exports security policy settings.	Management server
`ioutils importpolicy`	Imports security policy settings.	Management server
`ioutils exportupdategroup`	Exports update group settings.	Management server
`ioutils importupdategroup`	Imports update group settings.	Management server
`ioutils exportoplog`	Export operation logs stored in a management server.	Management server
`recreatelogdb`	Rebuilds indexes for the operation logs stored in the site server.	Site server
`movelog`	Moves operation log data within the site server.	Site server
`deletelog`	Deletes operation log data from site server	Site server
`ioutils exportfilter`	Exports filter settings.	Management server
`ioutils importfilter`	Imports filter settings.	Management server
`updatesupportinfo`	Uploads support information that is downloaded from the support service site.	Management server
`exportdb`	Acquires data owned by the management server for backup purposes.	Management server
`importdb`	Restores data owned by the management server to the state of the last backup point.	Management server
`reorgdb`	Reorganizes the database.	Management server
`stopservice`	Stops services on the management server.	Management server
`startservice`	Starts services on the management server.	Management server
`getlogs`	Collects troubleshooting information on the management server.	Management server
`getinstlogs`	Collects troubleshooting information about the installation process.	Management server

Command name	Functionality	Systems for the command to be executed in
addfwlist.bat	Sets up Windows Firewall exceptions for JP1/IT Desktop Management.	Management server
resetnid.vbs	Resets the unique ID (host ID) that is generated by the agent for identifying devices.	Agent
getinv.vbs	Collects device information about offline computers.	Agent
ioassetsfieldutil export	Exports the definitions of common management fields and additional management fields.	Management server
ioassetsfieldutil import	Imports the definitions of common management fields and additional management fields.	Management server

In a multi-server configuration:

Command name	Functionality	Systems for the command to be executed in
ioutils exportasset	Exports hardware asset information.	Database server
ioutils importasset	Imports hardware asset information.	Database server
ioutils exportfield	Exports custom field settings.	Database server
ioutils importfield	Imports custom field settings.	Database server
ioutils exporttemplate	Exports templates that define field mappings that are used when importing asset information.	Database server
ioutils importtemplate	Imports templates that define field mappings that are used when importing asset information.	Database server
ioutils exportdevice	Exports device information.	Database server
ioutils exportdevicedetail	Exports device information details.	Database server
ioutils exportpolicy	Exports security policy settings.	Database server
ioutils importpolicy	Imports security policy settings.	Database server
ioutils exportupdategroup	Exports update group settings.	Database server
ioutils importupdategroup	Imports update group settings.	Database server
recreatelogdb	Rebuilds indexes for the operation logs stored in the site server.	Site server
movelog	Moves operation log data within the site server.	Site server
deletelog	Deletes operation log data from the site server.	Site server
ioutils exportfilter	Exports filter settings.	Database server
ioutils importfilter	Imports filter settings.	Database server
updatesupportinfo	Registers support information that was downloaded from the support service site.	Database server
exportdb	Acquires data that the management server manages for backup purposes.	Database server
importdb	Restores data managed by the management server to the state of the last backup point.	Database server
reorgdb	Reorganizes the database.	Database server

Command name	Functionality	Systems for the command to be executed in
`stopservice`	Stops the services on the management server.	Management server Database server
`startservice`	Starts the services on the management server.	Management server Database server
`getlogs`	Collects troubleshooting information from the management server.	Management server Database server
`getinstlogs`	Collects troubleshooting information about the installation process.	Management server Database server
`addfwlist.bat`	Sets up Windows Firewall exceptions for JP1/IT Desktop Management.	Management server Database server Site server
`resetnid.vbs`	Resets the unique ID (host ID) for identifying devices that is generated by the agent.	Agent
`getinv.vbs`	Collects device information about offline computers.	Agent
`ioassetsfieldutil export`	Exports the definitions of common management fields and additional management fields.	Database server
`ioassetsfieldutil import`	Imports the definitions of common management fields and additional management fields.	Database server

17.4 ioutils exportasset (Exporting hardware asset information)

Functionality

This command exports hardware asset information to a CSV file.

For asset items displayed in a dash ("-") in the Asset module, a null value is exported. Using null values lets you avoid causing errors if the exported data is imported back without any modification. A file is exported even when no information items are available to export.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportasset -export export-file-name [ -filter filter-name][ -
encoding character-encoding][ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to export.

-filter *filter-name*

To export hardware asset information using a filter, select a filter name that is displayed in menu area in the operation window.

-encoding *character-encoding*

Specify a character code for hardware assert information to export. The following types of character codes can be specified. When you do not specify this argument, the character code is set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:
  In a single-server configuration system: When the management server is already set, and the server has started
  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`

Return values

The following table shows the return values of the `ioutils exportasset` command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
70	The specified filter does not exist.
101	Command execution failed because there is not enough memory, or due to some other.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export hardware asset information to C:\temp\hardwareexpo.csv.

ioutils exportasset -export C:\temp\hardwareexpo.csv -encoding UTF-8 -s

Related Topics:

- 17.1 Executing commands

17.5 ioutils importasset (Importing hardware asset information)

Functionality

This command imports hardware asset information using a CSV file. For details about hardware asset items and the CSV file description format, see theJob Management Partner 1/IT Desktop Management Overview and System Design Guide.

When a CSV file is imported, hardware asset information is updated with the values set in the CSV file. However, items whose values are empty in the CSV file will not be updated after importing (that is, null values are not overwritten).

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils importasset -import import-file-name -template template-name [ -
encoding character-encoding]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to import.

-template *template-name*

Specify a template to use for importing.

Only the items specified in the template will be imported.

If the specified items in the template do not exist in the import file, importing is performed as follows:

- Non-existent items are treated as omitted, and the values at the time of omission will be set for the asset information when importing is finished. The omitted items are not overwritten when importing overwrites the asset information.
- If a column associated with a mapping key does not exist, an error occurs and importing fails.

-encoding *character-encoding*

Specify a character encoding for the hardware assert information to import. The following types of character codes can be specified. When you do not specify this argument, the character code is set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP

- JIS

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`

Return value

The following table shows the return values of the `ioutils importasset` command.

Return values	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
72	The specified template does not exist.
80	The format of the file being imported is invalid.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to import the hardware asset information file hardwareexpo.csv, which was exported to C:\temp\, using a template specified for importing hardware asset information.

ioutils importasset -import C:\temp\hardwareexpo.csv -template for hardware asset information import-encoding UTF-8

Related Topics:

- 17.1 Executing commands

17.6 ioutils exportfield (exporting custom field settings)

Functionality

This command exports custom field settings to an XML file. One or more of the following fields can be specified:

- Hardware Asset Information
- Software License Information
- Contract Information

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportfield -export export-file-name -fieldtype type-of-custom-
field[ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-fieldtype *type-of-custom-field*

Specify the type of custom filed to export. The following types of custom fields are available:

- hardware: Hardware asset information field
- license: Software license Information field
- contract: Contract information field

Two or more field types can be specified. To export multiple filed types, use comma (",") to separate values.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.

- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`

Return value

The following table shows the return values of the `ioutils exportfield` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.

Return value	Description
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export the hardware asset information and software license information fields to C:\temp\hardexportfield.xml.

ioutils exportfield -export C:\temp\hardexportfield.xml -fieldtype hardware,license -s

Related Topics:

- 17.1 Executing commands

17.7 ioutils importfield (importing custom field settings)

Functionality

This command imports custom fields from an XML file. You can only import the files to which custom fields were previously exported.

This command only allows the adding of custom fields by importing. Fields cannot be added or changed with this command. Use this command to restore the custom fields from a backup file that was previously exported to, in the event of a failure or environment migration.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils importfield -import import-file-name
```

Argument

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`

- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

Return values

The following table shows the return values of the `ioutils importfield` command.

Return value	Description
0	The command finished normally.
1	Custom fields were imported normally, but some services have not started.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
80	The format of the file being imported is invalid.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to import previously exported file hardexportfield.xml. in C:\temp \.

ioutils importfield -import C:\temp\hardexportfield.xml

Related Topics:

- 17.1 Executing commands

17.8 ioutils exporttemplate (exporting template)

When importing asset information, you can use a template that defines field mappings. This section describes the `ioutils exporttemplate` command used to export the template.

Functionality

This command exports a template whose type and name you can specify. One of the following template types can be specified:

- Hardware Asset Information
- Software License Information
- Managed Software Information
- Contract Information
- Contact Vendor List

If you have multiple JP1/IT Desktop Management systems configured, this command enables a template created on one management server to be reused on another management server.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exporttemplate -export export-file-name -templatetype template-type
-name template-name[ -s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-templatetype *template-type*

Specify a template type to export. The following types of template type can be specified:

- assetImport: Template for importing hardware asset information
- licenseImport: Template for importing software license information
- softwareImport: Template for importing managed software information
- contractImport: Template for importing contract information
- vendorCatalogImport: Template for importing contract vendor list information

-name *template-name*

Specify a template name to export.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`

Return value

The following table shows the return values of the `ioutils exporttemplate` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
72	The specified template does not exist.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to export "hardware asset information template1" into C:\temp \assetexport.xml, which can be used as a template for importing hardware asset information.

ioutils exporttemplate -export C:\temp\assetexport.xml -templatetype assetImport -name "hardware asset information template1" -s

Related Topics:

- 17.1 Executing commands

17.9 ioutils importtemplate (importing a template)

When importing asset information, you can use a template that defines field mappings. This section describes the `ioutils importtemplate` command to be used to import the template.

Functionality

This command imports previously exported templates. The files you can import are only previously exported templates. You can provide a template name to register. If you do not specify a name, a template is registered with the name from a previous export.

If you have multiple JP1/IT Desktop Management systems configured, this command enables a template created on one management server to be reused on another management server.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils importtemplate -import import-file-name[ -name template-name][ -s]
```

Argument

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *template-name*

Specify a template name to import. If this argument is omitted, the template name from a previous export will be used.

-s

Overwrites the file even if a template with the same file name already exists. If this argument is not specified and a template with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the input or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`

- importdb
- ioassetsfieldutil export
- ioassetsfieldutil import
- ioutils exportasset
- ioutils exportdevice
- ioutils exportdevicedetail
- ioutils exportfield
- ioutils exportfilter
- ioutils exportoplog
- ioutils exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils importasset
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importupdategroup
- reorgdb
- startservice
- stopservice
- updatesupportinfo

Return value

The following table shows the return values of the `ioutils importtemplate` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
74	An invalid template name is specified.
80	The format of the file being imported is invalid.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to import a previously exported template file called assetexport.xml in C:\temp\, as a hardware asset information template named "hardware asset information template1".

ioutils importtemplate -import C:\temp\assetexport.xml -name "hardware asset information template1" -s

Related Topics:

- 17.1 Executing commands

17.10 ioutils exportdevice (exporting device information)

This section describes the `ioutils exportdevice` command to export device information.

Functionality

This command exports device information to a CSV file. A file is exported even when no information items are available to export.

If you have multiple JP1/IT Desktop Management systems configured, device information in one system can be reused in another system.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportdevice -export export-file-name[ -filter filter-name][ -
encoding character-encoding][ -s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to export.

-filter *filter-name*

Specify a filter name that is displayed in the menu area in the operation window, to export device information using a filter.

-encoding *character-encoding*

Specify a character code for device information to export. The following types of character codes can be specified. When you do not specify this argument, the character code is set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location of the file to be executed, by using the built-in command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following situations:

  In a single-server configuration system: When the management server setup is completed and the management server is not running

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
- The argument `-s` cannot be specified in a cluster environment or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

The following table shows the return values of the `ioutils exportdevice` command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
70	The specified filter does not exist.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export device information to C:\temp\deviceexpo.csv.

ioutils exportdevice -export C:\temp\deviceexpo.csv -encoding UTF-8 -s

Related Topics:

- 17.1 Executing commands

17.11 ioutils exportdevicedetail (exporting device information details)

This section describes the `ioutils exportdevicedetail` command for exporting device information details.

Functionality

This command exports device information details to a CSV file. A file is exported even when no information items are available to export.

If you have multiple JP1/IT Desktop Management systems configured, device information in one system can be reused in another system.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportdevicedetail -export export-file-name[ -template template-
name][ -filter filter-name][ -encoding character-encoding][ -s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to export.

-template *template-name*

Specify a template name to be used for export. The specified fields in the template will be exported in the specified encoding.

-filter *filter-name*

Specify a filter name that is displayed in the menu area in the operation window, to export device information using a filter.

-encoding *character-encoding*

Specify a character code for device information to export. The following types of character codes can be specified. When this argument is omitted, the character code is set to the one specified in the template if a template is specified. If a template is not specified, it is set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying storage location for the executable file, by using the built-in command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed and the management server is not running

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`

- The argument `-s` cannot be specified in a cluster environment or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

The following table shows the return values of the `ioutils exportdevicedetail` command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
70	The specified filter does not exist.
72	The specified template does not exist.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export device information to "C:\temp\devicedetailexpo.csv."

ioutils exportdevice -export C:\temp\deviceexpo.csv -encoding UTF-8 -s

Related Topics:

- 17.1 Executing commands

17.12 ioutils exportpolicy (exporting security policy settings)

Functionality

This command exports security policy settings to a specified file.

For an environment with multiple JP1/IT Desktop Management systems configured, this command enables security policy settings created on one management server to be reused on another management server.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportpolicy -export export-file-name -name security-policy-name[ -
s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-name *security-policy-name*

Specify a security policy name to export.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`

- `ioutils exportasset`
- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

- If a package is specified as a auto-enforce program for mandatory software defined in a security policy, the security policy cannot be exported.

Return value

The following table shows the return values of the `ioutils exportpolicy` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
75	The specified security policy does not exist.
85	A package exists.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export security policy settings called "policy for development group" to C:\temp\exportpolicy.xml.

ioutils exportpolicy -export C:\temp\exportpolicy.xml -name "policy for development group" -s

Related Topics:

- 17.1 Executing commands

17.13 ioutils importpolicy (importing security policy settings)

Functionality

This command imports previously exported security policy settings. You can only import the files that were previously exported. If you do not specify a security policy name, the security policy is registered with the name of the previous export.

If you have multiple JP1/IT Desktop Management systems configured, security policy settings created on one management server can be reused on another management server.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils importpolicy -import import-file-name[ -name security-policy-name]
[ -applygroup update-group-name-to-apply][ -excludegroup excluded-update-
group-name][ -s]
```

Argument

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *security-policy-name*

Specify a security policy name to import. If this argument is omitted, the security policy name from a previous export will be used.

-applygroup *update-group-name-to-apply*

Specify a name for the update group. If this argument is omitted, the update group name from a previous export will be applied.

-excludegroup *excluded-update-group-name*

Specify a name for the excluded update group. If this argument is omitted, the excluded update group name from a previous export will be applied.

-s

Overwrites the file even if a security policy with the same file name already exists. If this argument is not specified and a security policy with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the input or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.

- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
- When importing the exported security policy data containing tasks specified in it, the command checks whether the same task name already exists in the import destination folder. When the same task is detected, the task name being imported is prefixed with *imp_N_* (where *N* is an integer that is at least 1). If the task name exceeds the size limit, excess characters are omitted from the last part of the task name.

Return value

The following table shows the return values of the `ioutils importpolicy` command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
31	Another command is being executed.

Return value	Description
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
76	An invalid security policy name is specified.
80	The format of the file being imported is invalid.
83	No corresponding update group matches.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to import the previously exported security policy settings file exportpolicy.xml into C:\temp\, as a import name "policy for a development group." The excluded update group name is assumed to be "policy for Windows XP."

ioutils importpolicy -import C:\temp\exportpolicy.xml -name "policy for development group" -excludegroup "policy for Windows XP" -s

Related Topics:

- 17.1 Executing commands

17.14 ioutils exportupdategroup (exporting update group settings)

Functionality

This command exports update group settings to a specified file.

If you have multiple JP1/IT Desktop Management systems configured, an update group setting in one system can be reused in another system.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportupdategroup -export export-file-name -name update-group-
name[ -s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-name *update-group-name*

Specify an update group name whose settings you want to export.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location of the file to be executed by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`

- `ioutils exportasset`
- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

Return value

The following table shows the return values of the `ioutils exportupdategroup` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
83	No corresponding update group matches.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to export setting of an update group called "excluded group for headquarters" to C:\temp\updategroup.xml.

ioutils exportupdategroup -export C:\temp\updategroup.xml -name "excluded group for headquarters" -s

Related Topics:

- 17.1 Executing commands

17.15 ioutils importupdategroup (importing update group settings)

Functionality

This command imports previously exported update group settings. Only the files that the update group was exported into are allowed to be imported.

If you have multiple JP1/IT Desktop Management systems configured, an update group setting in one system can be reused in another system.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils importupdategroup -import import-file-name[ -name update-group-name]
[ -s]
```

Argument

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *update-group-name*

Specify an update group name to import. If this argument is omitted, the update group name specified in the previous export will be used.

-s

Overwrites the file even if an update group with the same file name already exists. If this argument is not specified and an update group with the same name already exists, an overwrite confirmation message appears. In this case, the system cancels the input or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following situations:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`

- `ioassetsfieldutil import`
- `ioutils exportasset`
- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

Return value

The following table shows the return values of the `ioutils importupdategroup` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
79	The specified update group name is invalid.
80	The format of the file being imported is invalid.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to import the previously exported update group settings file updategroup.xml in C:\temp\, with the import name "excluded group for headquarters".

ioutils importupdategroup -import C:\temp\updategroup.xml -name "excluded group for headquarters" -s

Related Topics:

- 17.1 Executing commands

17.16 ioutils exportoplog (exporting operation logs)

Functionality

This command exports operation logs on the management server into a CSV file at a specified time. Distributed operation logs stored in the site server cannot be exported.

If the size of the export file exceeds 2 GB, the file is split into multiple files. The split files are renamed with sequence numbers added at the end of the file names.

Even when no information items are available to export, a file is always exported.

For details about the output format of the file to be exported, see A.6 Output format of exported operation logs.

Execute this command on the management server in a single-server configuration system.

Format

```
ioutils exportoplog -export export-file-name{ -range export-period-of-time|
-within export-number-of-days}[ -encoding character-encoding][ -filter
filter-name][ -linenumber-of-lines-to-export][ -s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to export.

-range *export-period-of-time*

Specify export period of time in *YYYY-MM-DD*# format. The start date and the end date can be separated with a comma (",").

YYYY: year, MM: month, DD: day

This argument cannot be specified together with `-within`.

-within *export-number-of-days*

Specify the number of days of the logs to export. The number must be between 1 and 500.

This argument cannot be specified together with `-range`.

-encoding *character-encoding*

Specify a character code for the operation logs to export. The following types of character codes can be specified. When you do not specify this argument, the character code is automatically set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP

- JIS

-filter *filter-name*

Specify a filter name if you want to export specific operation logs using a filter.

In the filter conditions of the specified filter name, do not include **Operation Date/Time (Browser)**. If you specify a filter name whose filter conditions include **Operation Date/Time (Browser)**, filtering might not be performed correctly.

-line *number-of-lines-to-export*

Specify the number of lines you want to export into 1 file. The number must be between 1 and 4294967295. If this argument is omitted, 2 GB worth of operation logs are output to one file.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command when the management server setup is completed, and the services on the management server have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`

- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

Return value

The following table shows the return values of `ioutils exportoplog` command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server has not been set up.
70	The specified filter does not exist.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export operation logs to C:\temp\exportoplog.csv, with the number of days to export "25", and using a filter called "file copy operations"

ioutils exportoplog -export C:\temp\exportoplog.csv -within 25 -encoding UTF-8 -filter "file copy operations" -s

Related Topics:

- 17.1 Executing commands

17.17 recreatelogdb (recreating an operation log index on the site server)

This section describes the `recreatelogdb` command, which re-creates indexes to view the operation logs stored on the site server.

Functionality

This command re-creates indexes to be used for referring to the operation logs stored on the site server. It also reports the list of agent-operated logs managed by the site server up onto the management server.

Indexes are created on each site server and reported to the management server. When viewing the distributed operation logs from the operation window, the operation logs are searched through using the index information and thus the logs on the site server can be reached.

Operation logs stored on the site server cannot be viewed correctly if an inconsistency is introduced between the operation log data and the indexes on the site server due to the operation log data being manually added or removed, or if index information is corrupted due to a system failure. In such cases, you can use the `recreatelogdb` command. An operation log index will be re-created and the operation logs on the site server will be properly referred to.

Execute the `recreatelogdb` command in cases like the following:

- When operation log data is deleted from its own storage folder on the site server
- When backup data for the operation log is restored (added) to the site server
- When operation log data is copied or moved from an another site server
- When the operation log database on the site server is corrupted
- When the database on the management server is corrupted

This command must be executed on the site server.

Format

```
recreatelogdb{ -all| -add| -node}
```

Argument

-all

Re-creates indexes of the operation logs stored in the site server. Indexes are recreated after the command is completed, when the site server is started. Specify this argument to re-create indexes in such cases as when operation log data is moved or the database on the site server is corrupted.

If this command is executed with this argument when the site server is started, the server stops during command execution. The site server starts again when the command is completed. If this command is executed when the site server is stopped, the server remains stopped after the command is completed.

-add

Creates additional operation log indexes. Indexes are created after the command is completed, when the site server is started. Specify this argument when additional operation logs are added to the site server. For example, specify when operation log data is moved from another site server.

If the command is executed with this argument when the site server is started, the server stops during command execution. The site server starts again when the command is completed. If this command is executed when the site server is stopped, the server remains stopped after the command is completed.

-node

Reports the list of agent-operated logs managed by the site server up onto the management server. An index is not recreated. Specify this argument in the following cases:

- There is no defect in the database on the site server, but database on the management server is corrupted. The operation logs cannot be searched correctly.
- When the site server connection destination is changed to a management server in another system
- When the database is rebuilt (the `updatesupportinfo` command is executed) on the management server

Storage location

site-server-installation-folder\mgr\bin\

Notes

- When an argument other than `-node` is specified with the `recreatelogdb` command, the site server stops during command execution. Operation logs generated during the command execution cannot be viewed until the command is completed. Once the `recreatelogdb` command is completed, index creation begins when the site server starts. As the index creation process increases your server load, it might take a couple of days for the process to complete, depending on the size of the data. Operation logs generated during index creation cannot be viewed until index creation is completed. Keep these considarations in mind when executing the `recreatelogdb` command.
- If the job status recording file for the `deletelog` command (`deletelog_lasttime.txt`) exists in the work folder, the `recreatelogdb` command fails. In such a case, re-execute the `deletelog` command to complete deletion of the operation logs, and then execute the `recreatelogdb` command.
- If you moved operation logs to the data folder, and then re-created operation log indexes with the argument `-all` or `-add` specified, always execute the `recreatelogdb` command with the argument `-node`. By executing this command, a list of agent-operated logs is reported to the management server. If the logs are not reported to the server, a search through the operation logs might not be performed correctly.
- Execute this command when the site server setup is completed.
- This command cannot be simultaneously executed by multiple users.

Return value

The following table shows the return values of the `recreatelogdb` command.

Return value	Description
0	The command finished normally.
1	A warning was raised during command execution. The command stopped.
11	The specified format for the argument is incorrect.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The site server has not been set up.
58	Failed to connect to the management server.
62	A file access error occurred.
67	A job status recording file for the `deletelog` command exists.
101	Command execution failed because there is not enough memory, or due to some other reason.
102	Failed to automatically stop the site server.

Return value	Description
120	A database access error occurred.

Example

The following example shows use of this command to re-create indexes of the operation logs, in case the database on the site server has been corrupted.

recreatelogdb -all

Related Topics:

- 17.1 Executing commands

17.18 movelog (moving operation logs on the site server)

This section describes the `movelog` command, which moves operation log data to another folder within the site server.

Functionality

This command moves operation log data to a folder you specify on the site server.

You can use this command, for instance, to tweak your operational environment by installing an additional hard disk on the site server to save operation logs. This can be done by first changing storage folders of the operation logs during a site server setup, and then executing the `movelog` command to move the operation logs to a new storage folder.

This command stops the site server if the server is started at the time of command execution. The site server starts again when the command is completed. If this command is executed when the site server is stopped, the server remains stopped after the command is completed.

Execute this command on the site server.

Format

```
movelog -source folder-name-to-move-from -destination folder-name-move-to
```

Argument

-source *folder-name-to-move-from*

Specify the absolute path of the folder in which operation log data is stored.

The storage folder of the operation logs cannot be specified. Change the storage folder during the server setup before you execute this command.

-destination *folder-name-to-move-to*

Specify the absolute path of the folder into which to move the operation log data. To specify a path containing a space, enclose the strings with double quotation marks (").

The destination folder must be empty to move the data.

Storage location

site-server-installation-folder\mgr\bin\

Notes

- Even if the command fails to delete the source data, the command itself completes properly. If this happens, manually delete the source data.
- Execute this command when the site server setup is completed.
- This command cannot be simultaneously executed by multiple users.

Return value

The following table shows the return values of the `movelog` command.

Return value	Description
0	The command finished normally.
1	A warning was raised during command execution. The command stopped.
11	The format for specifying the command arguments is invalid.

Return value	Description
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The site server has not been set up.
61	The specified source folder is either the current storage folder or a folder that does not contain any operation logs, or the destination folder is not empty.
62	A file access error occurred.
101	Command execution failed because there is not enough memory, or due to some other reason.
102	Failed to automatically stop the site server.
120	A database access error occurred.

Example

The following example shows use of this command to move operation log data stored in D:\log_data_old to E:\log_data_new. In this example, the storage folder for the operation logs is assumed to have already been changed to E:\log_data_new during server setup.

movelog -source D:\log_data_old -destination E:\log_data_new

Related Topics:

- 17.1 Executing commands

17.19 deletelog (deleting operation logs on the site server)

Functionality

This command deletes operation log data for a specified period of time from the site server.

Use this command to delete any unnecessary operation logs if the disk space on the server is running out due to increasing logged data.

If this command is executed when the site server is started, the server stops during the command execution. The site server starts again when the command is completed. If this command is executed when the site server is stopped, the server remains stopped after the command is completed.

Execute this command on a site server.

Format

```
deletelog {-date date|-days number-of-days}[ -reorg][ -work work-folder-
name][ -s]
```

Arguments

-date *date*

Specify a base-point date (using the site server's local time) to delete operation logs. Operation logs of the base-point date and older will be deleted.

The date should be specified in YYYY-MM-DD format.

- YYYY: year (1970-9990)
- MM: month (01-12)
- DD: day (01-31)

If an invalid date is specified, the command returns an error. If you specify the exact date when this command is executed, or specify a future date, all operation logs will be deleted. The command returns an error if the operation log does not exist on the specified date.

Operation logs are managed on an hour-by-hour basis. If the command is executed in a time zone where the time difference from UTC is 15 or 30 minutes after the hour, the operation logs might only be deleted up to 23:45 or 23:30.

-days *number-of-days*

Specify the number of days for operation logs to be retained in the database. Operation logs for the time period of days specified here will be retained in the database, starting from the exact date when the command was executed. Other logs older than this period will be deleted.

Specify the number of days in the range 0-9999. When 0 is specified, all operation log data will be deleted.

Operation logs are managed on an hour-by-hour basis. If the command is executed in a time zone where the time difference from UTC is 15 or 30 minutes after the hour, the operation logs might only be deleted up to 23:45 or 23:30.

-reorg

Specify this to reorganize the database when operation logs are deleted.

If operation logs are deleted repeatedly, the database might be fragmented, causing reduced access speed to the database and other problems. If database access speed is reduced, add `-reorg` to the command to reorganize the database along with deleting the logs.

-work *work-folder-name*

Specify the absolute path to the backup folder in which the operation logs to remain in the database will be backed up. Only folders in the local drive can be specified.

The folder name must be 120 characters or less. Half-width alphanumeric characters, white space, and the following special characters are allowed:

"#" "@" "\" ":" "."(period) "(" ")"

If the specified folder does not exist, a new folder will be created.

When this argument is omitted, the folder below is used as a work folder:

data-folder\SITE\OPLOG\DELETELOG

-s

A confirmation prompt pops up during command execution. Specify this argument if you don't want the message to appear.

Storage location

site-server-installation-folder\mgr\bin\

Notes

- If the command stops due to a failure or is canceled by an administrator, the delete process of the operation logs will be aborted. Execute the command again to resume the delete operation. Arguments other than `-s` remain specified in the same condition used for the previous execution. A confirmation message comes up when resuming the command.

  The `deletelog` command records the progress status. This feature automatically applies the last conditions used for the command when it is re-executed, so that the operation logs are deleted correctly. However, if the progress status fails to be reloaded, you are not asked whether to continue re-execution. In this case, create the index information for the operation logs again by executing `recreatelogdb` command with `-all` specified in order to be able to refer to the remaining operation logs.
- The work folder requires enough free space to run the delete operation. The following is the equation for estimating the work folder capacity:

  Required size for the work folder (in bytes) = number of operation logs to retain in database x 67 + number of computers connecting to the site server to obtain distributed operation logs x (1,066 + number of days to retain operation logs in database x 500)
- Execute this command when site server setup is completed.
- This command cannot be simultaneously executed by multiple users.

Return value

The following table shows the return values of the `deletelog` command.

Return value	Description
0	The command finished normally.
1	A warning was raised during command execution. The command stopped.
2	Operation log data to delete does not exist.
11	The format for specifying the command arguments is invalid.
12	An invalid work folder was specified.
13	An invalid date was specified.
31	Another command is being executed.

Return value	Description
51	You do not have the permissions to execute this command.
54	The site server has not been set up.
62	A file access error occurred.
66	The work folder does not have enough free space.
101	The command execution failed due to not enough memory or some other reason.
102	Failed to automatically stop the site server.
103	Failed to report information to the management server.
120	A database access error occurred.

Example

The following example uses this command to delete operation log data stored in the site server, leaving operation logs for 120 days, beginning with the date when the command is executed, and then reorganize the database.

deletelog -days 120 -reorg

Related Topics:

- 17.1 Executing commands
- 17.17 recreatelogdb (recreating an operation log index on the site server)

17.20 ioutils exportfilter (exporting filter settings)

Functionality

This command exports filtering criteria. You can use one of the predefined filters displayed in the menu area in the following views.

- Hardware Assets
- Software Licenses
- Managed Software
- Contracts
- Device Inventory
- Software Inventory
- Computer Security Status
- Operation logs
- Windows Update
- Event list
- Packages
- Tasks
- Network Filter List#

#: This filter can be defined in the Settings module, **Network Access Control**, and the **Network Filter Settings** view by entering in the information area.

If you have multiple JP1/IT Desktop Management systems configured, a filter in one system can be reused in another system.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils exportfilter -export export-file-name -filtertype filter-type -name
export-filter-name[ -s]
```

Argument

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-filtertype *filter-type*

Specify a filter type to export. The following types of filters can be specified:

- asset: hardware assets
- license: software licenses
- mngsoft: managed software

- contract: contracts
- device: device inventory
- inssoft: software inventory
- secdevice: Computer Security Status
- oplog: operation logs
- update: windows update
- event: event list
- package: packages
- task: tasks
- netctl: Network Filter List

-name *export-filter-name*

Specify a filter name to export.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`

- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

The following table shows the filtering criteria that cannot be exported.

Item	Filtering criteria that cannot be exported when:
Device type	When the filter contains any optional items added by the user (such as the device type, asset status etc.)
Asset type	
Planned asset status	
License type	
License status	
Planned license status	
License type	
Contract type	
Contract status	
Department	When filter contains Department filed
Location	When filter contains Location field

Return value

The following table shows the return values of the `ioutils exportfilter` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient capacity.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.

Return value	Description
70	The specified filter does not exist.
86	Some items cannot be exported.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to export a hardware asset filter called "low-end computer" to C:\temp\exportfilter.xml.

ioutils exportfilter -export C:\temp\exportfilter.xml -filtertype asset -name "low-end computer" -s

Related Topics:

- 17.1 Executing commands

17.21 ioutils importfilter, importing filter settings

Functionality

This command imports previously exported filters. You can only import a file into which filters were previously exported.

If you have multiple JP1/IT Desktop Management systems configured, a filter in one system can be reused in another system.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
ioutils importfilter -import import-file-name[ -name filter-name][ -s]
```

Argument

-export *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *filter-name*

Specify a filter name to import. If the filter name is omitted, the name from a previous export will be used.

-s

Overwrites a filter with the same name if it is already exists without displaying an overwrite confirmation message. If this argument is not specified and a filter with the same name already exists, an overwrite confirmation message appears. In this case, the system cancels the input or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following situations:

  In a single-server configuration system: When the management server setup is completed, and the services on the management server have started.

  In a multi-server configuration system: When the management server and database server are already set, and the services on both servers have started.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`

- `ioutils exportasset`
- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

Return value

The following table shows the return values of the `ioutils importfilter` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, the disk does not have sufficient capacity, or the folder does not exist.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The management server or database server has not been set up.
77	The specified filter does not exist.
80	The format of the file being imported is invalid.
84	A custom field for asset management does not match between the export-from location and the import-to location.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.
150	Command execution was interrupted due to some other error.

Example

The following examples shows use of this command to import a previously exported filter, exportfilter.xml in C:\temp \, as a import filter name "PC to dispose."

ioutils importfilter -import C:\temp\exportfilter.xml -name "PC to dispose" -s

Related Topics:

- 17.1 Executing commands

17.22 updatesupportinfo (uploading support service information)

This section describes the `updatesupportinfo` command, which uploads information downloaded from the support service site to the management server.

Functionality

If the management server cannot connect to the support service site, you need to manually upload the latest information onto the management server.

First, connect to the support service site using a computer that has access to external networks to download the latest information. Copy the downloaded data manually to the management server (in a single server configuration system) or to the database server (in a multi-server configuration system), and execute the command. The latest information will be uploaded to the management server.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

```
updatesupportinfo -i support-information-file-name
```

Argument

-i *support-information-file-name*

Select the absolute path to the file to be registered to the management server (a support information file). To specify a path containing a space, enclose the strings with double quotation marks (").

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`

- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`

- This command cannot be executed when setup or database manager is running on the management server or database server

Return value

The following table shows the return values of `updatesupportinfo` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified file is invalid, or the file does not exist.
31	Another command is being executed.
37	The data folders shared among servers cannot be accessed due to the database server being stopped or a network failure.
38	The data folders shared among servers cannot be accessed due to invalid credentials.
51	You do not have the permissions to execute this command.
53	Services on either the management server or database server have not started.
54	The management server or database server has not been set up.
101	Failed to update all or some of the support information.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to upload a support information file called supportinfo.zip in C:\temp, onto the management server.

updatesupportinfo -i C:\temp\supportinfo.zip

Related Topics:

- 17.1 Executing commands

17.23 exportdb (acquiring backup data)

This section describes the `exportdb` command used to export data on the management server for backup purposes.

Functionality

This command exports data on the management server for backup purposes. The acquired backup can be used for data restoration in the event of a failure.

When you execute this command, a new backup storage folder is created with the name of *YYYYMMDDhhmmss*# under the backup folder you specify in the argument. The backup file will be created in this folder.

YYYY: year, MM: month, DD: day, hh: hours, mm: minutes, ss: seconds

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

In a multi-server configuration system, execute the commands in the following order:

1. Execute the `stopservice` command on the management server. Alternatively, you can go to the Windows **Start** menu, and select **Administrative Tools** and then **Services** to stop the following services:
   - JP1_DTNAVI_WEBCON
   - JP1_DTNAVI_AGCTRL
   - JP1_DTNAVI_MGRSRV
2. Execute the `stopservice` command on the database server.
3. Execute the `exportdb` command on the database server.

Format

```
exportdb[ -f backup-folder][ -s]
```

Arguments

-f *backup-folder*

Specify the absolute path to the backup storage folder. Only the folders in local drive can be specified. The size of the backup file varies depending on the operational environment and how long JP1/IT Desktop Management has been used. Make sure to keep enough free space for the disk drive in which the backup folder resides. The amount of space required is greater than the sum of the size of the database folder and the data folders that are already taking up capacity.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 135 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If any characters other than above are used for the JP1/IT Desktop Management installation folder, always specify this argument. If this argument is not specified, the following folder is used for the backup folder.

- When this argument is specified:
  *folder-specified-in-argument**YYYYMMDDhhmmss*

- When this argument is omitted:
  JP1/IT Desktop Management-installation-folder\mgr\backup*YYYYMMDDhhmmss*

Example:

If the command is executed on January 1, 2011 at 2:30:00:
JP1/IT Desktop Management-installation-folder\mgr\backup\20110101023000

-s

Specify this argument to stop management server services (`stopservice` command), exporting data backup (`exportdb` command), and start management of the server service (`startservice` command) automatically.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:
  In a single-server configuration system: When the management server is already set, and the server is stopped
  In a multi-server configuration system: When the database server is completed, and the services on the management server and the database server are not running
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`

- `startservice`
- `stopservice`
- `updatesupportinfo`

- The argument `-s` cannot be specified in a cluster environment or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

The following table shows the return values of the `exportdb` command.

Return value	Description
0	The command finished normally.
1	The backup was exported successfully, but the automatic starting of the management server failed.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid or the folder does not exist.
31	Another command is being executed.
32	A backup storage folder that was created at the same time exists.
33	The disk does not have enough space.
34	Failed to start the database.
35#	The management server or the database server was in a starting process when the command is executed.
36	The database was in a shutdown process when the command is executed.
51	You do not have the permissions to execute this command.
52	The argument `-s` is specified in a cluster environment or in a multi-server configuration system.
53	The management server has not stopped in a single-server configuration system. The management server or database server has not stopped in a multi-server configuration system.
54	The management server or database server has not been set up.
55	The default backup storage folder cannot be used.
61	Cannot connect to the backup folder for the operation logs.
62	Cannot log in to the backup folder for the operation logs.
63	The operation log-related folder does not have enough free space.
64	The backup of the operation log was interrupted due to some other error.
101	Failed to export backup data.
102	Failed to automatically stop the management server.
110	The command execution failed due to a problem with a license.
150	The command execution was interrupted due to some other error.

#: The value to be returned when argument `-s` is specified

Example

The following example shows use of this command to export backup data to C:\tmp\backup, stop the management server services, export data backup, and start the management server service automatically.

exportdb -f C:\tmp\backup -s

Related Topics:

- 17.1 Executing commands

17.24 importdb (restoring backup data)

This section describes the `importdb` command that restores data owned by the management server to the state of the last backup point.

Functionality

This command restores data owned by the management server to the state of the last backup point in case a disk failure occurs. To restore data, a backup file acquired with the `exportdb` command is used.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

In a multi-server configuration system, execute the commands in the following order:

1. Execute the `stopservice` command on the management server. Alternatively, you can go to the Windows **Start** menu and select **Administrative Tools** and then **Services**, to stop the following services:
   - JP1_DTNAVI_WEBCON
   - JP1_DTNAVI_AGCTRL
   - JP1_DTNAVI_MGRSRV
2. Execute the `stopservice` command on the database server.
3. Execute the `importdb` command on the database server.

Format

```
importdb[ -f data-storage-folder-name][ -w work-folder-name][ -s]
```

Argument

-f *data-storage-folder-name*

Specify the absolute path to the folder in which the backup file of the target restore point resides. Only a folder in a local drive can be specified.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\ ) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If any characters other than above are used for the JP1/IT Desktop Management installation folder, always specify this argument.

The following data storage folders are used during command execution for restoring data, when this argument is specified or omitted.

When this argument is specified:

The data storage folder specified in the argument is used.

When this argument is omitted:

The most up-to-date data storage folder available under the path below is chosen by name.

JP1/IT Desktop Management-installation-folder\mgr\backup\

For example, if the folder has three data storage folders, \20110101023000, \20110102023000, and \20110103023000, then \20110103023000 will be chosen to be used for restoring.

-w *work-folder-name*

Specify the absolute path to the work folder to be used for restoring to the backup point. Only the folders in a local drive can be specified. 10 GB or more is required for the drive where the work folder resides, in order to manage 10,000 devices.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\ ) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If characters other than above are used for the JP1/IT Desktop Management installation folder, always specify this argument. If the specified folder does not exist, an error is returned.

When this argument is omitted, the folder below is used as a work folder.

JP1/IT Desktop Management-installation-folder\mgr\temp

-s

Specify if you want to automatically run a set of commands for stopping the management server services (the `stopservice` command), restoring the database with a backup (the `importdb` command), and starting the management server services (the `startservice` command).

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed and the management server is not running

  In a multi-server configuration system: When the database server is completed, and the services on the management server and the database server are not running
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`

- `ioutils exportupdategroup`
- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

- The argument `-s` cannot be specified in a cluster environment or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

The following table shows the return values of the `importdb` command.

Return value	Description
0	The command finished normally.
1	Restoration from a backup was successful, but a failure occurred with automatically starting the management server.
11	The format for specifying the command arguments is invalid.
12	The specified data storage folder is invalid, or the folder does not exist.
13	A backup file does not exist in the specified data storage folder.
14	The specified work folder is invalid, or the folder does not exist.
15	The disk does not have enough space.
31	Another command is being executed.
34	The starting of the database failed.
35#	The management server or the database server was in a start process when the command is executed.
36	The database was in a shutdown process when the command was executed.
51	You do not have the permissions to execute this command.
52	The argument `-s` is specified in a cluster environment or in a multi-server configuration system.
53	The management server has not stopped in a single-server configuration system The management server or database server has not stopped in a multi-server configuration system.
54	The management server or database server has not been set up.
55	The default data storage folder and the work folder are not usable.
56	A backup of an older version was specified.
61	Cannot connect to the backup folder for the operation logs.
62	Cannot log in to the backup folder for the operation logs.

Return value	Description
63	The operation log-related folder does not have enough free space.
64	The backup of the operation log was interrupted due to some other error.
101	A restoration using a backup failed.
102	Failed to automatically stop the management server.
110	Command execution failed due to a problem with the license.
150	Command execution was interrupted due to some other error.

#: The value to be returned when argument `-s` is specified

Example

The following example shows use of this command to stop the management server services, restore data using a backup acquired on January 3rd, 2011, 2:30:00 (in the backup data folder C:\tmp\backup\20110103023000), and start the management server services automatically.

```
importdb -f C:\tmp\backup\20110103023000 -s
```

Related Topics:

- 17.1 Executing commands

17.25 reorgdb (reorganizing the database)

Functionality

This command reorganizes the database. We recommend that administrators run this command regularly to maintain good database performance.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

In a multi-server configuration system, execute the commands in the following order:

1. Execute the `stopservice` command on the management server. Alternatively, you can go to the Windows **Start** menu and select **Administrative Tools** and then **Services**, to stop the following services:
   - JP1_DTNAVI_WEBCON
   - JP1_DTNAVI_AGCTRL
   - JP1_DTNAVI_MGRSRV
2. Execute the `stopservice` command on the database server.
3. Execute the `reorgdb` command on the database server.

Format

```
reorgdb[ -s][ -w work-folder-name]
```

Argument

-s

Specify if you want to run a set of commands for stopping management server services (the `stopservice` command), reorganizing the database (the `reorgdb` command), and starting the management server services (the `startservice` command) automatically.

-w *work-folder-name*

Specify the absolute path to the work folder to be used during database reorganization. Only a folder in a local drive can be specified. 30 GB or more free space is required for the drive where the work folder resides, in order to manage 10,000 devices. In a cluster configuration, specify a folder on the shared disk.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If any other characters than above are used for the JP1/IT Desktop Management installation folder, always specify this argument. If the specified folder does not exist, an error is returned.

When this argument is omitted, the folder below is used as a work folder.

JP1/IT Desktop Management-installation-folder\mgr\temp

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command in the following state:

  In a single-server configuration system: When the management server setup is completed and the management server is not running

  In a multi-server configuration system: When the database server is completed, and the services on the management server and the database server are not running
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
- The argument `-s` cannot be specified in a cluster environment or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

The following table shows the return values of the `reorgdb` command.

Return value	Description
0	The command finished normally.
1	Reorganization of the database was successful. But a failure occurred with automatically starting the management server.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, or the folder does not exist.
31	Another command is being executed.
33	The disk does not have enough space.
34	The starting of the database failed.
35#	The management server or the database server was in a start process when the command is executed.
36	The database was in a shutdown process when the command was executed.
51	You do not have the permissions to execute this command.
52	The argument `-s` is specified in a cluster environment or in a multi-server configuration system.
53	The management server has not stopped in a single-server configuration system The management server or database server has not stopped in a multi-server configuration system.
54	The management server or database server has not been set up.
55	The default work folder is not usable.
101	Reorganization of the database failed.
102	Failed to automatically stop the management server.
110	The command execution failed due to a problem with the license.
150	The command execution was interrupted due to some other error.

#: The value to be returned when argument `-s` is specified

Example

The following example shows how to use this command to stop the management server services, reorganize the database, and start the management server services automatically in a single-server configuration system.

```
reorgdb -s
```

Related Topics:

- 17.1 Executing commands

17.26 stopservice (stopping services)

Functionality

This command stops the services associated with the management server or the database server to stop the management server or the database server.

Execute this command on the management server in a single-server configuration system.

In a multi-server configuration system, execute the commands in the order below. It might take some time before the service stops, or an error might occur if the commands are executed in a wrong order.

1. Execute the `stopservice` command on the management server.
2. Execute the `stopservice` command on the database server.

Format

```
stopservice
```

Arguments

No arguments are available for this command.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command when the management server and the database server setup is completed.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`

- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `updatesupportinfo`

Return values

The following table shows the return values of the `stopservice` command.

Return value	Description
0	The command finished normally.
1	The management server or database server has already stopped.
31	Another command is being executed.
35	The management server or database server was in a startup process when the command is executed.
37	Failed to access to the data folder shared between servers. The database server was stopped, or a network failure has occurred.
38	Invalid credentials. The data folders shared between servers cannot be accessed.
51	You do not have the permissions to execute this command.
52	This command cannot be executed in a cluster environment.
54	The management server or database server has not been set up.
101	Failed to stop the services of the management server or database server.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to stop services of the management server.

stopservice

Related Topics:

- 17.1 Executing commands

17.27 startservice (starting services)

Functionality

This command starts the services associated with the management server or the database server to start up the management server or the database server.

Execute this command on the management server in a single-server configuration system.

In a multi-server configuration system, execute the commands in the order below. It might take some time before the service starts if the commands are executed in a wrong order.

1. Execute the `startservice` command on the database server.
2. Execute the `startservice` command on the management server.

Format

```
startservice
```

Arguments

No arguments are available for this command.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- Execute this command when the management server and the database server setup is completed.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`

- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `stopservice`
- `updatesupportinfo`

Return value

The following table shows the return values of the `startservice` command.

Return value	Description
0	The command finished normally.
1	The management server or database server has already started.
31	Another command is being executed.
35	The management server or database server was in a shutdown process when the command is executed.
37	Failed to access to the data folder shared between servers. The database server is stopped, or a network failure has occurred.
38	Invalid credentials. The data folders shared between servers cannot be accessed.
51	You do not have the permissions to execute this command.
52	This command cannot be executed in a cluster environment.
54	The management serveror database server has not been set up.
101	An attempt to start a service of the management server or database server failed.
110	Command execution failed due to a problem with a license.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to start the service on the management server.

startservice

Related Topics:

- 17.1 Executing commands

17.28 getlogs (collecting troubleshooting information)

Functionality

This command collects troubleshooting information required by the support service in batch when you encounter a problem with an unknown cause or unresolved issues.

The troubleshooting information is output to two files: tsinf_1st.dat for primary use, and tsinf_2nd.dat for secondary use.

In a single-server configuration system, execute this command on the management server. In a multi-server configuration system, execute this command on the management server or database server.

Format

```
getlogs[ -f troubleshooting-information-storage-folder]
```

Argument

-f *troubleshooting-information-storage-folder*

Specify the absolute path to the storage folder for troubleshooting information. Only a folder in a local drive can be specified.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. All characters that Windows systems allow for folder names are acceptable.

If this argument is not specified, the troubleshooting information is stored into the following folder:

JP1/IT Desktop Management-installation-folder\mgr\troubleshoot

A temporary folder tsinf is created under the troubleshooting information folder when collecting information. It is deleted when the command is completed.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

- If the storage folder for the troubleshooting information already contains one or more of the following folders or files, the command cannot be not executed until the folder or the file is deleted:
  - tsinf folder
  - tsinf_1st.dat
  - tsinf_2nd.dat
- The `getlogs` command uses a temporary folder which is set in the user environment variables TEMP. If a message (KDEX4041-E) is returned on `getlogs` command execution, check if there is enough space in this folder.

Return value

The following table shows the return values of the `getlogs` command.

Return value	Description
0	The command finished normally.
1	Collecting troubleshooting information partially failed.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, or the folder does not exist.
51	You do not have the permissions to execute this command.
101	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to collect troubleshooting information into C:\tmp\troubleshoot.

getlogs -f C:\tmp\troubleshoot

Related Topics:

- 17.1 Executing commands

17.29 getinstlogs (collecting troubleshooting information about installation)

This section describes the `getinstlogs` command, which collects troubleshooting information regarding product installation on the management server or database server.

Functionality

This command collects troubleshooting information required by the support service from the administrator in batch, when an administrator encounters a problem with an unknown cause or unresolved issues in installing JP1/IT Desktop Management.

In a single-server configuration system, execute this command on the management server. In a multi-server configuration system, execute this command on the management server or database server.

Format

```
getinstlogs[ -f troubleshooting-information-storage-folder]
```

Argument

-f *troubleshooting-information-storage-folder*

Specify the absolute path to the storage folder for troubleshooting information. You can specify a network drive as well as a local drive.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. All characters that Windows systems allow for folder names are allowed.

If this argument is not specified, the troubleshooting information file will be stored on the Desktop.

Storage location

*root-directory-of-JP1/IT-Desktop Management-distribution-media*_PPDIR\P064274A\DISK1\

Notes

- If the storage folder for troubleshooting information already contains a folder or a file named JDNINST, the command cannot be executed until the folder or the file is deleted.
- Select an existing folder to specify a storage folder for troubleshooting information.

Return value

The following table shows the return values of the `getinstlogs` command.

Return value	Description
0	The command finished normally.
1	The collecting of troubleshooting information partially failed.
11	The format for specifying the command arguments is invalid.
12	The specified folder cannot be accessed, or the folder does not exist.
13	Cannot write the backup file to the specified data storage folder.
51	You do not have the permissions to execute this command.

Return value	Description
101	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to collect troubleshooting information about the installation process, into C:\tmp\troubleshoot\install.

getinstlogs -f C:\tmp\troubleshoot\install

Related Topics:

- 17.1 Executing commands

17.30 addfwlist.bat (setting Windows firewall exceptions)

When you install JP1/IT Desktop Management - Manager or JP1/IT Desktop Management - Remote Site Server onto a computer on which Windows Firewall is enabled, firewall exceptions are automatically set for the products. If Windows Firewall is disabled at product installation, the exceptions will not set. If you enable Windows Firewall after JP1/IT Desktop Management - Manager or JP1/IT Desktop Management - Remote Site Server is installed, execute this command to allow Windows Firewall exceptions.

Functionality

This command sets up Windows Firewall exceptions for JP1/IT Desktop Management - Manager and JP1/IT Desktop Management - Remote Site Server.

Execute this command on the management server, database server, or site server.

Format

```
addfwlist.bat
```

Arguments

No arguments available for this command.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\ (for management server or database server), or *site-server-installation-folder*\mgr\bin\ (for site server)

On a management server or database server, you can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management.

Notes

Execute this command while the Windows Firewall service is running.

Return value

The following table shows the return values of the `addfwlist.bat` command.

Return value	Description
0	The command finished normally.
-1	Execution command has terminated abnormally.

Example

The following example shows use of this command to allow Windows Firewall exceptions.

addfwlist.bat

Related Topics:

- 17.1 Executing commands

17.31 resetnid.vbs (resetting the host ID)

This section describes the `resetnid.vbs` command, which resets the unique ID (host ID) which is generated by the agent in order to distinguish devices from each other.

Functionality

A host ID is automatically created when an agent is installed.

If you install an agent by using the disk copy functionality, the host ID must be reset on the copy-source computer prior to the copy so that a new host ID will be created on the copy-destination computer. The host ID for the agent can be reset by executing the `resetnid.vbs` command on the copy-source computer. As the old ID is reset, a new host ID is created when the agent is installed, and the computer will be able to be identified with a unique ID.

Tip

If you install an agent via a disk copy without executing the `resetnid.vbs` command, the copy-destination computer is defined as an identical device to the copy-source computer. In such cases, because two or more computers are identical, execute the `resetnid.vbs` command on those computers and go to the Settings module, **Discovery**, and then **Managed Nodes** to delete the device information for the computers.

When the `resetnid.vbs` command is executed on a computer that was once identified by JP1/IT Desktop Management, the host IDs assigned to the computer before and after the command execution are both registered to JP1/IT Desktop Management. Accordingly, two instances of the device information are displayed per computer. However, you can update the view by deleting both device information instances in the Settings module by selecting **Discovery**, and then **Managed Nodes**. After this operation, only the latest device information will be displayed.

Tip

To reset the host ID on the computer on which the site server is installed, perform the procedure described below. If you do not perform this procedure, the operation logs managed on the site server cannot be searched.

1. Execute the `resetnid.vbs` command.
2. Restart the site server service (JP1_ITDM_Remote Site Service).
3. Specify the -node option, and then execute the `recreatelogdb` command.

Important note

Do not execute the `resetnid.vbs` command on a device on which the network monitor is installed.

If you execute the `resetnid.vbs` on the device on which the network monitor is installed, 2 instances of the device information appear per computer. To resolve this problem, you need to perform the following: Temporarily disable the network monitor. After that, in the Settings module, select **Discovery** and then **Managed Nodes**, and then temporarily delete both device information stances.

Execute this command on a computer on which the agent is already installed.

Format

```
resetnid.vbs /nodeid [ /i]
```

Argument

/nodeid

Always specify this argument. If this argument is omitted, the command cannot be executed.

/i

Displays, on the user's computer, the dialog box for selecting whether to execute the command and the dialog box for displaying execution results.

Storage location

agent-installation-folder\bin\

Notes

When the `resetnid.vbs` command is executed, the time required is equal to the shortest time of the intervals set for the fields before a new host ID is created. The time intervals are defined in the agent configuration menu **Basic Settings**, under **Agent Basic Settings**.

- Monitoring interval (security items) (minutes)
- Monitoring interval (other than security items) (minutes)
- Interval for acquiring information from the management server (minutes)

Return value

The following table shows the return values of the `resetnid.vbs` command.

Return value	Description
0	The command finished normally.
10001	Command execution was canceled on the user's computer.
10011	The argument syntax is incorrect.
10051	You do not have permission to execute the command.
10101	Failed to reset the host ID.
10150	Failed to reset the host ID.

Example

The following example shows use of this command to reset the host ID.

resetnid.vbs /nodeid

Related Topics:

- 17.1 Executing commands

17.32 getinv.vbs (collecting information about offline computers)

Functionality

This command collects device information about offline computers following the settings defined in the Information Collection Tool. The following operations are performed before collecting the information:

- The **End User Form** view is displayed.
- A software search is performed according to the software search conditions.
- Information about the latest antivirus security products is collected.

The following are the pre-requisitions for this command:

- The services on the agent are already started.
- The agent version is 10-01 or later.
- The process of collecting device information is not already running.
- The **End User Form** view is closed.
- The command is stored in a folder on a local drive.
- The length of the full path name to the folder where the command is stored is 128 characters or less.

This command must be executed directly on an offline computer, using external storage media.

Format

```
getinv.vbs[ /u][ /s][ /silent]
```

Argument

/u
Prevents displaying the **End User Form** view from the end-user's computers. When `/silent` is specified, the **End User Form** view is not displayed on the end-user's computer regardless of whether `/u` is specified.

/s
Does not collect the installed software details set in the **Software Search Conditions** view in the Settings module.

/silent
Prevents displaying the view from an end-user's computer.

Storage location

Same storage location as the Information Collection Tool (where the tool is extracted to).

Notes

You first need to re-create the Information Collection Tool before collecting device information in the following cases:

- When you changed which antivirus software performs authorization by the security policy.
- When you change custom field settings

Return value

The following table shows the return values of the `getinv.vbs` command.

Return value	Description
0	The command finished normally.
10001	The information collecting process has been canceled on the end-user's computer.
10011	The format for specifying the command arguments is invalid.
10031	An information collecting process using the Information Collection Tool is already being executed.
10032	A temporary error occurred.
10033	An information collecting process is in progress in the background.
10034	The **End User Form** view is displayed.
10051	The process was aborted due to the path to the storage folder being too long.
10052	The Information Collection Tool is not installed on the local disk.
10101	Failed to collect information.
10102	You do not have read/write permissions to the folder in which this command is stored.
10103	An agent is not installed on the computer.
10104	The version of the agent installed on the computer does not support offline management.
10105	The Information Collection Tool might be corrupted.
10106	The agent environment is corrupted.

Example

The following example shows use of this command to collect information without displaying the **End User Form** view on the end-user's computer.

getinv.vbs /u

17.33 ioassetsfieldutil export (exporting the definitions of common management fields and additional management fields)

This section describes the `ioassetsfieldutil export` command, which exports the definitions of common management fields and additional management fields.

Functionality

This command exports the definitions of common management fields and additional management fields to a CSV file.

You can export the definitions of the following common management fields and additional management fields as long as the data type of the field is hierarchical or enumeration:

- Common management fields of hardware asset information and device information
- Additional management fields of hardware asset information
- Additional management fields of software license information
- Additional management fields of contract information

Execute the command as follows:

- In a single-server configuration: Execute the command on the management server when setup of the management server setup is complete and when the service on the management server is running.
- In a multi-server configuration: Execute the command on the database server when setup of both the management server and the database server is complete and when the services on both servers are running.

Format

```
ioassetsfieldutil export -field export-file-name[ -encoding character-encoding][ -s]
```

Arguments

-field *export-file-name*

Specify the absolute path (by using 255 bytes or fewer) of the CSV file to be exported.

-encoding *character-encoding*

Specify the character encoding of the CSV file to be exported. You can use the character encodings shown below. If you omit this argument, the character encoding is set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP

- JIS

-s

Overwrites the file even if a file that has the same name already exists at the export destination. If you omit this argument and a file that has the same name already exists, an overwrite-confirmation message appears. In such a case, the system either cancels output of the file or overwrites the file according to your (the administrator's) response.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file by using the command prompt provided by JP1/IT Desktop Management.

Notes

- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils importasset`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`

Return values

The following table shows the return values of the `ioassetsfieldutil export` command.

Return value	Description
0	The command finished normally.
11	The argument syntax is incorrect.
12	The specified folder is invalid, the disk does not have sufficient free space, or the folder does not exist.
15	A file access error occurred when outputting the file, or the disk does not have sufficient free space.
31	Another command is currently executing.
51	You do not have permission to execute this command.
54	Either the management server or the database server is not set up.
101	Command execution failed either because there is insufficient memory or for some other reason.
120	A database access error occurred.
150	Command execution was interrupted because of some other error.

Example

The following example shows how to use this command to export the definitions of common management fields and additional management fields to C:\temp\common.csv.

ioassetsfieldutil export -field C:\temp\common.csv -encoding UTF-8 -s

Related Topics:

- 17.1 Executing commands

17.34 ioassetsfieldutil import (importing the definitions of common management fields and additional management fields)

This section describes the `ioassetsfieldutil import` command, which imports the definitions of common management fields and additional management fields.

Functionality

This command imports the definitions of common management fields and additional management fields from a CSV file. You can use this command to add, update, or delete the definitions of common management fields and additional management fields in a batch operation.

If the command fails to import the definitions because the format of the CSV file is incorrect, the import log file is output. No more than 100 errors in the CSV file format are detected. For details about the actions to be taken when the command fails to import the definitions because the format of the CSV file is incorrect, see 18.6 Troubleshooting problems when an attempt to import the definitions of the common management fields and additional management fields fails.

If you use the `ioassetsfieldutil import` command to move a department definition, the following information is transferred to the new department:

- The security policy assigned to the previous department
- The agent configurations assigned to the previous department
- Any report data that is associated with the previous department

Execute the command as follows:

- In a single-server configuration: Execute the command on the management server when setup of the management server is complete and when the service on the management server is running.
- In a multi-server configuration: Execute the command on the database server when setup of both the management server and the database server is complete and when the services on both servers are running.

Format

```
ioassetsfieldutil import -field import-file-name[ -agentupdate timing-for-
starting-user-entry][ -encoding character-encoding] [ -c]
```

Arguments

-field *import-file-name*

Specify the absolute path (by using 255 bytes or fewer) of the CSV file to be imported.

-agentupdate *timing-for-starting-user-entry*

Specify the time at which user entry is to start. If you omit this argument, the command is executed according to the setting displayed in **Start Date for Entry of User Information** that is displayed by choosing **Asset Field Definitions** from **Asset Management** in the Settings module.

You can specify the following values:

now

When a user executes the command, a message that prompts the user to enter information is displayed on the user's computer.

"*YYYY-MM-DD HH*:*MM*"[#]

A message that prompts a user to enter information is displayed on the user's computer at the specified date (according to the local time of the user's computer).

#: YYYY: year, MM: month, DD: day, HH: hour, MM: minute

-encoding *character-encoding*

Specify a character encoding of the CSV file to be imported. You can use the character encodings shown below. If you omit this argument, the character encoding is set to UTF-8.

- US-ASCII
- ISO-8859-1
- UTF-8
- UTF-8N
- UTF-16
- UTF-16LE
- UTF-16BE
- MS932
- Shift-JIS
- EUC-JP
- JIS

-c

Specify this argument if you want only to check the format of the CSV file to be imported.

Storage location

JP1/IT Desktop Management-installation-folder\mgr\bin\

Notes

- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioutils exportasset`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`

- `ioutils importasset`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`

- Do not execute this command while distribution is being executed. If you do, processing of the service (JP1_ITDM_Agent Control) temporarily stops, and the distribution might be delayed.

Return values

The following table shows the return values of the `ioassetsfieldutil import` command.

Return value	Description
0	The command finished normally.
1	Import succeeded, but an attempt to restart the agent control service failed.
11	The argument syntax is incorrect.
12	The specified folder is invalid, the disk does not have sufficient free space, or the folder does not exist.
31	Another command is currently executing.
51	You do not have permission to execute this command.
54	Either the management server or the database server is not set up.
80	The format of the file being imported is invalid.
87	An attempt to apply the imported data to the database failed.
101	Command execution failed either because there is insufficient memory or for some other reason.
120	A database access error occurred.

Example

The following example shows how to use this command to import the definitions of common management fields and additional management fields that had been exported to the file common.csv in C:\temp\.

ioassetsfieldutil import -field C:\temp\common.csv

Related Topics:

- 17.1 Executing commands

18 Troubleshooting

This section describes what actions to take when a problem occurs in JP1/IT Desktop Management.

18.1 Operational troubleshooting procedures

If a problem occurs during operation of a server or an agent, carry out the following procedures to resolve the problem:

When a problem occurs in the management server or in the database server

1. Check the error message.
   Check the error message as follows:
   - Check the error information in the dialog box that was displayed when the error occurred.
   - Check the error information in the output log files.
   - Check the event message in the Home module or in the Events module.
2. Check the cause of and workaround for the problem and take action.
   Using the error message, check the cause of and workaround for the trouble, and then take action to resolve the problem.

When a problem occurs in a site server

1. Check the error message.
   Check the event message in the Home module or in the Events module.
2. Using the information in the event message, determine and take action to resolve the problem.
   Collect information to be used for troubleshooting as necessary.

When a problem occurs in an agent

The system administrator must resolve the problem when a problem occurs in an agent.

1. Check the error message.
   Check the event message in the Home module or in the Events module.
2. Using the information in the event message, determine and take action to resolve the problem.
   Obtain information to be used for troubleshooting as necessary.

Message output format

Messages are output in the following format:

- KDEX*nnnn-Z message-text*
- KFPH*nnnnn-Z message-text*

The following describes the portions of a message ID:

K
   Indicates the system ID.

DEX
   Indicates that the message is a message other than a database-related message from JP1/IT Desktop Management.

FPH
   Indicates that the message is a database-related message from JP1/IT Desktop Management.

nnnn
   Indicates the serial number of the message. Serial numbers for database-related messages from JP1/IT Desktop Managementare expressed with five digits.

Z

Indicates the message type as follows:

- E: Indicates an error message.
- W: Indicates a warning message.
- I: Indicates an informational message.
- Q: Indicates a message to which the user needs to respond.

18.2 Actions to be taken when a device cannot be found

This section describes what actions to take when a device cannot be found after device discovery is executed.

Devices that meet any of the conditions below will not be found. If there is a device that meets any of the conditions, take the necessary actions so that the device no longer meets that condition, and then execute discovery again.

- The device is not included in the discovery range that was specified in the search conditions.
- The credentials (ID or community name) that were specified in the search conditions are invalid.
- The device is powered off.
- The device is not connected to the network.
- NAPT is being used.
- ICMP messages cannot get through due to Windows Firewall settings or router settings.
- The device is a virtual PC, and the IP address is being shared.
- The device is a virtual PC, and the private network is being shared.

18.3 Actions to be taken when an authentication error occurs

This section describes what actions to take when an authentication error occurs on an agentless computer after device discovery is executed:

Actions to be taken on the management server

Check the following items and take action if you find any problems:

Discovery range settings

Check that the discovery range is correctly set. For details about setting the discovery range, see 15.2 Specifying settings for discovery.

Registration of authentication information

Check that credentials (Windows authentication or SNMP authentication) are correctly registered. Note that when searching for a computer that is running a version of Windows that supports User Account Control (UAC), you need to set credentials for the built-in users of that computer. For details about how to register credentials, see 15.2 Specifying settings for discovery.

Credential Assignment

Check that credentials are correctly assigned. For details about how to assign credentials, see 15.2 Specifying settings for discovery.

Actions to be taken on the user's computer

Check the following items and take action if you find any problems:

SNMP authentication

- Check that the community name is correctly set.
- Check that the SNMP agent services are operating correctly.

Windows authentication

- Add file shares.
- If the administrative shares are disabled, enable them. You can check administrative shares by using the Windows `net share` command. If executing this command displays `admin$`, the administrative shares are enabled.
- In the authentication settings, set a user who has Administrator permission and whose account is enabled.
- On computers that are running Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, if User Account Control (UAC) is enabled, use a built-in user that has Administrator permission, or both use a user that has Administrator permission and disable UAC.
- On computers that are running Windows Server 2008, Windows Vista, or Windows XP, if the firewall is enabled, grant permission for files to be shared from external servers.
- On computers that are running Windows XP, disable simple file sharing.

18.4 Actions to be taken when notification of device information that was collected with the Information Collection Tool fails

If notification of device information fails, use the information in the notification-failure list (result_failed.txt) to collect the device information again, and then perform the notification again.

The notification-failure list (result_failed.txt) is generated when notification to one or more computers fails. The host name of each computer to which notification of device information failed is output to this list.

File location

The notification-failure list is created in the **Data** folder that was specified in the **Specify storage location** dialog box. This dialog box appears when you perform notification of device information.

Output format

YYYY/*MM*/*DD hh*:*mm*:*ss host-name*

In this string, YYYY represents the year, MM represents the month, DD represents the day, hh represents the hour, mm represents the minute, and ss represents the second.

Example output

```
2012/10/11 14:15:16 Host1
2012/10/11 14:15:18 Host2
2012/10/11 14:15:19 Host3
```

18.5 Actions to be taken when a CSV file is displayed incorrectly

When you import or export a CSV file, depending on your operating environment, the CSV file might be displayed incorrectly. This section describes what actions to take if the CSV file is displayed incorrectly.

When importing a CSV file

If data is displayed incorrectly in the **Map Fields** view when you import asset information, return to the **Upload CSV File** view, and then change the character set of the CSV file to be imported by changing the character set that is specified in **Encoding**.

When exporting a CSV file

If data is displayed incorrectly when you refer to an exported CSV file by using software such as a spreadsheet application, change the character set of the CSV file to be exported by changing the character set that is specified in **Encoding** in the **Select Export Columns** dialog box.

Tip

When editing and importing asset information that had previously been exported, specify the character set that was chosen when the file was exported.

18.6 Troubleshooting problems when an attempt to import the definitions of the common management fields and additional management fields fails

If an attempt to import the definitions of the common management fields and additional management fields fails because the format of the imported CSV file is incorrect, correct the CSV file based on the information in the import log file (*import-file-name.log*) that is output when the `ioassetsfieldutil import` command is executed, and then execute the `ioassetsfieldutil import` command again.

An import log file is generated only when an attempt to import the definitions fails because the format of the imported CSV file is incorrect.

The `ioassetsfieldutil import` command first reads all of the CSV files to be imported, changes the order of the rows to the order below, and then imports the data. For this reason, import log files are also output in the order below.

1. For definitions whose update category is A (addition), the order is from the definitions whose hierarchical level is high to those whose hierarchical level is low.
2. For definitions whose update category is U (update), the order is the same as the CSV files to be imported.
3. For definitions whose update category is D (deletion), the order is from the definitions whose hierarchical level is low to those whose hierarchical level is high.

Generation location

Folder that stores imported CSV files

Output format

message-ID #*row-number-of-the-imported-CSV-file*:*information-in-the-imported-CSV-file*

#: The message ID is output only for a row for which an attempt to import the definition failed.

Output example

```
8:a,common,ja,department,ja,,Development Department/Development C
Division,,,,
KDEX4388-E 3:u,common,ja,department,ja,Sales Department/Sales 1
Divisionerr,Sales Department/Sales Division,,,,
4:d,common,ja,department,ja,Sales Department/Sales 2 Division,,,,,
```

In the above output example, an attempt to update the definition on the third row of the imported CSV file failed. In this case, you need to correct the third row of the imported CSV file by referring to the KDEX4388-E message displayed in the command prompt, and then execute the `ioassetsfieldutil import` command again.

Related Topics:

- 17.34 ioassetsfieldutil import (importing the definitions of common management fields and additional management fields)

18.7 Actions to be taken when a disk is low on free space

If the disk that stores the JP1/IT Desktop Management database or operation logs, or the disk that is the output location for revision history archive does not have enough free space, you will not be able to add new data, and management will no longer be based on correct information.

To avoid such problems, it is necessary to monitor the free space available on the disk that JP1/IT Desktop Managementuses, and to take action when this space runs low.

You can check the free space on the disk that JP1/IT Desktop Managementuses from the **DB and Disk Usage** panel in the Home module.

When the free space on this disk runs low, a warning or an error message will appear in the **Topic** panel. If such a message appears, take actions to increase the amount of free space on the disk. The following shows examples of how to do this:

- Delete unnecessary data from the disk.
- If you are using a logical drive, increase its storage capacity by expanding the disk.

If you cannot secure free space on the disk, take actions such as changing folder paths during setup or replacing the management server.

18.8 Actions to be taken after a failover

The table below shows what actions to take when a failover occurs during cluster system operation. Choose the actions that correspond to the processing that was in progress when the failover occurred.

Processing in progress	Actions to take after failover
Referring to an operation window	After a communications error message or a database access error message appears, log out, and then log in again.
Registering a package	After a communications error message or a database access error message appears, log out, and then log in again. If registration of the package did not complete, register the package again.
Performing an import (for example, of asset information)	After a communications error message or a database access error message appears, log out, log in again, and then perform the import again.
Performing an export (for example, of asset information)	After a communications error message or a database access error message appears, log out, log in again, and then perform the export again.
Running the database manager	Execute the process that was in progress again.
Running setup	Move the owner of the cluster group back to the node that it was on before the failover occurred, and then run setup again.
Registering components	Register the component again.
Registering USB devices	Register the USB device again.
Executing commands	Execute the command again. Depending on the command that you were executing, also perform the following actions: • ioutils exportasset (to export hardware asset information) Delete the exported file. • ioutils exportfield (to export custom-field settings) Delete the exported file. • ioutils exporttemplate (to export templates) Delete the exported file. • ioutils exportpolicy (to export security-policy settings) Delete the exported file. • ioutils exportupdategroup (to export security-update settings) Delete the exported file. • ioutils exportoplog (to export operation logs) Delete the exported file. • ioutils exportfilter (to export filter settings) Delete the exported file. • exportdb (to obtain a backup) Delete the backup destination folder. • getlogs (to obtain troubleshooting information from the management server) Do not delete the folder in which the troubleshooting information is stored. This information might be necessary if you contact Customer Support. • getinstlogs (to obtain troubleshooting information collected during installation) Do not delete the folder in which the troubleshooting information is stored. The information might be necessary if you contact Customer Support.

18.9 Troubleshooting problems on the management server

When an error occurs, a message will appear in the JP1/IT Desktop Managementview. Determine the cause of the problem and the actions to be taken by following the instructions in the message, and then take the necessary actions.

In the Events module, if you find an event that requires action to be taken, check the event message, and then take the necessary action.

Also, log files are output when an error occurs. Check the log files for the cause of the error and the actions to be taken.

The following table describes the causes of and actions to be taken for events that require such action:

Event number	Type	Message	Cause	Actions to be taken
002	Settings	The device has been added as a managed node.	The device has been excluded from the set of objects to be managed.	In the Settings module, select **Discovery**, and then check the **Ignored Nodes** view.
004	Settings	Failed to register the device as a managed node. You have already reached the limit of licenses available for managed devices.	It was detected that the licensed number of objects has been exceeded.	Purchase the number of licenses corresponding to the number of objects to be managed. After that, in the Settings module, select **Product Licenses**, and then add the licenses in the **License Details** view.
005	Settings	The agent has been uninstalled.	The uninstallation of an agent was detected.	Check whether the device has permission to uninstall the agent.
019	Error	Failed to obtain detailed information from *function-name*.	Discovery of a device or collection of device information failed.	Check settings such as authentication information and discovery range, and check the operating status of the JP1_ITDM_Agent Control service. Alternatively, check the status of the target device. After making these checks, perform the device discovery or collection of device information again. If neither of these procedures solves the problem, obtain troubleshooting information by using the `getlogs` command, and then contact Customer Support.
050	Security	The security status has been judged. The judgment result is *violation-level*.	A security inspection determined that the security status of the target computer is dangerous.	Carry out security measures on the target computer.
051	Security	The security status has been judged. The judgment result is *violation-level*.	A security inspection determined that the security status of the target computer requires caution or attention.	Carry out security measures on the target computer.
055	Error	Failed to send an e-mail notification to the System Administrator.	• Cause 1 The administrator does not have an email address set, or the administrator's email address is invalid. • Cause 2 The mail server settings are invalid, or the mail server is not running.	Select and take the appropriate actions from the list below: • For Cause 1 In the Settings module, select **User Management**. Then, in the **User Account Management** view, set an email address for the administrator. Alternatively,

Event number	Type	Message	Cause	Actions to be taken
055	Error	Failed to send an e-mail notification to the System Administrator.	• Cause 3 The authentication settings that are required for connection to the mail server are invalid.	correct the administrator's email address. • For Cause 2 In the Settings module, select **General**. Then, in the **Mail Server Settings** view, correct the mail server settings. Alternatively, contact the mail server administrator. • For Cause 3 In the Settings module, select **General**. Then, in the **Mail Server Settings** view, correct the authentication settings that are used for the mail server.
057	Error	Failed to send a message notification to the user.	Message notification failed because of a network failure between the management server and the computer.	Obtain troubleshooting information by using the `getlogs` command, and then contact Customer Support.
074	Error	Failed to apply security measures.	Enforcement of security measures failed.	Obtain troubleshooting information by using the `getlogs` command, remove the cause of the error, and then enforce the security measures. Also, ask users to enforce security measures by using message notifications or by other means.
078	Error	Failed to unblock the printing operation.	Release of a printing restriction failed.	Check whether the user who tried to release the printing restriction has permission to do so. If the user has permission, contact the user and give him or her the correct password for releasing the printing restriction. If the user does not have permission, contact the user as necessary and notify him or her that printing restrictions are currently in place.
081	Error	Failed to implement security measures. The group policy assigned to the device has been violated.	An attempt was made to enforce security measures, but those measures differed from with the security policy that is already in place.	Check the contents of the security policy that is already in place and the contents of the security measures.
200	Error	An error occurred in the operation (JP1_ITDM_Service). The operation (JP1_ITDM_Service) will be stopped.	A critical internal error occurred in the service (JP1_ITDM_Service).	Obtain troubleshooting information by using the `getlogs` command, and then contact Customer Support.
203	Error	Failed to collect product update information. Settings are invalid.	A setting in the **Product Update Settings** view, which is selected from **General** in the Settings Module, is invalid.	Determine the information that is used to connect to the Support Service site. After that, in the Settings module, select **General**, and then correct the settings in the **Product Update Settings** view. You can check connectivity to the Support Service by clicking the **Test** button.

Event number	Type	Message	Cause	Actions to be taken
206	Error	Failed to connect Active Directory. Active Directory settings are invalid.	The Active Directory server is not running. Alternatively, a setting in the **Active Directory Settings** view, which is selected from **General** in the Settings module, is invalid.	Check whether the Active Directory server is running. If the Active Directory server is running, in the Settings module, select **General**, and then correct the settings in the **Active Directory Settings** view. You can check connectivity to the Active Directory server by clicking the **Test** button.
208	Error	An error occurred while updating received files.	Receipt of information from the agent failed.	Resources in the management server environment might be insufficient. If this error occurs frequently, revise the management server environment.
209	Error	An error occurred in *function-name*.	An error occurred in the internal processing of the manager service.	After checking the **Discovery** view in the Settings module, checking the **Agent** view in the Settings module, or checking the Device module, perform discovery or agent deployment again. If this error reoccurs, use the `getlogs` command to obtain troubleshooting information, and then contact Customer Support.
210	Error	Failed to update. Error occurred while updating received files.	Receipt of information from the agent failed, and update processing has been canceled because recovery from this error cannot be expected.	Resources in the management server environment might be insufficient. Revise the management server environment and obtain the information again.
211	Error	Failed to update the file. The file format was invalid.	A file in an invalid format was received.	The source data might include special characters, such as control codes. If you can edit the source data, remove the special characters and then obtain the information again. If this error reoccurs, use the `getlogs` command to obtain troubleshooting information, and then contact Customer Support.
1003	Settings	The agent's operation has been stopped.	The agent execution environment has become corrupted due to a problem such as an agent file being deleted.	Restore the environment by performing an update on the agent side.
1004	Device	New software has been discovered.	New software has been detected.	In the **Software Information** view of the Device module, make sure that there are no problems with the software.
1006	Error	Failed to stop the prohibited operation.	An attempt to stop an unauthorized service failed.	Check the status of the agent.
1016	Distribution	Mandatory software will be distributed.	It was detected that mandatory software is not installed.	An Auto Enforce will be performed. In the Distribution module, check the execution result of the task
1017	Distribution	Prohibited software will be deleted.	It was detected that unauthorized software is installed.	An Auto Enforce will be performed. In the Distribution module, check the execution result of the task

Event number	Type	Message	Cause	Actions to be taken
1018	Distribution	Package distribution task has been terminated abnormally.	Installation failed for some reason.	Check the cause of the problem in the event detail, resolve the problem, and then perform the installation again.
1019	Distribution	Unistallation task has been terminated.	Uninstallation failed for some reason.	Check the cause of the problem in the event detail, resolve the problem, and then perform the uninstallation again.
1021	Distribution	On-demand tasks has ended.	Tasks that the administrator executed have completed.	In the Distribution module, check the execution result of the task.
1022	Assets	An unconfirmed hardware asset (*device-type*) has been recognized.	The addition of a device that is to be managed, or the registration of a USB device has been executed.	In the Assets module, edit the hardware asset information of the asset whose asset status is **Unconfirmed**.
1028	Settings	IP Discovery is complete.	Network discovery finished.	In the **Discovery Log** view of the Settings module, confirm the discovery result.
1029	Settings	Active Directory synchronization is complete.	Active Directory discovery finished.	In the **Discovery Log** view of the Settings module, confirm the discovery result.
1032	Security	An error occurred while backing up (automatic) the Operations logs.	• Cause 1 An internal error occurred. • Cause 2 There might be insufficient space on the disk for the local data folder. • Cause 3 The operation log backup folder either does not exist, or cannot be accessed. • Cause 4 The user name or the password that is used to access the operation log backup folder is incorrect. • Cause 5 There might be insufficient space on the disk for the operation log backup folder.	Select and take the appropriate actions from the list below: • For Cause 1 Use the `getlogs` command to obtain troubleshooting information, and then contact Customer Support. • For Cause 2 Either increase the amount of free space on the disk that was specified during setup for the local data folder, or move the local data folder to a disk that has sufficient free space. • For Cause 3 Check whether the operation log backup folder that was specified during setup exists and whether that folder can be accessed. • For Cause 4 Make sure that the user name and the password that were specified during setup are correct. • For Cause 5 Either increase the amount of free space on the disk that was specified during setup for the operation log backup folder, or move the operation log backup folder to a disk that has sufficient free space.
1034	Error	An error occurred while restoring Operations logs.	• Cause 1 An internal error occurred.	Select and take the appropriate actions from the list below:

Event number	Type	Message	Cause	Actions to be taken
1034	Error	An error occurred while restoring Operations logs.	• Cause 2 There might be insufficient space on the disk for the local data folder. • Cause 3 The operation log backup folder either does not exist, or cannot be accessed. • Cause 4 The user name or the password that is used to access the operation log backup folder is incorrect. • Cause 5 There might be insufficient space on the disk for the operation log backup folder. • Cause 6 There are no backup files in the operation log backup folder.	• For Cause 1 Use the `getlogs` command to obtain troubleshooting information, and then contact Customer Support. • For Cause 2 Either increase the amount of free space on the disk that was specified during setup for the local data folder, or move the local data folder to a disk that has sufficient free space. • For Cause 3 Check whether the operation log backup folder that was specified during setup exists and whether that folder can be accessed. • For Cause 4 Make sure that the user name and the password that were specified during setup are correct. • For Cause 5 Either increase the amount of free space on the disk that was specified during setup for the operation log backup folder, or move the operation log backup folder to a disk that has sufficient free space. • For Cause 6 If the backup files were moved to another folder, copy them to the operation log backup folder, and then restore the operation logs again.
1035	Security	The Operations logs restoration may have missed some data.	There are no backup files that have the applicable date in the operation log backup folder.	If the backup files that have the applicable date were moved to another folder, then copy the files to the operation log backup folder, and then restore the operation logs again.
1036	Error	Failed to expand database files for Operations logs.	The operation log database folder has no free space.	Increase the amount of free space on the disk by moving or deleting unnecessary files, and then start the service again. If this error reoccurs even though the disk has sufficient free space, use the `getlogs` command to obtain troubleshooting information, and then contact Customer Support.
1037	Error	Failed to retrieve inventory and organizational information from Active Directory Server.	• Cause 1 Connection to the Active Directory server failed. • Cause 2 Authentication to the Active Directory server failed.	Select and take the appropriate actions from the list below: • Cause 1 In the Settings module, select **General**, and then check the host name and port number that are

Event number	Type	Message	Cause	Actions to be taken
1037	Error	Failed to retrieve inventory and organizational information from Active Directory Server.	• Cause 3 The specified domain cannot be found. • Cause 4 The OU information that is specified on the Active Directory server cannot be found. • Cause 5 Encrypted communication with the Active Directory server has failed.	set in the **Active Directory Settings** view. Alternatively, check whether the Active Directory server is running. • Cause 2 In the Settings module, select **General**, and then check the user ID and password that are set in the **Active Directory Settings** view. • Cause 3 In the Settings module, select **General**, and then check the domain name that is set in the **Active Directory Settings** view. • Cause 4 In the Settings module, select **General**, and then check the root OU that is set in the **Active Directory** view. • Cause 5 In the Settings module, select **General**, and then check the port number that is set in the **Active Directory** view. Alternatively, check whether a certificate is installed on the Active Directory server. You can check connectivity to the Active Directory server by clicking the **Test** button.
1048	Suspicious Operations	E-mail transmission with attachments has been detected.	The sending of an email that has an attachment was detected and deemed to be a suspicious operation.	Make sure that there are no problems with the operation.
1049	Suspicious Operations	File upload to Web Server/FTP Server was detected.	The uploading of a file to a Web or FTP server was detected and deemed to be a suspicious operation.	Make sure that there are no problems with the operation.
1050	Suspicious Operations	File Copy or File Move to a unregistered removable drive has been detected.	The copying or moving of files to a removable disk drive was detected and deemed to be a suspicious operation.	Make sure that there are no problems with the operation.
1051	Suspicious Operations	Mass-Printing has been detected.	The printing of a large number of pages was detected and deemed to be a suspicious operation.	Make sure that there are no problems with the operation.
1055	Error	Failed to collect product update information.	A setting in the **Support Service Settings** view, which is selected from **General** in the Settings Module, is invalid.	Determine the information that is used to connecting to the Support Service site. After that, in the Settings module, select **General**, and then correct the settings in the **Support Service Settings** view. You can check connectivity to the Support Service by clicking the **Test** button.
1056	Error	Failed to notify System Administrators by e-mail.	• Cause 1	Select and take the appropriate actions from the list below:

Event number	Type	Message	Cause	Actions to be taken
1056	Error	Failed to notify System Administrators by e-mail.	The administrator does not have an email address set, or the administrator's email address is invalid. • Cause 2 The mail server settings are invalid, or the mail server is not running. • Cause 3 The authentication settings that are required for connection to the mail server are invalid.	• For Cause 1 In the Settings module, select **User Management**. Then, in the **User Account Management** view, set an email address for the administrator. Alternatively, correct the administrator's email address. • For Cause 2 In the Settings module, select **General**. Then, in the **Mail Server Settings** view, correct the settings for the mail server. Alternatively, contact the mail server administrator. • For Cause 3 In the Settings module, select **General**. Then, in the **Mail Server Settings** view, correct the authentication settings that are used for the mail server.
1057	Error	Available disk space is limited. Please increase available space or change the path to a disk with sufficient space.	Free disk space fell below the warning threshold value that was specified for disks in the environment information.	Increase the amount of free space on the disk, or change to a disk that has sufficient free space.
1058	Error	Available disk space is limited. A database failure might occur due to limited disk space. Please increase available space or change the path to a disk with sufficient space.	Free disk space fell below the error threshold value that was specified for disks in the environment information.	Increase the amount of free space on the disk, or change to a disk that has sufficient free space.
1059	Settings	The product license will expire soon.	The system detected that the license is about to expire.	Please purchase a new license key.
1064	Error	Failed to apply security measures for account (*account-name*).	Enforcement of security measures failed.	Obtain troubleshooting information by using the `getlogs` command, remove the cause of the error, and then enforce the security measures. Also, ask users to enforce security measures by using message notifications or by other means.
1065	Error	Failed to apply security measures for the device (Account *account-name*). Violated the assigned group policy. Confirm the policy and security measure contents.	An attempt was made to enforce security measures, but those measures differed from the group policy that is already in place.	Confirm the contents of the security policy that is already applied and the contents of the security measures.
1071	Error	Failed to apply security measures. Apply security measures after the System Administrator collects troubleshooting information and eliminates the cause of error.	Enforcement of security measures failed.	Obtain troubleshooting information by using the `getlogs` command, remove the error cause, and then enforce security measures. Also, request the users to enforce security measures such as by message notification.

Event number	Type	Message	Cause	Actions to be taken
1072	Error	Failed to apply security measures for the device. Violated the assigned group policy.	An attempt to enforce security measures was made but the group policy differed from the one already applied.	Check the contents of the security policy that is already in place and the contents of the security measures.
1076	Security	The Operations log was deleted.	• Cause 1 The date and time settings on the agent are incorrect. • Cause 2 The agent was unable to connect to the management server for a long time.	Select and take the appropriate actions from the list below: • Cause 1 Check the date and time settings on the agent. • Cause 2 Make sure that the agent can periodically connect to the management server.
1085	Settings	Failed to enable network access control.	Enabling of network monitoring failed.	Check the error message that was output to the installer trace log file, and then take action according to that error message. The installer trace log file is the file %WINDIR%\Temp\JDNINMA\JDNINS01.log on the source host.
1086	Settings	The attempt to disable the network access control failed.	Disabling of network monitoring failed.	Check the error message that was output to the installer trace log file, and then take action according to that error message. The installer trace log file is the file %WINDIR%\Temp\JDNINMA\JDNINS01.log on the source host.
1088	Error	AMT authentication failed. (AMT power control)	When accessing AMT by using the AMT admin password that was set, an authentication error occurred.	Revise the settings in the AMT Settings view, or change the AMT authentication information by going to the following URL: http://*host-name*:16992
1089	Error	AMT authentication failed. (AMT Settings)	When accessing AMT by using the AMT admin password that was set, an authentication error occurred.	Revise the password for administrative privileges in the AMT Settings view, or change the AMT authentication information by going to the following URL: http://*host-name*:16992
1090	Error	Free space on the disk containing the operation log data folder has become scarce. Increase the free disk space, or change to a disk that has enough free space.	The disk that stores the operation logs for the site server is running out of free space.	Increase the amount of free space on the disk, or change to a disk that has sufficient free space.
1091	Error	The operation log collection service stopped because there is almost no free space on the disk containing the operation log data folder. Increase the free disk space, or change to a disk that has enough free space.	The disk that stores the operation logs for the site server is almost out of free space.	Increase the amount of free space on the disk, or change to a disk that has sufficient free space.

Event number	Type	Message	Cause	Actions to be taken
1094	Error	Free space on the disk containing the data folder has become scarce. Increase the free disk space, or change to a disk that has enough free space.	The disk that stores the data folder for the site server is running out of free space.	Increase the amount of free space on the disk, or change to a disk that has sufficient free space.
1095	Error	A package cannot be downloaded to the site server because there is almost no free space on the disk containing the data folder. Increase the free disk space, or change to a disk that has enough free space.	The disk that stores the data folder for the site server is almost out of free space.	Increase the amount of free space on the disk, or change to a disk that has sufficient free space.
1100	Error	Installation of the site server program failed.	Installation of the site server program failed.	Check the error message that was output to the installer trace log file, and then take action according to that error message. The installer trace log file is the file %WINDIR%\Temp\JDNINMA\JDNINS01.log on the source host. If the problem persists, obtain troubleshooting information by using the appropriate command, and then contact Customer Support.
1101	Error	Uninstallation of the site server program failed.	Uninstallation of the site server program failed.	Check the error message that was output to the installer trace log file, and then take action according to that error message. The installer trace log file is the file %WINDIR%\Temp\JDNINMA\JDNINS01.log on the source host. If the problem persists, obtain troubleshooting information by using the appropriate command, and then contact Customer Support.
1103	Error	A database access error occurred on the site server.	The database service (JP1_ITDM_DB Service) might not have started.	Start the database service (JP1_ITDM_DB Service) from the site server.
1105	Settings	Failed to enable network access control.	• Cause 1 A product is installed that cannot coexist with the network monitor. • Cause 2 An installer is running. • Cause 3 A folder or file is in use within the installation folder for the network access control agent.	Select and take the appropriate actions from the list below: • For Cause 1 Uninstall the product that cannot coexist with the network monitor, and then retry the installation. • For Cause 2 Wait a short time, and then from the operation menu, select **Enable network access control** to retry the operation that enables network access control. If the problem persists, obtain troubleshooting information by using the appropriate command, and then contact Customer Support.

Event number	Type	Message	Cause	Actions to be taken
1105	Settings	Failed to enable network access control.	• Cause 1 A product is installed that cannot coexist with the network monitor. • Cause 2 An installer is running. • Cause 3 A folder or file is in use within the installation folder for the network access control agent.	• For Cause 3 Close the folder or file within the installation folder, and then from the operation menu, select **Enable network access control** to retry the operation that enables network access control.

1106	Error	Installation of the site server program failed.	• Cause 1
			A product is installed that cannot coexist with the site server application.
			• Cause 2
			An installer is running.
			• Cause 3
			A folder or file is in use within the installation folder for the site server.
			• Cause 4
			There is insufficient free space in the installation destination folder.
			• Cause 5
			There is insufficient free space in the database folder.
			• Cause 6
			This operating system is not supported.
				Select and take the appropriate actions from the list below:
				• For Cause 1
				Uninstall the product that cannot coexist with the site server application, and then retry the installation.
				• For Cause 2
				Wait a short time, and then from the operation menu, select **Install a site server program** to retry the installation. If the problem persists, obtain troubleshooting information by using the appropriate command, and then contact Customer Support.
				• For Cause 3
				A folder or file is in use within the installation folder for the site server. Retry the installation by selecting **Install a site server program** in the operation menu at one of the following times:
				  • After closing the folder or file within the installation folder
				  • After a site server command or program has finished executing, or after site server setup is complete
				• For Cause 4
				Increase the amount of free space in the installation folder, and then select **Install a site server program** from the operation menu to retry the installation.
				• For Cause 5
				Increase the amount of free space in the database folder, and then select **Install a site server program** from the operation menu to retry the installation.
				• For Cause 6
				Install the site server program on an operating system that is supported.

Event number	Type	Message	Cause	Actions to be taken
1108	Error	Failed to synchronize device information with MDM (*product-name*).	• Cause 1 An attempt to connect to the MDM server and to the proxy server failed. • Cause 2 Authentication with the MDM server failed. • Cause 3 Authentication with the proxy server failed. • Cause 4 An error occurred in MDM linkage. • Cause 5 An error occurred while obtaining the settings information of the MDM server.	Select and take the appropriate actions from the list below: • For Cause 1 Check the host name, IP address, and port number that are specified in the MDM linkage settings for the MDM server and the proxy server. Also, check whether the MDM server is running. • For Cause 2 Check the user ID and the password that are specified in the MDM linkage settings for the MDM server. • For Cause 3 Check the user ID, password, IP address, and port number that are specified in the MDM linkage settings for the proxy server. • For Cause 4 Obtain troubleshooting information by using the appropriate command, and then contact Customer Support. • For Cause 5 In the Settings module, make sure that the information that is set for MDM linkage has not been deleted.
1111	Error	Failed to lock a smart device.	• Cause 1 An attempt to connect to the MDM server and to the proxy server failed. • Cause 2 Authentication with the MDM server failed. • Cause 3 Authentication with the proxy server failed. • Cause 4 The smart device to be managed is not registered in the MDM system or in an MDM-managed product. • Cause 5 An error occurred in MDM linkage. • Cause 6 An error occurred while obtaining the settings information of the MDM server.	Select and take the appropriate actions from the list below: • For Cause 1 Check the host name, IP address, and port number that are specified in the MDM linkage settings for the MDM server and the proxy server. Also, check whether the MDM server is running. • For Cause 2 Check the user ID and the password that are specified in the MDM linkage settings for the MDM server. • For Cause 3 Check the user ID, password, IP address, and port number that are specified in the MDM linkage settings for the proxy server. • For Cause 4 Register the smart device on the MDM server, and then obtain the information. • For Cause 5

Event number	Type	Message	Cause	Actions to be taken
1111	Error	Failed to lock a smart device.	• Cause 1 An attempt to connect to the MDM server and to the proxy server failed. • Cause 2 Authentication with the MDM server failed. • Cause 3 Authentication with the proxy server failed. • Cause 4 The smart device to be managed is not registered in the MDM system or in an MDM-managed product. • Cause 5 An error occurred in MDM linkage. • Cause 6 An error occurred while obtaining the settings information of the MDM server.	Obtain troubleshooting information by using the appropriate command, and then contact Customer Support. • For Cause 6 In the Settings module, make sure that the information that is set for MDM linkage has not been deleted.
1113	Error	Failed to reset the password of a smart device.	• Cause 1 An attempt to connect to the MDM server and to the proxy server failed. • Cause 2 Authentication with the MDM server failed. • Cause 3 Authentication with the proxy server failed. • Cause 4 The smart device to be managed is not registered in the MDM system. • Cause 5 An error occurred in MDM linkage. • Cause 6 An error occurred while obtaining the settings information of the MDM server.	Select and take the appropriate actions from the list below: • For Cause 1 Check the host name, IP address, and port number that are specified in the MDM linkage settings for the MDM server and the proxy server. Also, check whether the MDM server is running. • For Cause 2 Check the user ID and the password that are specified in the MDM linkage settings for the MDM server. • For Cause 3 Check the user ID, password, IP address, and port number that are specified in the MDM linkage settings for the proxy server. • For Cause 4 Register the smart device on the MDM server, and then obtain the information. • For Cause 5 Obtain troubleshooting information, and then contact Customer Support. • For Cause 6 In the Settings module, make sure that the information that is set for MDM linkage has not been deleted.

Event number	Type	Message	Cause	Actions to be taken
1115	Error	Failed to initialize a smart device.	• Cause 1 An attempt to connect to the MDM server and to the proxy server failed. • Cause 2 Authentication with the MDM server failed. • Cause 3 Authentication with the proxy server failed. • Cause 4 The smart device to be managed is not registered in the MDM system. • Cause 5 An error occurred in MDM linkage. • Cause 6 An error occurred while obtaining the settings information of the MDM server.	Select and take the appropriate actions from the list below: • For Cause 1 Check the host name and port number that are specified in the MDM linkage settings for the MDM server and the proxy server. Also, check whether the MDM server is running. • For Cause 2 Check the user ID and the password that are specified in the MDM linkage settings for the MDM server. • For Cause 3 Check the user ID, password, IP address, and port number that are specified in the MDM linkage settings for the proxy server. • For Cause 4 Register the smart device on the MDM server, and then obtain the information. • For Cause 5 Obtain troubleshooting information by using the appropriate command, and then contact Customer Support. • For Cause 6 In the Settings module, make sure that the information set for MDM linkage has not been deleted.
1116	Error	Failed to delete a smart device.	A database access error might have occurred.	In the Settings module, select the **Managed Devices** view, select the device you want to delete, and then delete that device.
1118	Error	Synchronization of device information with the MDM system (MDMName) failed.	• Cause 1 An error occurred in the connection to the MDM server or to the proxy server. • Cause 2 An error occurred in authentication with the MDM server. • Cause 3 An error occurred in the authentication for connection to the proxy server. • Cause 4 An error occurred in the MDM server. • Cause 5 An error occurred in MDM linkage. • Cause 6	• Cause 1 Make sure that there are no errors in the host name, IP address, or port number that were set in the settings window for MDM linkage. Also make sure that the MDM server is running. • Cause 2 Make sure that there are no errors in the user ID or password of the MDM server that were set in the settings window for MDM linkage. • Cause 3 Make sure that there are no errors in the IP address, port number, user ID, or password of the proxy

Event number	Type	Message	Cause	Actions to be taken
1118	Error	Synchronization of device information with the MDM system (MDMName) failed.	An error occurred while settings information of the MDM server was being obtained. • Cause 7 The server certificate of the MDM server is invalid.	server that were set in the settings window for MDM linkage. • Cause 4 Contact the MDM server administrator. • Cause 5 Collect troubleshooting information by using the appropriate command, and then contact Customer Support. • Cause 6 Check whether the settings information set in the settings window for MDM linkage has been deleted. • Cause 7 Execute the keytool command to check whether the server certificate has been imported. If it has not, execute the keytool command to import the server certificate. For details about the keytool command, see the relevant documentation.
1132	Error	A fatal error occurred during collection of the revision history.	An internal error occurred.	Collect troubleshooting information, and then contact customer support.
1133	Error	Failed to output the file for saving the revision history.	• Cause 1 An internal error occurred. • Cause 2 The storage destination of the revision history does not exist, or you cannot connect to the destination. • Cause 3 The user name or password used to connect to the storage destination of the revision history is incorrect. • Cause 4 There might not be enough space on the disk where the revision history is stored.	Select and take the appropriate actions from the list below: • For Cause 1 Collect troubleshooting information by using the appropriate command, and then contact customer support. • For Cause 2 Make sure that the storage destination of the revision history exists and that you can connect to the destination. • For Cause 3 Make sure that the user name and password that you specified during setup are correct. • For Cause 4 Either increase the amount of free space on the disk that was specified during setup for the storage destination of the revision history, or move the storage destination of the revision history to a disk that has sufficient free space.

The following table describes the log files that are output when an error occurs:

Log type	Output destination	File name	Description
Message log files	*JP1/IT Desktop Management-installation-destination-folder*\mgr\log	JDNMAIN*n*.log# (*n* = 1 to 9)	Outputs information that you can use to check the operational status of JP1/IT Desktop Management.
Event logs	Operating system event log	--	Outputs information on the startup of, the shutdown of, and critical errors generated byJP1/IT Desktop Management. Information on critical errors includes information that is not output to message log files. Use the operating system's Event Viewer to check the event logs.

Generation control is used to manage the files. When the size of the log file exceeds the limit, a new log file is created with the following number. The number starts from 1. If the number reaches 9, it returns to 1.

Obtain the troubleshooting information by using the `getlogs` command as required. For details about the `getlogs` command, see 17.28 getlogs (collecting troubleshooting information).

Related Topics:

- 13.1 Viewing event details

18.10 Troubleshooting problems with agents

This section describes what actions to take for problems that occur with an agent, and how to obtain troubleshooting information.

For information on errors that occurred when JP1/IT Desktop Management - Agent was deployed, please check the Events module.

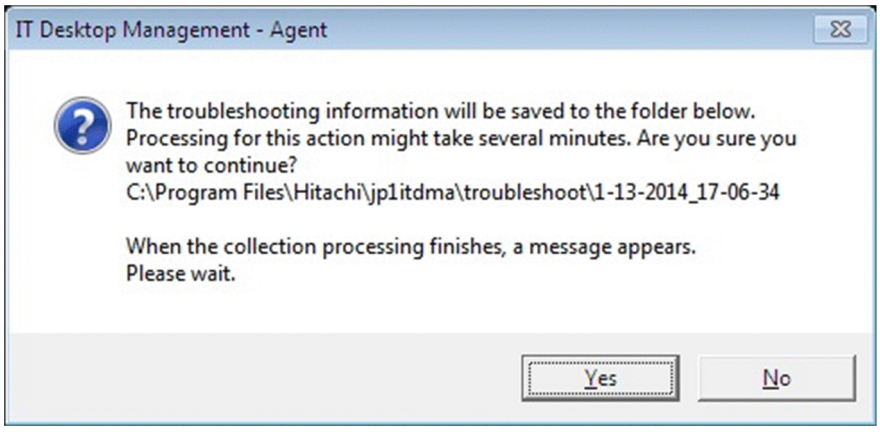
To obtain troubleshooting information for an agent:

Obtain troubleshooting information on the computer where the problem occurred. Note that you must use a user that has Administrator privileges to execute the command.

If a problem occurred on a computer that has an agent for off-line management installed, then in addition to the information that can be collected by performing the following procedures, collect the files in the Data folder that was generated by the Information Collection Tool.

1. Double click `getlogs.vbs`.

   A dialog box confirming that you want to obtain troubleshooting information is displayed.

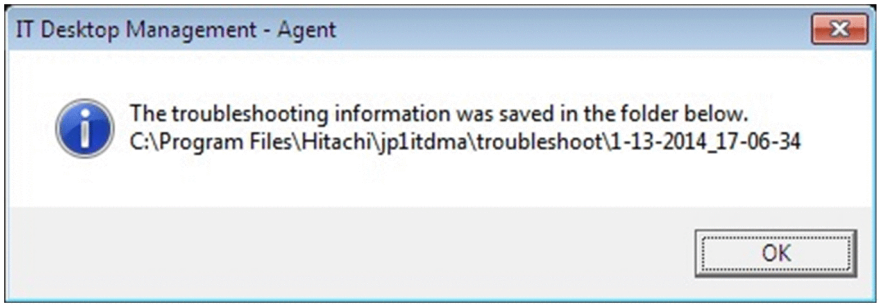


   The location of `getlogs.vbs` is as follows:

   JP1/IT-Desktop-Management-Agent-installation-destination-folder\bin

2. Click the **Yes** button.

   Collection of troubleshooting information begins. When the collection of troubleshooting information finishes, a dialog box indicating completion appears. This dialog box shows the location of the troubleshooting information.



   The location of the troubleshooting information that was collected is as follows:

   JP1/IT-Desktop-Management-Agent-installation-destination-folder\troubleshoot\YYYY-MM-DD_hh-mm-ss#

   # YYYY represents the year, MM represents the month, DD represents the day, hh represents the hour, mm represents the minute, and ss represents the second.

3. Click the **OK** button.
   The dialog box closes.

The following table describes the troubleshooting information that can be collected by performing the above procedure:

Troubleshooting information	Contents
Agent logs	*JP1/IT Desktop Management -Agent-installation-destination-folder*\log
System information	• System information The result of `msinfo32/nfo`. • Environment variables The result of running the `SET` command. • Registry information Registry entries that are located under HKEY_LOCAL_MACHINE_SOFTWARE\Hitachi. • File information A list of sub-folders and files that are located under *JP1/IT Desktop Management -Agent-installation-destination-folder*. • Event logs Application, System, and Security logs.

To undo changes to settings that were made during security Auto Enforcement:

The following table explains how to undo changes to security settings on a target management computer that were made when applying a security policy or during a security Auto Enforce:

Security settings	Action
Security updates	Perform the following two steps: • From the applicable computer, manually uninstall the security updates. • From the Windows Control Panel, start **Windows Update** in order to return to the original settings.
Software use	Perform the following two steps: • If you have installed mandatory software, uninstall it as necessary. • If you have uninstalled unauthorized software, install it as necessary.
Windows services	From the Windows Control Panel, start **Administrative Tools**, and then double-click **Services**. Return unauthorized services to their original settings.
Operating system security settings	Check and change the following items. Note that the exact method will differ depending on the settings and on your operating system. • Settings in the **Properties** pane of **My Computer**. • Settings in the **Screen Properties** view. • Settings in the **Administrative Tools** that are located in the **Control Panel**. • Settings for Explorer. • Items that were edited in the Registry.
Restricted operations (settings for usage supression and startup suppression)	Uninstall the agent programs.

18.11 Troubleshooting problems with a site server

Operation logs cannot be stored in the database

Operation logs cannot be stored if a site server's database runs low on space. In such cases, create a new site server, and then specify the new server as the location where operation logs are to be stored.

To resolve the problem of insufficient free space for a site server's database:

1. Create a new site server.
2. Add the new site server to the site server group that the Agent is connected to.

18.12 Troubleshooting problems in multi-server configuration

Cannot log in to the management server

Make the following checks:

- Make sure that the database server is running.
- Check whether a network failure has occurred between the management server and the database server.

Cannot access a data folder shared between servers

Make the following checks:

- Make sure that the database server is running.
- Check whether a network failure has occurred between the management server and the database server.

When a failure occurs, a message will appear in the JP1/IT Desktop Managementview. Determine the cause of the problem and the actions to be taken by following the instructions in the message, and then take the necessary actions.

In the Events module, if you find an event that requires action to be taken, check the event message, and then take the necessary action.

Also, log files are output when an error occurs. Check the log files for the cause of the error and the actions to be taken.

The following table describes the causes of and actions to be taken for events that require such action:

Event number	Type	Message	Cause	Actions to be taken
1121	Error	An error occurred in the service (JP1_ITDM_Service). Could not access the data folder shared between servers.	• Cause 1 The database server is not running. Alternatively, a network failure might have occurred. • Cause 2 The user ID or the password specified for the data folder that is shared between the servers is incorrect.	Select and take the appropriate actions from the list below: • For Cause 1 Start the database server. Alternatively, check the network connection between the management server and the database server. • For Cause 2 Make sure that the user name and the password that are used to connect to the shared data-folder are correct.

The following table describes the log files that are output when an error occurs:

Log type	Output destination	File name	Description
Message log files	*JP1/IT Desktop Management-installation-destination-folder*\mgr\log	JDNMAIN*n*.log[#] (*n* = 1 to 9)	Outputs information that you can use to check the operational status of JP1/IT Desktop Management.
Event logs	Operating system event log	--	Outputs information on the startup of, the shutdown of, and critical errors generated by JP1/IT Desktop Management. Information on critical errors includes information that is not output to message log files. Use the operating system's Event Viewer to check the event logs.

Legend: --: Not applicable

Generation control is used to manage the files. When the size of the log file exceeds the limit, a new log file is created with the following number. The number starts from 1. If the number reaches 9, it returns to 1.

Obtain the troubleshooting information by using the `getlogs` command as required. For details about the `getlogs` command, see 17.28 getlogs (collecting troubleshooting information).

Related Topics:

- 13.1 Viewing event details

18.13 Troubleshooting problems during remote control

The remote computer's screen is not displayed on the controller

If an application that was created in Java2 and that uses Direct Draw to draw graphics is activated on the remote computer, the remote computer's screen might not be displayed on the controller.

Action to be taken

On the remote computer, specify the following option when starting Java2 so that Java2 does not use Direct Draw.

```
-Dsun.java2d.noddraw=true
```

Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000 does not start after installing the Agent

If another company's remote-control product was already installed, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000 might not start after installing the Agent

Actions to be taken

The following procedure explains how to uninstall the other company's remote-control product and then reinstall the Agent:

1. Start the operating system in Safe Mode, and then uninstall the Agent.
2. Restart the computer.
3. If another company's remote-control product was already installed, uninstall that product.
4. Restart the computer.
5. Re-install the Agent.

The following procedure explains how to start the computer in Safe Mode:

1. Restart the computer.
2. If a message appears at the bottom of the screen requesting that you press the **F8** key to display startup options, press the **F8** key.
3. Use the arrow keys to select **Safe Mode**, and then press the **Enter** key.
4. Use the arrow keys to select the operating system that you want to start.

18.14 Troubleshooting problems when controlling network access

A device that was previously blocked from accessing the network is now permitted to do so, but the device does not immediately connect to the network

If permission to access the network is manually set in the Device module for a device that had previously been blocked from accessing the network, it might take a few minutes for the device to reconnect to the network.

Actions to be taken

Wait a few minutes until the device can connect to the network. If the device still cannot connect to the network, restart the device.

No devices can connect to the network

If you are using a white list method and you have not granted network-access permission to the router, you will not be able to use the network.

Actions to be taken

If the router is blocked from accessing the network, network monitor settings cannot be changed, because communication with the management server is not possible. In this case, open the Windows **Control Panel** on the computer that has the network monitor enabled, open **Management Tools**, open **Services**, and then stop the service JP1_ITDM_Network Monitor (displayed as NXNetMonitor). After that, connect to the management server and change the settings for the network control list. Note that depending on the router, you might need to restart the router.

Related Topics:

- 8.7.2 Editing devices in the network control list

18.15 Troubleshooting problems when browsing operation logs

Operation logs that are stored in the site server cannot be browsed

If you cannot browse operation logs that are stored in the site server, the cause of the problem might be one of the following:

1. A problem has occurred in the network between the management server and the site server.
2. The service on the site server or the database on the site server is stopped.

Action to be taken

In the Events module or the message log files of the site server, check whether anything has occurred that might be the cause of the problem.

Related Topics:

- 17.17 recreatelogdb (recreating an operation log index on the site server)
- 17.18 movelog (moving operation logs on the site server)
- 17.19 deletelog (deleting operation logs on the site server)

18.16 Troubleshooting problems during Active Directory linkage

When a device links with Active Directory, an event that has a message such as "'Auto Enforce' failed because it differs from the group policy that is already applied to the device" might be output, even if the security settings in the security policy are set to "Auto Enforce".

Action

In such cases, the group policy settings for Active Directory and the security policy for JP1/IT Desktop Management might be in conflict. Because JP1/IT Desktop Management settings take priority over Active Directory settings, change the group policy settings for Active Directory as necessary.

To check group policy settings for Active Directory:

1. From the Windows **Start** menu, select **Run**.
2. In the **Open** box, enter `gpedit.msc`.
3. In the group policy that appears, select **Local Computer Policy**, **Computer Configuration**, **Windows Settings**, and then **Security Settings**.

The group policy for Active Directory will be displayed. Please check the settings.

18.17 Troubleshooting problems during MDM linkage

Information about smart devices is not updated

If authentication information for the remote MDM system is not set correctly, information about smart devices cannot be obtained.

Action

Check if an event number that has event number 1108 or a message that has an ID of KDEX5427-E has been output. If such an event or message has been output, the password that is set in **MDM Linkage Settings** in the Settings module is incorrect. Set the correct password.

18.18 Troubleshooting problems during JP1/IM linkage

This section describes what actions to take when a problem occurs in the JP1/IM linkage configuration system:

Events are not reported to JP1/IM

If JP1/IT Desktop Management and JP1/Base are not communicating with each other, JP1/IM events are not reported.

Action

Check if an event that has event number 1120 or a message that has an ID of KDEX6511-E has been output. If such an event or message has been output, check the configuration procedure and revise the settings.

18.19 Troubleshooting problems with the database

A database connection error occurs

If a database connection error occurs, the cause of the error might be one of the following:

1. The database is stopped or is currently starting.
2. The database is in blocked status.

Actions to be taken

If the cause of the error is item 1 above, use the `stopservice` command followed by the `startservice` command to start the management server service.

If the cause of the error is item 2 above, initialize the database by using JP1/IT Desktop Management setup.

Backing up, restoring, or reorganizing of the database fails

If backing up, restoring, or reorganizing of the database fails, the cause of the problem might be one of the following:

1. You do not have permission to access the folder in which the database is stored.
2. An I/O error has occurred.

Actions to be taken

If the cause of the problem is item 1 above, check the permissions that you have to access the folder in which the database is stored.

If the cause of the problem is item 2 above, check whether a disk failure has occurred.

Related Topics:

- 17.26 stopservice (stopping services)
- 17.27 startservice (starting services)

19 Messages

This section lists and describes the messages and events of JP1/IT Desktop Management.

19.1 Format of message explanations

JP1/IT Desktop Management messages consist of a message ID, message type, and message text.

The following shows the format of message IDs and message types, and the meanings of the constituent parts of a message.

Format: KDEXpnnn-m

KDEX

Indicate a message output from JP1/IT Desktop Management.

p

Indicates the component that output the message. The following table shows the correspondence between the numbers and the components:

Number	Component
1	Installer or setup
2	GUI
3	API
4	Utility
5	Manager service
6	Agent control
7	Agent
8	Site server

nnn

Indicates the message number.

m

Indicates the message type. The following are the message types:

Message code	Type	Description
E	Error	Processing could not continue because an error occurred.
W	Warning	A warning was output, and processing continued. See the warning message to determine whether there is a problem.
I	Information	Processing ended successfully.
Q	Query	The system is waiting for a user response.
K	Processing	Processing is currently being performed.

19.2 List of messages

KDEX1001-E

The user does not have Administrative Privileges. Installation is cancelled.
[Cause] The user does not have Administrative Privileges.
[Action] Cancel installation.
[Workaround] Retry installation as a user with Administrative Privileges.

KDEX1002-E

Installation failed. The OS is not supported.
[Cause] The OS is not supported.
[Action] Cancel installation.
[Workaround] Retry the installation on a supported OS.

KDEX1003-E

A newer version of the software is already installed.
Installation is canceled.
[Cause] A newer version of the software is already installed.
[Action] Cancel installation.
[Workaround] Compare the two software versions (between installed and intended to be installed). You can retry installation after uninstalling the installed software.

KDEX1004-W

Insufficient disk space for the database folder.
Free disk space (required): *disk-space-required-to-create-database* GB
[Cause] The disk space is not sufficient for installation to proceed.
[Action] Return to the main screen and continue installation.
[Workaround] Free the disk space or specify an alternate disk with sufficient space.

KDEX1005-W

No components have been selected.
[Cause] No components are selected for installation.
[Action] Return to the main screen and continue installation.
[Workaround] Select a component to install.

KDEX1006-W

Invalid path. You cannot specify a path exceeding *number-of-bytes* bytes.
[Cause] The specified path exceeds the maximum path length.
[Action] Return to the main screen and continue installation.
[Workaround] Enter a valid path.

KDEX1008-E

An error occurred during installation/uninstallation.
The operation is canceled.
[Cause] An error occurred during installation/uninstallation.
[Action] Cancel installation/uninstallation.
[Workaround] Retry installation/uninstallation. If the problem persists, contact Support Service.

KDEX1021-W

Could not configure Windows firewall.
[Cause] Could not configure Windows firewall.
[Action] Continue installation.
[Workaround] If Windows firewall is in use, confirm the settings and execute the addfwlist.bat command to enable communication.

KDEX1022-W

Could not restore Windows firewall setting.
[Cause] Could not restore Windows firewall setting.
[Action] Continue uninstallation.
[Workaround] If Windows firewall is in use, confirm the settings and execute the netsh command to disable communication (for the program [*Product Name*]).

KDEX1024-W

The folder path contains an invalid character ('*invalid-character*').
[Cause] The folder path contains an invalid character.
[Action] Return to the main screen and continue installation.
[Workaround] Enter a valid folder path.

KDEX1027-E

An installation instance is currently running.
Retry installation after this installation instance ends.
[Cause] An installation instance is running.
[Action] Cancel installation.
[Workaround] Retry installation after the installation instance (current) has ended.

KDEX1030-I

Installation complete.

KDEX1031-W

Please specify the User name and Company name.
[Cause] The User name or Company name is not specified.
[Action] Return to the main screen and continue installation.

[Workaround] Specify User and Company name.

KDEX1032-W

Could not delete the database.
[Cause] The database was not deleted properly during uninstallation.
[Action] Continue uninstallation.
[Workaround] After uninstallation is complete, delete the database and local data folders.
Default database folder: <*Application data folder for All Users*>\Hitachi\jp1itdmm\Database\db
Default local data folder: <*Application data folder for All Users*>\Hitachi\jp1itdmm\LocalData
Default operation log database folder: <*Application data folder for All Users*>\Hitachi\jp1itdmm\Database\oplogdb

KDEX1033-E

Insufficient disk space for the installation folder.
[Cause] The disk space is insufficient for installation to proceed.
[Action] Cancel installation.
[Workaround] Free the disk space or specify an alternate disk with sufficient space. Then, retry installation.

KDEX1034-E

Does not support Silent installation.
Installation is canceled.
[Cause] Silent installation was executed.
[Action] Cancel installation.
[Workaround] Run installation without invalid arguments.

KDEX1035-W

Please specify *folder-specified-by-installer* on a local disk.
[Cause] A non-local folder was specified.
[Action] Return to the main screen and continue installation.
[Workaround] Specify a local folder.

KDEX1036-W

There is no disk space (sufficient) to upgrade the database.
Free disk space (required): *disk-space-required* GB, Mount point: *mount-point*
[Cause] There is no disk space (sufficient) to upgrade the database.
[Action] Return to the main screen and continue installation.
[Workaround] Free disk space or perform custom installation, and then change the database folder (during Setup).

KDEX1037-E

An error occurred during installation.
Might be insufficient disk space for *Folder Specified by Setup*.

[Cause] Insufficient disk space for installation to proceed.

[Action] Cancel installation.

[Workaround] Either free the disk space, Or perform custom installation, and then change the corresponding folder (during Setup).

KDEX1038-E

An error occurred during installation/uninstallation.

Files or folders in the installation folder may be used by another process.

[Cause] Files or folders in the installation folder are currently in use.

[Action] Cancel installation/uninstallation.

[Workaround] Confirm that files or folders in the installation folder are not used by other processes. Then, retry installation/uninstallation.

KDEX1040-W

Component registration failed.

After installation is complete, from the **Start** menu, run **Component Registration**.

[Cause] Component registration failed.

[Action] Continue installation.

[Workaround] After installation is complete, from the **Start** menu, run **Component Registration**.

KDEX1043-E

Could not register the license.

Installation is canceled.

[Cause] An error occurred while registering the license.

[Action] Cancel installation.

[Workaround] Retry installation. If the problem persists, contact Customer Support.

KDEX1046-W

Cannot use the folder path specified for *folder-specified-by-installer*.

A file with a same name as the specified folder already exists in the given path.

[Cause] A file with the same name as the specified folder already exists in the given path. Cannot create a folder with the same name.

[Action] Return to the main screen and continue installation.

[Workaround] Change the name of the existing file, delete the file, or specify a different folder path.

KDEX1047-W

The computer name (*computer-name*) contains an invalid character.

Valid characters are alphanumerals and hyphen(-).

The first character must be an alphabet and the last character must be an alphabet or a number.

[Cause] The computer name contains an invalid character.

[Action] Return to the main screen and continue installation.

[Workaround] Change the computer name and restart the OS. Then, retry installation.

KDEX1049-E

Failed to proceed installation since *Excluded software* is currently installed.

[Cause] Excluded software from *Product name* has been installed in the computer.

[Action] Cancel installation.

[Workaround] Retry installation after uninstalling *Excluded software* since both the software cannot be used simultaneously.

KDEX1050-Q

Hard disk space might become insufficient later due to large volume of operation logs. Click [OK] to continue.

Required space for database:*required-space* GB

[Cause] Insufficient hard disk space for folders (in which the database will be created).

[Action] If you want to continue, click [OK]. Clicking [Cancel] will return to the previous screen.

[Workaround] Increase the available disk space for database creation, or specify an alternate hard disk with sufficient space.

KDEX1052-I

Restart the OS after completing *"installation" or "uninstallation"*.

KDEX1053-E

Installation failed. The OS language is not supported.

[Cause] The OS language is not supported.

[Action] Cancel installation.

[Workaround] Retry installation on the OS with supported language.

KDEX1054-E

Service operation failed. Service name=*service-name*

[Cause] An error occurred while operating the service.

[Action] Cancel installation/uninstallation.

[Workaround] Check the message logs, and take action based on the error logs.

KDEX1055-E

Installation of *name-of-product-for-which-installation-was-executed* cannot continue.

[Cause] Required software (*a prerequisite product name*) is not installed in the computer.

[Action] Cancels installation of *name-of-product-for-which-installation-was-executed*.

[Workaround] Install the required software (*a prerequisite product name*), and then retry installation of *name-of-product-for-which-installation-was-executed*.

KDEX1056-E

Installation cannot continue.

[Cause] There is not enough free space on the disk containing the database folder.

Required space: *Required space for database* GB

[Action] Cancels installation.

[Workaround] Increase the free disk space, or specify a folder on a disk that has enough free space, and then retry installation.

KDEX1057-E

Failed to execute the command. The specified arguments are invalid. Command name=*command-name*.
[Cause] The specified arguments are invalid.
[Action] Cancel command execution.
[Workaround] Confirm the command arguments, and retry execution.

KDEX1058-E

The troubleshooting information folder is not accessible.
[Cause] The specified troubleshooting information folder does not exist or is not accessible.
[Action] Cancel command execution.
[Workaround] Check if the specified folder exists and is accessible. Then, retry command execution.

KDEX1059-E

Failed to execute the command. You do not have the required permissions. Command name=*command-name*.
[Cause] The command was executed by a user without Administrator privileges.
[Action] Cancel command execution.
[Workaround] Retry executing the command as a user with Administrator privileges.

KDEX1060-E

Could not collect troubleshooting information.
[Cause] A critical error occurred during command execution.
[Action] Cancel command execution.
[Workaround] Contact Customer Support.

KDEX1061-I

Collected the troubleshooting information.

KDEX1062-W

Could not collect some troubleshooting information.
The following troubleshooting information are not collected.
Folders and files failed to be collected.
[Cause] Insufficient disk space for the troubleshooting information folder.
[Action] Cancel command execution.
[Workaround] Free the disk space, and retry command execution. If the problem persists, get troubleshooting information displayed above individually.

KDEX1063-E

Failed to write to the folder.

Folder path = *A folder path*

[Cause] The folder is not accessible or an I/O error occurred.

[Action] Cancel command execution.

[Workaround] Check if the specified folder is writable. Then, retry command execution.

KDEX1065-E

Installation cannot continue.

[Cause] There is not enough free space on the disk containing the installation folder.

Required space: *Required space for installation* MB

[Action] Cancels installation.

[Workaround] Increase the amount of free space on the disk containing the installation folder, and then retry the installation. If you are distributing software by using a package distribution task, edit the site server package, change the installation folder of the install command (the third argument) to a folder on a disk that has enough free space, and then retry the distribution.

KDEX1066-E

Installation cannot continue.

[Cause] A folder that is not on the local disk was specified for the installation folder.

[Action] Cancels installation.

[Workaround] Edit the site server package, specify a local disk for the installation folder of the install command (the third argument), and then retry the distribution.

KDEX1067-W

The database could not be deleted.

[Cause] An error occurred during database deletion.

[Action] Continue uninstallation.

[Workaround] After uninstallation is complete, delete the database folder.

Default database folder: <*application-folder-for-All-Users*>\Hitachi\jp1itdms\Database\db

KDEX1068-E

The trial version cannot be installed because the actual product is already installed.

[Cause] A user attempted to install a trial version in an environment where the product was already installed.

[Action] Cancels installation of the trial version.

[Workaround] If necessary, uninstall the product, and then install the trial version.

KDEX1069-E

Installation cannot continue.

[Cause] A path that exceeds *maximum-number-of-bytes-of-path* bytes is specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter.

[Action] Cancels installation.

[Workaround] Check the path specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter of the jdn_manager_setup.conf file, and then re-create the package for distributing site server programs.

KDEX1070-E

Installation cannot continue.

[Cause] The path specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter contains an invalid character (*invalid-character*).

[Action] Cancels installation.

[Workaround] Check the path specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter of the jdn_manager_setup.conf file, and then re-create the package for distributing site server programs.

KDEX1071-E

Installation cannot continue.

[Cause] Either a folder that is not on the local disk or an invalid path is specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter.

[Action] Cancels installation.

[Workaround] Check the path specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter of the jdn_manager_setup.conf file, and then re-create the package for distributing site server programs.

KDEX1072-E

Installation cannot continue.

[Cause] The value specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter is outside the valid range. Valid range: *valid-range*

[Action] Cancels installation.

[Workaround] Check the value specified for the *parameter-specified-for-jdn_manager_setup.conf* parameter of the jdn_manager_setup.conf file, and then re-create the package for distributing site server programs.

KDEX1073-E

Installation cannot continue.

[Cause] The folders specified for the *parameter1-specified-for-jdn_manager_setup.conf* and *parameter2-specified-for-jdn_manager_setup.conf* parameters are the same folder, or one is a subfolder of the other.

[Action] Cancels installation.

[Workaround] Check the paths specified for the *parameter1-specified-for-jdn_manager_setup.conf* and *parameter2-specified-for-jdn_manager_setup.conf* parameters of the jdn_manager_setup.conf file, and then re-create the package for distributing site server programs.

KDEX1074-E

Installation cannot continue.

[Cause] A path exceeding *maximum-number-of-bytes-of-path* bytes is specified for the installation folder.

[Action] Cancels installation.

[Workaround] Edit the site server package, change the specification of the installation folder of the install command (the third argument), and then retry the distribution.

KDEX1075-E

Installation cannot continue.

[Cause] The path for the installation folder contains an invalid character (*invalid-character*).

[Action] Cancels installation.

[Workaround] Edit the site server package, change the specification of the installation folder of the install command (the third argument), and then retry the distribution.

KDEX1076-E

The full-product version cannot be installed because the trial version is installed.

[Cause] An attempt was made to install the full-product version in an environment in which the trial version was installed.

[Action] Cancels installation of the full-product version.

[Workaround] Remove the trial version, and then try to install the full-product version again.

KDEX1077-E

Failed to write to the data folder shared between servers.

(data folder shared between servers = *pass-of-data-folder-shared-between-servers*)

[Cause] You do not have permission to access the data folder shared between servers, or an I/O error occurred.

[Action] Cancels installation.

[Workaround] Verify that you are able to write to the data folder shared between servers, and then retry installation.

KDEX1078-W

Failed to delete the ODBC data source.

[Cause] An error occurred during deletion of the ODBC data source.

[Action] Continues removal.

[Workaround] After the product has been removed, start the 32-bit version of ODBC Data Source Administrator, and then delete the system data source (JDN_HIRDB).

KDEX1501-E

Failed to start Setup.

[Cause] Installation was terminated abnormally.

[Action] Cancel Setup.

[Workaround] Perform re-installation.

KDEX1502-W

Could not find the import file.

[Cause] The import file does not exist.

[Action] Return to the main screen and continue Setup.

[Workaround] Specify a valid and existing import file.

KDEX1503-E

An error occurred during Setup.

Setup is canceled.

[Cause] An error occurred during Setup.

[Action] Cancel Setup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1504-E

Failed to initialize the database.

[Cause] An error occurred while initializing the database.

[Action] Cancel Setup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1505-E

Failed to delete the database or the ODBC data source.

[Cause] Possible causes are as follows:

(1) You do not have permission to access the database folder, the operation log database folder, or the local data folder.

(2) An I/O error occurred.

[Action] Cancels setup.

[Workaround] Check the following, and then retry setup.

(1) Verify that you have permission to access the database folder, the operation log database folder, and the local data folder.

(2) Verify that no disks have failed.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX1506-E

Failed to create the database or the ODBC data source.

[Cause] Possible causes are as follows:

(1) You do not have permission to access the database folder, the operation log database folder, or the local data folder.

(2) An I/O error occurred.

[Action] Cancels setup.

[Workaround] Check the following, and then retry setup.

(1) Verify that you have permission to access the database folder, the operation log database folder, and the local data folder.

(2) Verify that no disks have failed.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX1508-E

The database folder could not be changed.

[Cause] An error occurred while changing the database folder. The possible reasons are:

(1) Improper access privileges to the database folder, the operation log database folder, the operation log backup folder, or the database extraction folder.

(2) An I/O error occurred.

[Action] Cancel Setup.

[Workaround]

(1) Confirm the access rights of the database folder, the operation log database folder, the operation log backup folder, and the database extraction folder.

(2) Confirm that a disk failure has not occurred.

If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1509-E

An error occurred during Setup.

Setup is canceled.

[Cause] An error occurred during Setup.

[Action] Cancel Setup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1510-W

The specified value for *Input item name (ex. Logical IP Address)* is invalid (out of valid range: *Valid range*).

[Cause] An invalid value for *Input item name (ex. Logical IP Address)* was specified.

[Action] Return to the main screen and continue Setup.

[Workaround] Specify a value within the valid range.

KDEX1511-E

The user does not have Administrative Privileges.

[Cause] The user doest not have Administrative Privileges.

[Action] Cancel Setup.

[Workaround] Retry Setup as a user with Administrative Privileges.

KDEX1512-E

Currently, another Setup instance is running.

[Cause] Another Setup instance is currently running.

[Action] Cancel the new Setup.

[Workaround] Continue running the existing Setup instance.

KDEX1513-E

Could not find the setting file for Setup or the file may be corrupted.

[Cause] The setting file (Setup) does not exist or is corrupted.

[Action] Cancel Setup.

[Workaround] Retry installation after uninstalling the program.

KDEX1514-E

Could not upgrade the database.

[Cause] An error occurred while upgrading the database. The possible reasons are:

(1) Improper access privileges to database folder, local data folder, or database extraction folder.

(2) An I/O error occurred.

[Action] Cancel Setup.

[Workaround]

(1) Confirm the access rights of database folder, local data folder, and database extraction folder.

(2) Confirm that a disk failure has not occurred.

If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1516-E

Could not stop the service. Service name=*service-name*.

Setup is canceled.

[Cause] An error occurred while stopping the service.

[Action] Cancel Setup.

[Workaround] Check the message logs and take action based on the errors in the logs.

KDEX1517-E

Could not start the service. Service name=*service-name*.

Setup is canceled.

[Cause] An error occurred while starting the service.

[Action] Cancel Setup.

[Workaround] Check the message logs, and take action based on the error logs.

KDEX1518-E

Could not chage the startup service type. Service name=*service-name*.

Setup is being canceled.

[Cause] An error occurred while changing the startup service type.

[Action] Cancel Setup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1519-Q

To continue Setup, JP1/IT Desktop Management - Manager services must be stopped. Do you want to stop the service? The service will start automatically when the Setup is complete.

KDEX1520-Q

To continue Setup, set the cluster resources associated with the following services offline. Then, click OK to resume Setup.

Set the cluster resources online after the Setup is completed.

(service = *service-name*)

KDEX1521-Q

To continue Setup, set the cluster resources associated with the following services offline. Then, click OK to resume Setup.
(service = *service-name*)

KDEX1524-W

Insufficient disk space. Required free disk space: *required-free-disk-space* GB, Mount point: *mount-point*.
[Cause] Insufficient disk space.
[Action] Return to the main screen and continue Setup.
[Workaround] Free the disk space or specify an alternate disk with sufficient space.

KDEX1525-W

Invalid cluster configuration content.
The cluster resource status is either offline or another node is set as the resource owner.
[Cause] Either the cluster resource status is offline or another node is set as the resource owner.
[Action] Return to the main screen and continue Setup.
[Workaround] Confirm the status and ownership of the cluster resource.

KDEX1526-I

(JP1_ITDM_Web Container) service has started.

KDEX1527-I

(JP1_ITDM_Web Container) service has stopped.

KDEX1528-E

Could not start (JP1_ITDM_Web Container)service.
[Cause] An error occurred while starting the service.
[Action] Cancel the service initiation.
[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1529-E

(JP1_ITDM_Web Container) service has terminated abnormally due to an unexpected cause.
[Cause] An unrecoverable error occurred in the service.
[Action] Stop the service.
[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1530-E

Could not start (JP1_ITDM_Web Container) service since JP1/IT Desktop Management - Manager Setup was not complete.

[Cause] The service was started before the JP1/IT Desktop Management - Manager Setup was complete.
[Action] Cancel (JP1_ITDM_Web Container) service initiation.
[Workaround] Complete the JP1/IT Desktop Management - Manager Setup first and then start the service.

KDEX1531-I

Setup successful.

KDEX1532-E

Setup failed.

KDEX1533-W

Could not create login shortcut for JP1/IT Desktop Management - Manager.
To log in JP1/IT Desktop Management - Manager, use the URL:
URL-to-log-in-to-JP1/IT Desktop Management - Manager
To launch from a shortcut, create an internet shortcut of the above URL in the following file:
full-path-of-<installation folder>\mgr\conf\jdn_login.url
[Cause] An error occurred while creating a login shortcut for JP1/IT Desktop Management - Manager.
[Action] Continue Setup.
[Workaround] To log in JP1/IT Desktop Management - Manager, access the URL provided in this message.
To launch from a shortcut, create an internet shortcut as directed.

KDEX1534-W

The folder specified for the *Folder Specified by Setup* is unusable.
[Cause] Among the following folders that were specified during the current or previous setup, at least two folders are identical or have a parent-child relationship:
- Database folder
- Data folder
- Local data folder
- Database backup folder

[Action] Return to the previous window and continue the setup.
[Workaround] For the following folders that were specified during the current or previous setup, specify a unique folder that does not have a parent-child relationship with another:
- Database folder
- Data folder
- Local data folder
- Database backup folder

KDEX1535-W

Specify *folder-specified-by-setup* on a local disk.
[Cause] *folder-specified-by-setup* is not on the local disk, or the path is invalid.
[Action] Return to the main screen and continue Setup.

[Workaround] Specify a folder on the local disk for folder types like database, data, local data, and database extraction.

KDEX1536-E

An error occurred during Setup.

Insufficient disk space for *folder-specified-by-setup*.

[Cause] Not enough disk space for the specified folders.

[Action] Cancel Setup.

[Workaround] Free the disk space and retry Setup or specify a folder on a disk with sufficient free space.

KDEX1537-W

Invalid content in import file.

[Cause] An invalid import file was specified.

[Action] Return to the main screen and continue Setup.

[Workaround] Specify a correct import file. If the specified import file is not correct, try copying the import file from the primary server.

KDEX1538-E

An error occurred during Setup.

Insufficient disk space.

Required free disk space=*required-free-disk-space* GB, Mount point=*mount-point*

[Cause] Insufficient disk space to complete Setup.

[Action] Cancel Setup.

[Workaround] Free the disk space and retry Setup or specify a folder on a disk with sufficient free space.

KDEX1539-W

Insufficient disk space to upgrade the database.

Required free disk space=*required-free-disk-space* MB, Mount point=*mount-point*.

[Cause] Insufficient disk space to complete Setup.

[Action] Return to the main screen and continue Setup.

[Workaround] Free the disk space and retry Setup or specify a folder on a disk with sufficient free space.

KDEX1543-E

The license could not be registered.

License registration is being canceled.

[Cause] An error occurred while registering the license.

[Action] Cancel Setup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX1545-E

Could not launch Setup. Database Manager or a command is running.

[Cause] Setup was launched when the Database Manager or a command was running.

[Action] Cancel Setup launch.

[Workaround] Wait until the executing process (Database Manager or command) ends, and then retry Setup.

KDEX1546-W

You cannot specify a path that exceeds *The number of bytes* bytes for *Folder Specified by Setup*.

[Cause] The specified path for *Folder Specified by Setup* exceeds the maximum path length.

[Action] Return to the main screen and continue setup.

[Workaround] Enter a valid path.

KDEX1547-E

Could not start (JP1_ITDM_Web Container) service. An executing process (Setup, Database Manager, or a command) might be running.

[Cause] Started the (JP1_ITDM_Web Container) service when an executing process (Setup, Database Manager, or a command) was running.

[Action] Cancel the (JP1_ITDM_Web Container) service initiation.

[Workaround] Wait until the executing process (Setup, Database Manager, or command) ends, and retry starting (JP1_ITDM_Web Container) service.

KDEX1548-W

Invalid cluster configuration content.

[Cause] Secondary server option was not selected.

[Action] Return to the main screen and continue Setup.

[Workaround] Select the secondary server option, and continue Setup.

KDEX1550-W

The specified logical IP address for the cluster configuration is invalid.

[Cause] The specified logical IP address does not exist as a cluster resource.

[Action] Return to the main screen and continue Setup.

[Workaround] If on the primary server, check the specified logical IP address. If on the secondary server, check if the import file is correct.

KDEX1551-W

Cannot use the specified folder for *folder-specified-by-setup*.

A file with a same name as the specified folder already exists in the folder path.

[Cause] Cannot create a folder with this name in the folder path. Since the folder already contains a file with the same name.

[Action] Return to the main screen and continue Setup.

[Workaround] Change the name of the existing file, delete the file, or specify a different folder path.

KDEX1552-E

The computer name (*computer-name*) contains an invalid character.

Valid characters are alphanumerals and hyphen(-).
The first character must be an alphabet and the last character must be an alphabet or a number.
[Cause] The computer name contains an invalid character.
[Action] Cancel Setup.
[Workaround] Change the computer name and restart the OS. Then, retry Setup.

KDEX1555-W

Failed to connect *operation-log-backup-folder*.
[Cause] An error occurred while connecting to the specified network resource.
[Action] Return to the main screen and continue Setup.
[Workaround] Create a folder on a valid network or specify a folder on a local disk.

KDEX1556-W

Please specify folders on the network in UNC format.
[Cause] A network drive was specified.
[Action] Return to the main screen and continue Setup.
[Workaround] Set the folder in UNC format.

KDEX1557-W

The folder specified for *Folder Specified by Setup* is unusable.
[Cause] Among the following folders that were specified during the current or previous setup, at least two folders are identical or have a parent-child relationship:
- Folder specified in the Folder Settings window
- Operation log database folder
- Operation log storage folder
- Output folder for saving the revision history

[Action] Return to the previous window and continue the setup.
[Workaround] For the following folders that were specified during the current or previous setup, specify a unique folder that does not have a parent-child relationship with another:
- Folder specified in the Folder Settings screen
- Operation log database folder
- Operation log storage folder
- Output folder for saving the revision history

KDEX1558-W

The specified Username or Password is invalid.
[Cause] The Username or Password used for connecting to the network resource was invalid.
[Action] Return to the main screen and continue Setup.
[Workaround] Specify a valid Username and Password.

KDEX1559-E

An error occurred during setup.

Insufficient disk space for *folder-specified-in-Folder-Settings-window or operation-log-storage-location*.
[Cause] Insufficient disk space for the specified folder.
[Action] Cancel Setup.
[Workaround] Free the disk space and retry Setup or specify a folder on a disk with sufficient free space.

KDEX1560-E

An error occurred during Setup.
Failed to connect *operation-log-backup-folder*.
[Cause] An error occurred while connecting to the specified network resource.
[Action] Cancel Setup.
[Workaround] Specify a folder on a valid network or specify a folder on a local disk. Then retry Setup.

KDEX1561-E

An error occurred during Setup.
The Username or Password used for connecting to *operation-log-backup-folder* is invalid.
[Cause] The Username or Password specified for connecting to the network resource was invalid.
[Action] Cancel Setup.
[Workaround] Confirm that the Username and Password are valid, and then retry Setup.

KDEX1562-I

Username and Password has been set successfully to connect to the operation log backup folder.

KDEX1563-W

Specify *operation-log-storage-area* on a local disk.
[Cause] *operation-log-storage-area* is not on the local disk, or the path is invalid.
[Action] Return to the main screen and continue Setup.
[Workaround] Specify a folder on a local disk.

KDEX1564-Q

If the operation logs backup setting is off, the operations logs will be deleted. If you want to keep operations logs, change the automatic backup settings to on.
Click OK to start. Click Cancel to review.

KDEX1565-W

Invalid folder path for *operation-log-storage-area*.
[Cause] An invalid folder path is specified for *operation-log-storage-area*.
[Action] Return to the main screen and continue Setup.
[Workaround] Specify a valid folder path for *operation-log-storage-area*.

KDEX1566-W

The specified *folder-specified-by-setup* is not accessible.

[Cause] The possible reasons are:

(1) Either the cluster resource status is offline or another node is set as the resource owner.

(2) An I/O error occurred.

[Action] Return to the main screen and continue Setup.

[Workaround] Confirm the specified folder is accessible. If you are specifying the cluster shared disk, confirm the status and ownership of the disk resource.

KDEX1567-W

Component registration failed.

After setup is complete, from the **Start** menu, run **Component Registration**.

[Cause] Component registration failed.

[Action] Continue setup.

[Workaround] After setup is complete, from the **Start** menu, run **Component Registration**.

KDEX1568-W

Failed to start the service. Service name=*service-name*.

[Cause] An error occurred while starting the service.

[Action] Continue Setup.

[Workaround] Check the message logs, and take action based on the error logs.

KDEX1569-I

Restart the OS after completing Setup.

KDEX1570-Q

The settings will be modified so that operation logs are not collected. This will delete already collected operation logs.

(To obtain already collected operation logs and reference these logs in an environment where a site server is used and the operation logs are distributed, specify the settings so that operation logs are collected.)

Do you want to continue?

KDEX1571-E

The configuration file specified for setup is invalid.

[Cause] An invalid file was specified for the configuration file specified for setup.

[Action] Cancels setup.

[Workaround] Perform installation again. If the problem persists, use the troubleshooting information collection command to collect troubleshooting information, and contact Customer Support.

KDEX1572-E

The folder specified for the *folder-specified-by-the-configuration-file* is not usable.

[Cause] The specified folder is a database folder, data folder, or operation log data folder, or has a parent-child relationship with such a folder.

[Action] Cancels setup.

[Workaround] Specify a folder that is not a database folder, data folder, or operation log data folder, and does not have a parent-child relationship with such a folder.

KDEX1573-E

The path specified for the *folder-specified-by-the-configuration-file* is not usable.

[Cause] An invalid path or a path to a non-local disk was specified for *folder-specified-by-the-configuration-file*.

[Action] Cancels setup.

[Workaround] Specify a path on a local disk.

KDEX1574-E

The folder path specified for the *folder-specified-by-the-configuration-file* is not usable. An existing file has the same name as the path folder.

[Cause] The folder cannot be created because an existing file has the same name as the path folder.

[Action] Cancels setup.

[Workaround] Change the name of the existing file, delete the file, or specify a different folder path.

KDEX1575-E

The disk containing the folder specified for the *folder-specified-by-the-configuration-file* cannot be accessed.

[Cause] A disk failure occurred.

[Action] Cancels setup.

[Workaround] Make sure the disk containing the specified folder can be accessed.

KDEX1576-W

The folder specified for *folder-specified-by-setup* is unusable.

[Cause] Among the following folders that were specified during the current or previous setup, at least two folders are identical or have a parent-child relationship:

- Database folder
- Data folder
- Operation log data folder

[Action] Return to the previous window and continue the setup.

[Workaround] For the following folders that were specified during the current or previous setup, specify a unique folder that does not have a parent-child relationship with another:

- Database folder
- Data folder
- Operation log data folder

KDEX1577-E

Setup cannot start because a command is executing.

[Cause] Setup was executed while a command was executing.

[Action] Cancels the start of setup.

[Workaround] Wait until the command finishes, and then re-execute setup.

KDEX1578-W

The port number specified for *specified-reserved-port-number* cannot be used.

[Cause] A reserved port number was specified for *specified-reserved-port-number*.

[Action] Return to the main screen and continue Setup.

[Workaround] Specify another port number, and then retry Setup.

KDEX1579-E

An attempt to stop the service failed.

[Cause] Setup was executed during processing to start or stop the service used by JP1/IT Desktop Management - Manager.

[Action] Cancels setup.

[Workaround] Wait a while, and then re-execute Setup.

KDEX1580-E

An attempt to start the service failed (service name = *service-name*). Setup will be canceled.

[Cause] Setup was executed during processing to start or stop the service.

[Action] Cancels setup.

[Workaround] Wait a while, and then re-execute Setup.

KDEX1581-E

The service (*Web-Container-service-name*) cannot be started from a *type-of-server*. Service startup will be canceled.

[Cause] The service was started on a server other than the management server.

[Action] Cancels startup of the service.

[Workaround] Start the service (*Web-Container-service-name*) from the management server.

KDEX1582-W

Failed to connect to *data-folder-of-database-server*.

[Cause] The data folder shared between servers that was specified in the folder settings window cannot be connected to.

[Action] Returns to the previous window and continues setup.

[Workaround] Verify that the path of the specified data folder shared between servers is correct, and then check whether there are any problems in the network.

KDEX1583-W

Failed to read files from the database server.

[Cause] Possible causes are as follows:

(1) The path specified for the data folder shared between servers is incorrect.

(2) Database server setup is incomplete.

(3) You do not have permission to access the data folder shared between servers.

(4) An I/O error occurred.

[Action] Returns to the previous window and continues setup.

[Workaround]

(1) Specify the same path for both of the following:

- The path specified for the data folder in the folder settings window during database setup
- The path specified for the data folder shared between servers

(2) Verify that database server setup is complete.

(3) Verify that you have permission to both read from and write to the data folder shared between servers.

(4) Verify that no disks have failed.

KDEX1584-E

An error occurred during setup.

[Cause] The *management-server* is accessing the database.

[Action] Cancels setup.

[Workaround] Stop the service given below, which is used by JP1/IT Desktop Management - Manager on the *management-server*, and then retry setup.

(service = *service-name*)

KDEX1587-Q

From the management server, stop the service given below, which is used by JP1/IT Desktop Management - Manager. If you continue while this service is running, setup might not finish properly.

(service = *service-name-of-management-server*)

The database server service will stop automatically. The database server service that is stopped in this way will start automatically after setup is complete.

Are you sure you want to stop the database server service?

KDEX1588-Q

From the management server, stop the service given below, which is used by JP1/IT Desktop Management - Manager. If you continue while this service is running, setup might not finish properly.

(service = *service-name-of-management-server*)

Take offline the cluster resources associated with the service given below. After doing so, click [OK] to continue setup.

After setup is complete, bring the cluster resources back online.

(service = *service-name-of-database-server*)

KDEX1589-Q

From the management server, stop the service given below, which is used by JP1/IT Desktop Management - Manager. If you continue while this service is running, setup might not finish properly.

(service = *service-name-of-management-server*)

Take offline the cluster resources associated with the service given below. After doing so, click [OK] to continue setup.

(service = *service-name-of-database-server*)

KDEX1590-E

Failed to write to the data folder shared between servers.

(data folder shared between servers = *pass-of-data-folder-shared-between-servers*)

[Cause] Possible causes are as follows:

(1) You do not have permission to access the data folder shared between servers.

(2) An I/O error occurred.

[Action] Cancels setup.

[Workaround] Check the following, and then retry setup.

(1) Verify that you have permission to write to the data folder shared between servers.

(2) Verify that no disks have failed.

KDEX1591-W

A folder that cannot be used is specified for the *folder-specified-by-Setup*.

[Cause] The same folder as the installation folder was specified for the *folder-specified-by-Setup*.

[Action] Returns to the previous window and continues setup.

[Workaround] For the *folder-specified-by-Setup*, specify a folder other than the installation folder.

KDEX1592-E

An error occurred during setup processing.

[Cause] Possible causes are as follows:

(1) The IP address specified in the database connection settings window during setup is invalid.

(2) An I/O error occurred.

[Action] Cancels setup.

[Workaround] Check the following, and then retry setup.

(1) Verify that the IP address specified in the database connection settings window during setup is valid.

(2) Verify that no disks have failed.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX1593-E

Failed to connect to the database.

[Cause] Possible causes are as follows:

(1) In the database connection settings window during setup, an IP address was specified that does not exist in the segment that includes the management server.

(2) In the cluster environment settings window for the database server, the IP address specified for the logical IP address does not exist in the segment that includes the management server.

(3) The database is not running.

[Action] Cancels setup.

[Workaround] Check the following, and then retry setup.

(1) Verify that the IP address specified in the database connection settings window during setup exists in the segment that includes the management server.

(2) Verify that the logical IP address specified in the cluster environment settings window for the database server is an IP address that exists in the management server segment.

(3) Verify that the database server service (*service-of-database-server*) is running.

KDEX1594-E

Failed to create the folder for storing operation logs.

[Cause] Possible causes are as follows:

(1) You do not have permission to access the folder for storing operation logs.

(2) An I/O error occurred.

[Action] Cancels setup.

[Workaround] Check the following, and then retry setup.

(1) Verify that you have permission to access the folder for storing operation logs.

(2) Verify that no disks have failed.

KDEX1597-E

Failed to create the output folder for saving the revision history.

[Cause] Possible causes include the following:

(1) You do not have access rights for the output folder.

(2) An I/O error occurred.

[Action] Cancels setup.

[Workaround] Verify the following, and then retry setup.

(1) Verify that you have access rights for the output folder.

(2) Verify that no disk failure has occurred.

KDEX1598-E

Failed to upgrade the database.

[Cause] An error occurred in an attempt to upgrade the database. Possible causes are as follows:

(1) You do not have permission to access the database folder, the local data folder, or the database backup folder.

(2) An I/O error occurred.

(3) The management server is accessing the database.

[Action] Cancels setup.

[Workaround]

(1) Verify that you have permission to access the database folder, the local data folder, or the database backup folder.

(2) Make sure that no disk failure has occurred.

(3) Stop the following services that are being used by JP1/IT Desktop Management on the management server, and then re-execute setup:

service-name

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX2003-I

Exported device information successfully.

KDEX2004-E

Could not export device information.

KDEX2005-I

Imported asset information successfully.

KDEX2006-E

Could not import asset information.

KDEX2007-I

Exported asset information successfully.

KDEX2008-E

Could not export asset information.

KDEX3004-I

Logon succeeded. UserID=*user-ID*.

KDEX3005-E

Failed to log in. The specified User ID or Password is invalid. User ID=*user-ID*.
[Cause] The specified User ID or Password is invalid.
[Action] Cancel login.
[Workaround] Log in using a valid User ID and Password.

KDEX3006-E

Logon failed. UserID=*user-ID (or null if not obtainable)*, cause message=*cause-message*
[Cause]Database error or Expiration of Usage period.
[Response] Cancel Logon.
[Action] For expiration of usage period, purchase a license. For other reasons, collect troubleshooting information from troubleshooting collection information command and contact support service.

KDEX3007-I

Logoff successful UserID=*user-ID*

KDEX3029-E

Lock user account. UserID=*user-ID*

KDEX3030-I

Unlock user account. UserID=*user-ID*

KDEX3200-I

User is registered. User ID=*user-ID*, Permissions list=*permissions-list*

KDEX3201-I

User is deleted. User ID=*user-ID*

KDEX3202-I

User's permission is changed. User ID=*user-ID*, Permissions list=*permissions-list*

KDEX3203-I

The security policy has been updated. Policy name=*policy-name*, Policy ID=*policy-ID*, Update type=*update-type*

KDEX3204-W

The security policy could not be updated. (policy name = *policy-name*, policy ID = *policy-ID*, update type = *update-type*, cause of failure = *cause-of-failure*)

[Cause] If the cause of failure is "application error" and the update type is "update", security policy names are duplicated. If the cause of failure is "application error" and the update type is "delete", an attempt was made to delete a security policy associated with a device or group. In other cases, an error occurred in the database.

[Action] Cancels the update of the security policy.

[Workaround] If the cause of failure is "application error" and the update type is "update", specify a security policy name that does not conflict with another. If the cause of failure is "application error" and the update type is "delete", remove all associations, and then delete the security policy. In other cases, collect troubleshooting information by using the troubleshooting information collection command, and then contact customer support.

KDEX3205-I

Agent setting is updated. agent_setting_name=*agent-setting-name*, setting_ID=*setting-ID*, update_type=*update-type*

KDEX3206-W

An agent setting could not be updated. (agent setting name = *agent-setting-name*, setting ID = *setting-ID*, update type = *update-type*, cause of failure = *cause-of-failure*)

[Cause] If the cause of failure is "application error" and the update type is "update", agent setting names are duplicated. If the cause of failure is "application error" and the update type is "delete", an attempt was made to delete an agent setting associated with a device or group. In other cases, an error occurred in the database.

[Action] Cancels the update of the agent setting.

[Workaround] If the cause of failure is "application error" and the update type is "update", specify an agent setting name that does not conflict with another. If the cause of failure is "application error" and the update type is "delete", remove all associations, and then delete the agent setting. In other cases, collect troubleshooting information by using the troubleshooting information collection command, and then contact customer support.

KDEX3238-I

Successful license file registration.

KDEX3239-W

Error in license file registration.

KDEX3240-I

Updated login credentials or proxy login credentials in support service site setting. userId=*user-ID*, proxyUserId=*proxy-user-ID*, proxyIPAddress=*proxy-IP-address*, proxyPortno=*proxy-port-number*

KDEX3241-W

Login credentials or proxy login credentials in support service site setting failed. userId=*user-ID*, proxyUserId=*proxy-user-ID*, proxyIPAddress=*proxy-IP-address*, proxyPortno=*proxy-port-number*

KDEX3242-I

Updated login credentials in discovery settings. credentialName=*credential-name*, credentialKind=*credential-kind*, userName or communityName =*user-name or community-name*

KDEX3243-W

Login credentials update in discovery setting failed. credentialName=*credential-name*, credentialKind=*credential-kind*, userName or communityName =*user-name or community-name*

KDEX3244-I

Updated login credentails for AMT settings. userId=*user-ID*

KDEX3245-W

Login credential update for AMT setting failed. userId=*user-ID*

KDEX3246-I

Updated login credentials for AD setting. userId=*user-ID*, hostname=*host-name*, portno=*port-number*, domainName=*domain-name*

KDEX3247-W

Login credential update for AD setting failed. userId=*user-ID*, hostname=*host-name*, portno=*port-number*, domainName=*domain-name*

KDEX3248-I

Updated login credentials for mail server connection settings. userId=*user-ID*, hostname=*host-name*, portno=*port-number*

KDEX3249-W

Login credential update for mail server connection setting failed. userId=*user-ID*, hostname=*host-name*, portno=*port-number*

KDEX3252-I

The mandatory software will be distributed based on the security policy settings. You can check the task progress status on the distribution screen. Task name=*task-name*

KDEX3253-I

The unauthorized software will be uninstalled based on the security policy settings. You can check the task progress status on the distribution screen. Task name=*task-name*

KDEX3254-I

Task started on schedule *execution-start-time*. Task name=*task-name*

KDEX3255-I

This on demand task has been executed some time ago. It is deleted now. Task name=*task-name*

KDEX3265-I

The credential ID or Password in the discovery setting was deleted. discoveryCredentialInformationID=*discovery-credential-information-ID*, discoveryCredentialInformationName=*discovery-credential-information-name*

KDEX3266-I

The administrator permissions password for the AMT settings was updated.

KDEX3267-W

An attempt to update the administrator permissions password for the AMT settings failed.

KDEX3299-I

An MDM setting was added. (setting ID = *setting-ID*, MDM setting name = *MDM-setting-name*)

KDEX3300-E

Failed to add an MDM setting. (setting ID = *setting-ID*, MDM setting name = *MDM-setting-name*)

KDEX3301-I

The user ID or password of an MDM server or proxy server was updated. (setting ID = *setting-ID*, MDM setting name = *MDM-setting-name*)

KDEX3302-E

Failed to update the user ID or password of an MDM server or proxy server. (setting ID = *setting-ID*, MDM setting name = *MDM-setting-name*)

KDEX3303-I

An MDM setting was deleted. (setting ID = *setting-ID*, MDM setting name = *MDM-setting-name*)

KDEX3304-E

Failed to delete an MDM setting. (setting ID = *setting-ID*, MDM setting name = *MDM-setting-name*)

KDEX3319-I

The auto update settings of the network filter list were changed.

KDEX3320-E

Failed to change the auto update settings of the network filter list.

KDEX3321-I

Changed the JP1/NETM/NM - Manager linkage settings.

KDEX3322-E

Failed to change the JP1/NETM/NM - Manager linkage settings.

KDEX4000-E

Failed to execute the command. The specified arguments are invalid. Command name=*command-name*.
[Cause] The specified arguments are invalid.
[Action] Cancel command execution.
[Workaround] Confirm the command arguments, and retry execution.

KDEX4001-E

Failed to execute the command. You do not have the required permissions. Command name=*command-name*.
[Cause] The command was executed by a user without Administrator privileges.
[Action] Cancel command execution.
[Workaround] Retry executing the command as a user with Administrator privileges.

KDEX4002-E

Failed to execute the command. An executing process (Setup, Database Manager, or a command) might be running. Command name=*command-name*
[Cause] The command was executed when either Setup, Database Manager, or a command was running.
[Action] Cancel command execution.
[Workaround] Wait until the executing process (Setup, Database Manager, or a command) ends, and then retry command execution.

KDEX4003-E

Failed to execute the command. Setup has not completed. Command name=*command-name*

[Cause] The JP1/IT Desktop Management - Manager Setup has not completed.

[Action] Cancel command execution.

[Workaround] Retry executing the command, after JP1/IT Desktop Management - Manager Setup.

KDEX4009-E

Failed to execute the command. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] A critical error has occurred while executing the command.

[Action] Cancel command execution.

[Workaround] Use the troubleshooting information collection command to collect troubleshooting information and contact support service.

KDEX4010-E

Failed to execute the command. Cannot execute in a cluster environment. Command name=*command-name*.

[Cause] The start / stop command was executed in a cluster environment.

[Action] Cancel command execution.

[Workaround] Use the cluster software utility to start/stop JP1/IT Desktop Management - Manager.

KDEX4011-I

JP1/IT Desktop Management - Manager is stopped. Command name=*command-name*.

KDEX4012-I

JP1/IT Desktop Management - Manager is forced to stop. Command name=*command-name*.

KDEX4013-E

Failed to execute the command. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4014-W

JP1/IT Desktop Management - Manager is stopped. Command name=*command-name*.

[Cause] Executed stop command (when JP1/IT Desktop Management - Manager was stopped).

[Action] Cancel stop command execution.

[Workaround] None.

KDEX4015-I

JP1/IT Desktop Management - Manager is started. Command name=*command-name*.

KDEX4016-E

Failed to execute the command. Command name=*command-name*, Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4017-W

JP1/IT Desktop Management - Manager is started. Command name=*command-name*.

[Cause] Executed the start command (when JP1/IT Desktop Management - Manager was launched).

[Action] Cancel command execution.

[Workaround] None.

KDEX4020-E

Command execution failed. JP1/IT Desktop Management - Manager is not stopped. (command name = *command-name*)

[Cause] The command was executed without stopping JP1/IT Desktop Management - Manager on the management server or database server.

[Action] Cancels command execution.

[Workaround] Stop JP1/IT Desktop Management - Manager, and then re-execute the command.

KDEX4021-E

Failed to execute the command. Could not stop JP1/IT Desktop Management - Manager. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use the troubleshooting information collection command to collect troubleshooting information and contact support service.

KDEX4022-W

Database reorganization successful. But, an error occurred while starting JP1/IT Desktop Management - Manager. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4023-E

Command execution failed. The -s option cannot be specified. (command name = *command-name*)

[Cause] Possible causes include the following:

(1) The -s option was specified in a cluster environment.

(2) The -s option was specified in an environment with a multi-server configuration.

[Action] Cancels command execution.

[Workaround]

(1) Stop JP1/IT Desktop Management - Manager by using the cluster software functionality. Then, re-execute the command without specifying the -s option.

(2) Stop JP1/IT Desktop Management - Manager on the management server and database server by using the stopservice command. Then, re-execute the command without specifying the -s option.

KDEX4024-I

The database reorganization was successful. Command name=*command-name*.

KDEX4025-E

Failed to execute the command. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] Critical error occurred during commanf execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4026-E

Failed to execute the command. The backup folder is invalid or does not exist. Command name=*command-name*.

[Cause] The specified backup folder is invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Check if the specified folder exists and is accessible. Then, retry command execution.

KDEX4027-E

Failed to execute the command. A backup folder with an identical timestamp already exists. Command name=*command-name*.

[Cause] The command could not create the backup folder since a folder with the same name (a string indicating the date and time) already exists.

[Action] Cancel command execution.

[Workaround] retry command execution.

KDEX4028-I

The database backup was successful. Command name=*command-name*, Backup folder=*backup-folder*.

KDEX4029-E

Failed to execute the command. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4030-E

Failed to execute the command. The data folder is either invalid or does not exist. Command name=*command-name*.

[Cause] The specified data folder is either invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Check if the specified folder exists and is accessible. Then, try executing the command.

KDEX4031-I

The database restoration was successful. Command name=*command-name*, Data folder=*data-folder*.

KDEX4032-E

Failed to execute the command. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4033-E

Failed to execute the command. Insufficient disk space for the backup folder. Command name=*command-name*.

[Cause] Insufficient disk space for the backup folder.

[Action] Cancel command execution.

[Workaround] Free the disk space, and then try executing the command.

KDEX4034-E

Failed to execute the command. Insufficient disk space for the temporary folder. Command name=*command-name*.

[Cause] Insufficient disk space for the temporary folder.

[Action] Cancel command execution.

[Workaround] Free the disk space, and then try executing the command.

KDEX4035-E

Failed to execute the command. The temporary folder is either invalid or does not exist. Command name=*command-name*.

[Cause] The specified temporary folder is either invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Check if the temporary folder exists and is accessible. Then, try executing the command.

KDEX4036-E

Failed to execute the command. Could not start the database. Command name =*command-name* .

[Cause] Insufficient disk space to start the database.

[Action] Cancel command execution.

[Workaround] Free the space on the disk where you have the installation folder, and retry command execution. If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4037-E

The database reorganization failed. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

KDEX4038-E

The database backup failed. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

KDEX4039-E

The database restoration failed. Command name=*command-name*, Error code=*error-code (maintenance-code)*.

KDEX4040-I

Collected the troubleshooting information.

KDEX4041-E

Could not collect troubleshooting information.

[Cause] Insufficient disk space for the troubleshooting information folder.

[Action] Cancel command execution.

[Workaround] Free the disk space, and retry command execution. If the problem persists, contact Customer Support.

KDEX4042-I

Canceled the troubleshooting information collection.

KDEX4043-W

Could not collect some troubleshooting information.

[Cause] Failed to collect some of the troubleshooting information.

[Action] Cancel command execution.

[Workaround] Retain the partially collected troubleshooting information file, and retry command execution. If the problem persists, contact Customer Support with the retained troubleshooting information.

KDEX4044-E

The troubleshooting information folder is either invalid or does not exist.

[Cause] The specified troubleshooting information folder is either invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Check if the specified folder exists and is accessible. Then, retry command execution.

KDEX4050-E

Failed to execute the command. Could not use the default backup folder. Command name=*command-name*

[Cause] The installation folder name contains characters that cannot be used in the backup folder name.

[Action] Cancel command execution.

[Workaround] Retry executing the command with option -b.

KDEX4051-E

Failed to execute the command. Could not use the default data folder and temporary folder. Command name=*command-name*.

[Cause] The installation folder name contains characters that cannot be used in the data folder name and temporary folder name.

[Action] Cancel command execution.

[Workaround] Retry executing the command with option -b and option -w.

KDEX4052-E

Failed to execute the command. Could not use the default temporary folder. Command name=*command-name*.

[Cause] The installation folder name contains invalid characters that cannot be used as temporary folder name.

[Action] Cancel command execution.

[Workaround] Retry executing the command with option -w.

KDEX4053-W

The database backup was successful. But, an error occurred while starting JP1/IT Desktop Management - Manager. Command name=*command-name*, Error code=*error-code (maintenance-code)*, Backup folder=*backup-folder*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Start JP1/IT Desktop Management - Manager using the start command. If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4054-W

The database restoration was successful. But, an error occurred while starting JP1/IT Desktop Management - Manager. Command name=*command-name*, Error code=*error-code (maintenance-code)*, Data folder=*data-folder*.

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4055-E

Failed to execute the command. Command name=*command-name*, Data folder=*data-folder*.

[Cause] The specified data folder does not contain backup files.

[Action] Cancel command execution.

[Workaround] Confirm that the specified folder is correct. Then, retry command execution.

KDEX4056-E

Failed to execute the command. The temporary folder is either invalid or does not exist. Command name=*command-name*.

[Cause] The specified temporary folder is either invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Check if the specified folder exists and is accessible. Then, retry command execution.

KDEX4057-E

Failed to execute the command. Insufficient disk space for the temporary folder. Command name=*command-name*.

[Cause] Insufficient disk space for the temporary folder.

[Action] Cancel command execution.

[Workaround] Free the disk space, and retry command execution.

KDEX4058-E

Failed to execute the command. The old version couldn't be backed up. Command name=*command-name*, Backup folder=*backup-folder*.

[Cause] The specified backup was obtained from a version older than the current version.

[Action] Cancel command execution.

[Workaround] Backup the current version and retry command execution.

KDEX4061-E

Failed to execute the command. Could not establish connection to access operation logs for backup destination folder. Command name=*command-name*

[Cause] The backup destination folder does not exist. Or could not establish connection to the backup destination folder.

[Action] Cancel command execution.

[Workaround] Check if the backup destination folder (specified for operation logs during the Setup) exists, and then reestablish the connection.

KDEX4062-E

Failed to execute the command. Could not establish connection to access operation logs for backup destination folder. Command name=*command-name*

[Cause] The User name or Password authentication for the backup destination folder has failed.

[Action] Cancel command execution.

[Workaround] Check the Username or Password that was specified during the Setup.

KDEX4063-E

Failed to execute the command. Command name=*command-name*

[Cause] Insufficient backup space for the local data folder or the operation logs.

[Action] Cancel command execution.

[Workaround] Change the backup destination for the local data folder or the operation logs. Or, free hard disk space.

KDEX4064-E

Failed to execute the command. The operation logs backup has failed. Command name=*command-name*

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4065-E

Failed to execute the command. Could not start JP1/IT Desktop Management - Manager. Command name =*command-name*

[Cause] The possible reasons are given below:

(1) The license is not registered.

(2) The license has expired.

(3) The Windows Management Instrumentation Service is not started normally.

(4) The license information is invalid.

[Action] Cancel command execution.

[Workaround]

(1) Register a valid license.

(2) Purchase a valid license.

(3) Confirm The Windows Management Instrumentation Service is started normally.

(4) Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4070-E

Failed to execute the command. Command name=*command-name*.

[Cause] The specified support information file is either invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Check if the specified file exists and is correct. Then, retry command execution.

KDEX4071-E

Failed to execute the command. Command name=*command-name*.

[Cause] Executed the command without starting JP1/IT Desktop Management - Manager.

[Action] Cancel command execution.

[Workaround] Start JP1/IT Desktop Management - Manager, then retry command execution.

KDEX4072-E

Failed to execute the command. Failed to update all or part of information for JP1/IT Desktop Management - Manager. Command name=*command-name*, Not updated information=*information-that-could-not-be-updated (Windows updates, antivirus software, definition files for Manager behavior, Agent)*

[Cause] The possible reasons are given below:

(1) An update for another function is running.

(2) Insufficient space in the installation folder or the database folder.

(3) Improper access privileges to the installation folder or the database folder.

(4) An I/O error has occurred.

[Action] Cancel command execution.

[Workaround]

(1) Retry command execution after a while.

(2) Free the disk space.

(3) Confirm the access rights.

(4) Confirm that a disk failure has not occurred.

KDEX4073-I

Updated JP1/IT Desktop Management - Manager.

Command name=*command-name*

KDEX4074-E

Command execution failed. The data folder shared between servers cannot be accessed. (command name = *command-name*)

[Cause] Possible causes include the following:

(1) The database server is stopped.

(2) A network failure occurred.

[Action] Cancels command execution.

[Workaround]

(1) Start the database server, and then re-execute the command.

(2) Resolve the cause of the network failure, and then re-execute the command.

KDEX4075-E

Command execution failed. The data folder shared between servers cannot be accessed. (command name = *command-name*)

[Cause] The user name or password for connecting to the data folder shared between servers is incorrect.

[Action] Cancels command execution.

[Workaround] Verify that the user name and password for connecting to the data folder shared between servers are correct. (This user name and password were specified during management server setup.) Then, re-execute the command.

KDEX4076-E

Command execution failed. This command cannot be executed on the management server. (command name = *command-name*)

[Cause] An attempt was made to execute a command that cannot be executed on the management server.

[Action] Cancels command execution.

[Workaround] Execute the command on the database server.

KDEX4080-E

Failed to execute the command. The file path is invalid. Command name=*command-name*, Subcommand name=*subcommand-name*, File path=*file-path*.

[Cause] The possible reasons are:

(1) The folder in the specified path does not exist, or the specified file path is incorrect.

(2) The specified path exceeds the maximum path length.

(3) You do not have file access permission for the specified file.

(4) Insufficient disk space for the specified file.

(5) An I/O error occurred.

[Action] Cancel command execution.

[Workaround]

(1) Make sure the folder in the specified path exists and the specified path is correct.

(2) Check the path length.

(3) Make sure you have file access permission.

(4) Free the disk space for the specified file or specify another file which has sufficient space.

(5) Confirm that a disk failure has not occurred.

After these are confirmed, retry command execution.

KDEX4081-E

Failed to execute the command. The patch group is invalid. Command name=*command-name*, Subcommand name=*subcommand-name*, Update group name=*update-group-name*.

[Cause] The specified update group is does not exist.

[Action] Cancel command execution.

[Workaround] Make sure the specified update group exists and retry command execution.

KDEX4082-E

Failed to execute the command. The filter cannot be used. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The specified filter is invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Make sure the specified filter exists and the type of the filter is correct. Then, retry command execution.

KDEX4083-E

Failed to execute the command. Database access error occurred. Detailed information=*detailed-information*, Command name =*command-name*, Subcommand name=*subcommand-name*.

[Cause] JP1/IT Desktop Management - Manager stopped or the displayed error occurred.

[Action] Cancel command execution.

[Workaround] Start JP1/IT Desktop Management - Manager or resolve the displayed error and retry command execution. If the problem persists, execute troubleshooting information collection command to collect troubleshooting information and contact customer support.

KDEX4084-E

Failed to execute the command. Cannot export. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The possible reasons are:

(1) Insufficient disk space for the export folder.

(2) You do not have file access permission for the specified export file.

(3) An I/O error occurred.

[Action] Cancel command execution.

[Workaround]

(1) Free the disk space for the export folder or specify another file which has sufficient space.

(2) Make sure you have file access permission for the specified export file.

(3) Confirm that a disk failure has not occurred.

After these are confirmed, retry command execution.

KDEX4085-I

expanded-inventory-name export successful. Command name=*command-name*, Subcommand name=*subcommand-name*.

KDEX4086-E

Failed to execute the command. Command name=*command-name*, Subcommand name=*subcommand-name*, Error code=*error-code (maintenance-code)*.

[Cause] Insufficient memory for the command execution environment. Or a critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Make sure there is sufficient memory for the command execution environment, and retry command execution. If the problem persists, use the troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4087-I

Export or Import is canceled. Command name=*command-name*, Subcommand name=*subcommand-name*.

KDEX4088-E

Failed to execute the command. Cannot use the template. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The specified template is invalid or does not exist.

[Action] Cancel command execution.

[Workaround] Make sure the specified template exists and the type of the template is correct. Then, retry command execution.

KDEX4089-E

Failed to execute the command. Cannot import the specified file. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] Invalid file format.

[Action] Cancel command execution.

[Workaround] Make sure the specified import file is correct and retry command execution.

KDEX4090-E

Failed to execute the command. Cannot import the specified file. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The template and specified import file do not match.

[Action] Cancel command execution.

[Workaround] Make sure the specified import file is correct and retry command execution.

KDEX4091-I

Successfully imported the asset. Type of asset=*asset-type*, add=*number-of-information-items*, update=*number-of-information-items*, error=*number-of-information-items*.

KDEX4092-I

expanded-inventory-name import successful. Command name=*command-name*, Subcommand name=*subcommand-name*.

KDEX4093-E

Failed to execute the command. The specified template name is invalid. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause]The specified template name has an invalid character.

[Action] Cancel command execution.

[Workaround] Make sure the specified template name is correct and retry command execution.

KDEX4094-E

Failed to execute the command. Cannot use the Security Policy. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The specified security policy does not exist.

[Action] Cancel command execution.

[Workaround] Make sure the specified security policy exists and retry command execution.

KDEX4095-E

Failed to execute the command. The specified security policy name is invalid. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The specified security policy name has an invalid character.

[Action] Cancel command execution.

[Workaround] Make sure the specified security policy name is correct and retry command execution.

KDEX4096-E

Failed to execute the command. The specified filter name is invalid. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The filter name length is invalid or the filter name has an invalid character.

[Action] Cancel command execution.

[Workaround] Make sure the specified filter name is correct and retry command execution.

KDEX4097-E

Failed to execute the command. The specified update group name is invalid. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The specified update group name has an invalid character.

[Action] Cancel command execution.

[Workaround] Make sure the specified update group name is correct and retry command execution.

KDEX4098-E

Failed to execute the command. Cannot import the specified file. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The additional custom fields in the import file doesn't exist.

[Action] Cancel command execution.

[Workaround] Make sure you specify the additional custom fields and retry command execution.

KDEX4099-W

Failed to execute the command. Cannot distribute Update information to the update group. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] The update information does not exist.

[Action] Cancel command execution.

[Workaround] Make sure the Update information is updated from Product update. Then, retry command execution.

KDEX4100-E

The export of *expanded-inventory-name* failed. Command name=*command-name*, Subcommand name=*subcommand-name*.

KDEX4101-E

The import of *expanded-inventory-name* failed. Command name=*command-name*, Subcommand name=*subcommand-name*.

KDEX4102-E

Failed to execute the command. Cannot export the specified security policy. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] This security policy is part of mandatory (auto-enforce) software installation package.

[Action] Cancel command execution.

[Workaround]Delete this security policy from auto-enforce settings and retry executing the command.

KDEX4103-E

Failed to execute the command. Cannot export the specified filter. Command name=*command-name*, Subcommand name=*subcommand-name*.

[Cause] Following might be the possible causes:

(1) The specified user definition already exists in the filter.

(2) The specified location or department already exists in the filter.

[Action] Cancel command execution.

[Workaround]

(1) Make sure this user definition already exists in the filter, delete this definition and retry command execution.

(2) Make sure this department or location already exists in the filter and delete the specified location or department and retry executing the command.

KDEX4104-E

Failed to execute the command. JP1/IT Desktop Management - Manager cannot be started or stopped. Command name =*command-name*

[Cause] A command was executed during processing to start or stop JP1/IT Desktop Management - Manager.

[Action] Cancel command execution.

[Workaround] Retry command execution after a while.

KDEX4105-E

Failed to execute the command. Could not stop JP1/IT Desktop Management - Manager. Command name =*command-name*

[Cause] A command was executed during processing to start JP1/IT Desktop Management - Manager.

[Action] Cancel command execution.

[Workaround] Retry command execution after a while.

KDEX4106-E

Failed to execute the command. Could not start the database. Command name =*command-name*

[Cause] A command was executed during processing to stop the database.

[Action] Cancel command execution.

[Workaround] Retry command execution after a while.

KDEX4126-W

Custom fields was imported normally, but some services have not started. (command name = *command-name*, subcommand name = *subcommand-name*)

[Cause] Some services have not started.

[Action] Ends the command normally.

[Workaround] Check whether all services have started. If they have not, start the services.

KDEX4200-E

Setup is not complete.

[Cause] Since the setup is not complete, could not start the database manager.

[Action] Cancel launching the Database Manager.

[Workaround] Retry starting the Database Manager after Setup ends.

KDEX4202-E

Database Manager can be started only from the database server.

[Cause] An attempt was made to start Database Manager on a server other than the database server.

[Action] Cancels startup of Database Manager.

[Workaround] Start Database Manager from the database server.

KDEX4203-E

Could not start Database Manager.

[Cause] Could not start the Database Manager due to an unknown error.

[Action] Cancel launching the Database Manager.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4204-E

Please start (JP1_ITDM_DB Service).

[Cause] The (JP1_ITDM_DB Service) was stopped, so could not start the Database Manager.

[Action] Cancel launching the Database Manager.

[Workaround] Retry launching the Database Manager after starting (JP1_ITDM_DB Service).

KDEX4205-E

The user does not have Administrator privileges.

[Cause] The user does not have Administrator privileges.

[Action] Cancel launching the Database Manager.

[Workaround] Retry launching the Database Manager as a user with Administrator privileges.

KDEX4206-E

Could not start the Database Manager because either Setup or a command is running.

[Cause] Started the Database Manager while either Setup or a command was executing.

[Action] Cancel launching Database Manager.

[Workaround] Wait until the executing process (Setup or command) ends, and then retry launching the Database Manager.

KDEX4207-E

The Database Manager has already started.

[Cause] The Database Manager was already started.

[Action] Cancel launching the Database Manager.

[Workaround] Continue operation with the Database Manager started already.

KDEX4208-E

An error occurred in the Database Manager.

[Cause] An error occurred in the Database Manager.

[Action] Cancel the execution of Database Manager.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4210-Q

To continue operation, JP1/IT Desktop Management - Manager service must be stopped. Would you like to stop the service?

The service will automatically start when the process ends.

KDEX4212-E

Database is in maintenance, so cannot continue the process.

[Cause] Could not continue the process since the database is in maintenance.

[Action] Cancel the execution of Database Manager.

[Workaround] Retry execution after database maintenance ends.

KDEX4213-E

Cannot use the folder path specified for *folder-specified-by-Database-Manager*.

A file with a same name as the specified folder already exists in the given path.

[Cause] A file with the same name as the specified folder already exists in the given path.

[Action] Cancel the execution.

[Workaround] To resume execution, either change or delete the duplicate filename, or specify an alternate folder path.

KDEX4214-E

Failed to acquire server ID authentication. Authentication server ID file is invalid.

[Cause] Invalid file for server ID authentication.

[Action] Cancel Database Manager execution.

[Workaround] Make sure the authentication server ID file is valid and restart Database Manager.

KDEX4215-Q

From the management server, stop the service given below. If you continue while this service is running, processing might not finish properly.

(service = *service-name-of-management-server*)

The database server service will stop automatically. The database server service that is stopped in this way will start automatically after processing is complete.

Are you sure you want to stop the database server service?

KDEX4216-Q

From the management server, stop the service given below. If you continue while this service is running, processing might not finish properly.

(service = *service-name-of-management-server*)

Take offline the cluster resources associated with the service given below. After doing so, click **OK** to continue processing. After processing is complete, bring the cluster resources back online.

(service = *service-name-of-database-server*)

KDEX4220-E

Failed to start the database.

[Cause] Failed to start the database. Possible causes are as follows:

(1) The disk containing the installation folder does not have enough free space to start the database (required space = *required-space* MB).

(2) The service (JP1_ITDM_DB Service) has stopped.

[Action] Cancels database startup.

[Workaround]

(1) Free up more space on the disk containing the installation folder, and then restart the service (JP1_ITDM_DB Service).

(2) Start the service (JP1_ITDM_DB Service).

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX4221-E

A database failure occurred.

[Cause] A database failure occurred because there was not enough hard disk space for a database extension.

[Action] Cancels database extension.

[Workaround] Use Setup to re-create the database. If a backup of the database exists, after re-creating the database, restore the backup by using Database Manager.

KDEX4230-E

Could not start the service. Service name=*service-name*.

[Cause] An error occurred while starting the service.

[Action] Cancel the service.

[Workaround] Check the message logs and take action based on the errors in the logs.

KDEX4231-E

Could not stop the service. Service name=*service-name*.

[Cause] An error occurred while stopping the service.

[Action] Cancel the service.

[Workaround] Check the message logs and take action based on the errors in the logs.

KDEX4232-E

An attempt to stop the service failed.

[Cause] Processing was executed during processing to start or stop the service used by JP1/IT Desktop Management - Manager.

[Action] Cancel the execution of Database Manager.

[Workaround] Wait a while, and then retry the operation.

KDEX4233-E

Database backup, restoration, or reorganization processing failed.

[Cause] The database is being accessed from the management server.

[Action] Cancels database backup, restoration, or reorganization processing.

[Workaround] From the management server, stop the service given below, and then retry the database backup, restoration, or reorganization.

(service = *service-name-of-management-server*)

KDEX4270-I

The database is backed up.

KDEX4271-E

An error occurred while backing up the database. Backup has been canceled.

[Cause] Backup failed due to the following possible reasons:

(1) Improper access privileges for the backup folder or data folder.

(2) An I/O error occurred.

[Action] Cancel backup.

[Workaround]

(1) Confirm the access rights of the backup folder and data folder.

(2) Confirm that a disk failure has not occurred.

If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4272-E

The backup folder is not specified.

[Cause] The backup folder is not specified.

[Action] Cancel backup.

[Workaround] Specify a backup folder, and then retry backup .

KDEX4273-E

The backup folder path contains invalid characters. Valid characters are alphanumeric, #, @, \, period(.), space, and round brackets ().

[Cause] The backup folder path contains invalid characters.

[Action] Cancel backup.

[Workaround] Specify a valid backup folder path, and then retry backup.

KDEX4275-Q

The specified backup folder already exists.

To overwrite the existing backup folder, click OK.

KDEX4276-E

Backup failed.

[Cause] The backup folder is either on a non-local disk or the path is invalid.

[Action] Cancel backup.

[Workaround] Specify a backup folder on a local disk, and then retry backup.

KDEX4277-E

An error occurred during database backup. Canceled backup. The disk space may be insufficient for the backup folder.

[Cause] Insufficient disk space for the backup folder.

[Action] Cancel backup.

[Workaround] Free the disk space or specify another backup folder, and then retry backup.

KDEX4278-E

The backup folder path should not exceed *number-of-bytes* bytes.

[Cause] The backup folder path exceeds the maximum path length.

[Action] Cancel backup.

[Workaround] Check the path length, and then retry backup.

KDEX4280-I

Restored the database.

KDEX4281-E

An error occurred while restoring the database. Restoration is canceled.

[Cause] Restore failed due to the following possible reasons:

(1) Improper access privileges for the temporary or the data folder.

(2) An I/O error occurred.

[Action] Cancel restoration.

[Workaround]

(1) Confirm the access rights of the temporary and data folders.

(2) Confirm that a disk failure has not occurred.

If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4282-E

The data folder (*folder-path-specified-by-user*) does not exist. Please check the data folder.

[Cause] The data folder does not exist.

[Action] Cancel restoration.

[Workaround] Specify a valid data folder, and then retry restoration.

KDEX4283-E

The data folder is not specified.

[Cause] The data folder was not specified.

[Action] Cancel restoration.

[Workaround] Specify a data folder, and then retry restoration.

KDEX4284-E

The data folder path contains invalid characters. Valid characters are alphanumeric, #, @, \, period(.), space, and round brackets ().

[Cause] The data folder path contains invalid characters.

[Action] Cancel restoration.

[Workaround] Specify a valid data folder path, and then retry restoration.

KDEX4285-E

The data folder does not contain the required files for restoration.

[Cause] The data folder does not contain the required files.

[Action] Cancel restoration.

[Workaround] Specify a valid data folder, and then retry restoration.

KDEX4286-E

An error occurred while restoring the database. Restoration is canceled. The disk space may be insufficient for the temporary folder.

[Cause] Insufficient disk space for the temporary folder.

[Action] Cancel restoration.

[Workaround] Free the disk space or specify another temporary folder, and then retry restoration.

KDEX4287-E

Failed to restore the backup of an older version. Folder=*specified-folder-path*

[Cause] An older version was backed up than the current version.

[Action] Cancel restoration.

[Workaround] Backup the current version.

KDEX4288-E

Restoration failed.

[Cause] The data folder is either on a non-local disk or the path is invalid.

[Action] Cancel restoration.

[Workaround] Specify a data folder on a local disk, and then retry restoration.

KDEX4289-E

The data folder path should not exceed *number-of-bytes* bytes.

[Cause] The data folder path exceeds the maximum path length.

[Action] Cancel restoration.

[Workaround] Check the path length of the data folder, and retry restoration.

KDEX4290-I

Reorganized the database.

KDEX4291-E

An error occurred while reorganizing the database. Reorganization has been canceled.

[Cause] Reorganization failed due to the following possible reasons:

(1) Insufficient privileges to access the temporary folder.

(2) An I/O error occurred.

[Action] Cancel reorganization.

[Workaround]

(1) Confirm the access rights of the temporary folder.

(2) Confirm that a disk failure has not occurred.

If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4292-E

The reorganization parameters are not specified.

[Cause] The reorganization parameters were not specified.

[Action] Cancel reorganization.

[Workaround] Retry executing reorganization by specifying the parameters.

KDEX4293-E

A temporary folder is not specified.

[Cause] A temporary folder was not specified.

[Action] Cancel reorganization.

[Workaround] Specify a temporary folder, and then retry reorganization.

KDEX4294-E

The temporary folder path contains invalid characters. Valid characters are alphanumeric, #, @, \, period(.), space, and round brackets ().

[Cause] The temporary folder path contains invalid characters.

[Action] Cancel reorganization.

[Workaround] Specify a valid temporary folder path, and then retry reorganization.

KDEX4295-E

Reorganization failed.

[Cause] The temporary folder is either on a non-local disk or the path is invalid.

[Action] Cancel reorganization.

[Workaround] Specify a temporary folder on a local disk, and then retry reorganization.

KDEX4296-E

An error occurred while reorganizing the database. Reorganization has being canceled. The disk space may be insufficient for the temporary folder.

[Cause] Insufficient disk space for the temporary folder.

[Action] Cancel reorganization.

[Workaround] Free the disk space or specify another temporary folder, and then retry reorganization.

KDEX4297-E

You cannot specify a temporary folder path exceeding *number-of-bytes* bytes.
[Cause] The temporary folder path exceeds the maximum path length.
[Action] Cancel reorganization.
[Workaround] Check the path length of the temporary folder, and retry reorganization.

KDEX4300-E

A temporary folder is not specified.
[Cause] A temporary folder was not specified.
[Action] Cancel restoration.
[Workaround] Specify a temporary folder, and then retry restoration.

KDEX4301-E

The temporary folder path contains invalid characters. Valid characters are alphanumeric, #, @, \, period(.), space, and round brackets ().
[Cause] The temporary folder path contains invalid characters.
[Action] Cancel restoration.
[Workaround] Specify a valid temporary folder path, and then retry restoration.

KDEX4302-E

You cannot specify a temporary folder path exceeding *number-of-bytes* bytes.
[Cause] The temporary folder path exceeds the maximum path length.
[Action] Cancel restoration.
[Workaround] Check the path length of the temporary folder, and retry restoration.

KDEX4303-E

Restoration failed.
[Cause] The temporary folder is either on a non-local disk or the path is invalid.
[Action] Cancel restoration.
[Workaround] Specify a temporary folder on a local disk, and then retry restoration.

KDEX4354-I

The database backup was successful.

KDEX4355-E

The database backup failed.

KDEX4356-I

The database restoration was successful.

KDEX4357-E

The database restoration failed.

KDEX4358-I

The database reorganization was successful.

KDEX4359-E

The database reorganization failed.

KDEX4360-E

Backup for data other than operations logs successful. But, operation logs backup failed. So the backup process will stop now.

[Cause] An internal error occurred.

[Action] Cancel backup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4361-E

Backup for data other than operations logs successful. But, operation logs backup failed. So the backup process will stop now.

[Cause] Insufficient space for *local-data-folder or operation-log-storage-area* for data backup.

[Action] Cancel operation logs backup.

[Workaround] Change *operation-log-storage-area* or free the disk space.

KDEX4362-E

Backup for data other than operations logs successful. But, operation logs backup failed. Could not establish the connection to the operation log backup folder. So the backup process will stop now.

[Cause] Either the operation log backup folder does not exist, Or could not establish the connection to the network drive.

[Action] Cancel operation logs backup.

[Workaround] Check if the operation log backup folder (specified for operation logs during the Setup) exists, and then reestablish the connection.

KDEX4363-E

Backup for data other than operations logs successful. But, operation logs backup failed. Could not establish the connection to the operation log backup folder. So the backup process will stop now.

[Cause] The Username or Password authentication used for accessing the operation log backup folder has failed.

[Action] Cancel operation logs backup.

[Workaround] Check the Username or Password that was specified during Setup.

KDEX4364-E

Failed to restore the database. Restoration will be stopped. Insufficient disk space.

[Cause] Insufficient hard disk space for *local-data-folder*.

[Action] Restoration will be stopped.

[Workaround] Change *local-data-folder*, or increase hard disk space.

KDEX4365-E

Database restoration failed. Restoration will be stopped.

Could not establish the connection to the operation log backup folder.

[Cause] Either the operation log backup folder does not exist, Or, could not establish the connection to a network drive.

[Action] Cancel restoration.

[Workaround] Check that the operation log backup folder exists, and reestablish the connection.

KDEX4366-E

Database restoration failed. Restoration will be stopped.

Could not establish the connection to the operation log backup folder.

[Cause] The Username or Password authentication has failed for the operation log backup folder.

[Action] Cancel restoration.

[Workaround] Check the Username or Password specified during Setup.

KDEX4367-E

Automatic operation logs backup failed.

[Cause] An internal error occurred.

[Action] Cancel the operation logs backup.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4368-E

Automatic operation logs backup failed.

An I/O error has occurred.

[Cause] Insufficient hard disk space for *local-data-folder-oroperation-log-backup-folder*.

[Action] Cancel the operation logs backup.

[Workaround] Change *local-data-folder-oroperation-log-backup-folder*, or increase hard disk space.

KDEX4369-E

Automatic operation logs backup failed.

Could not establish the connection to the operation log backup folder.

[Cause] Either the operation log backup folder does not exist, Or, could not establish the connection to a network drive.

[Action] Cancel the operation logs backup.

[Workaround] Check that the operation log backup folder exists, and reestablish the connection.

KDEX4370-E

Operation log backup failed. Could not establish the connection to the operation log backup folder.

[Cause] The Username or Password authentication has failed for the operation log backup folder.

[Action] Cancel the operation logs backup.

[Workaround] Check the Username or Password specified during Setup.

KDEX4371-E

Restore operation logs failed.

[Cause] An internal error has occurred.

[Action] Cancel restoration.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX4372-E

Restore operation logs failed.

An I/O error has occurred.

[Cause] Insufficient hard disk space for *local-data-folder*.

[Action] Cancel restoration.

[Workaround] Change *local-data-folder*, or increase hard disk space.

KDEX4373-E

Restore operation logs failed.

Could not establish the connection to the operation log backup folder.

[Cause] Either the operation log backup folder does not exist, Or could not establish the connection to the network drive.

[Action] Cancel restoration.

[Workaround] Check that the operation log backup folder (specified during Setup) exists, and reestablish the connection.

KDEX4374-E

Restore operation logs failed. Could not establish the connection to the operation log backup folder.

[Cause] The Username or Password authentication has failed for the operation log backup folder.

[Action] Cancel restoration.

[Workaround] Check the Username or Password specified during the Setup.

KDEX4375-W

Skipped some operation logs data during restoration.

Skip time:*skip-time*

[Cause] Backup file (operation logs) for the specified day does not exists in the operation log backup folder.

[Action] Continue operation logs restoration.

[Workaround] If the backup data for the specified day has been moved to any other folder, then copy the data to the operation log backup folder. Restore the operation logs again.

KDEX4376-E

Restore operation logs failed.

[Cause] The backup files do not exists in the operation log backup folder.

[Action] Cancel restoration.

[Workaround] If the backup files has been moved to any other folder, then copy the files to the operation log backup folder. Restore the operation logs again.

KDEX4377-E

Restore operation logs failed.

[Cause] Improper backup files. In the operation log backup folder there is no catalog file(OPR_CATALOG_*YYYYMMDD*.csv), which has the same date of the backup file(OPR_DATA_*YYYYMMDD*.zip).

[Action] Cancel restoration.

[Workaround] If the backup files has been moved to any other folder, then restore the files and try restoration. Else you can remove the backup files and the improper catalog file, and then try operation logs restoration.

KDEX4378-Q

If automatic operation logs backup setting is disabled, the operations logs will not be backed up. Enable the automatic backup setting to store the logs.

Click **OK** to resume. Click **Cancel** to review.

KDEX4379-E

An error occurred while restoring the database. Restoration has been canceled.

[Cause] The backup data version is different from the current version.

[Action] Cancel restoration.

[Workaround] Specify backup data whose version is same as the current version.

KDEX4380-E

Restore operation logs failed.

[Cause] Operation log backup folder was not specified during Setup.

[Action] Cancel restoration.

[Workaround] Check if the operation log backup folder was specified during Setup.

KDEX4381-E

Failed to backup the operation logs.

Connection to the operation log backup folder could not be established.

[Cause] Anonymous access to shared folders is restricted on the management server.

[Action] Cancel the operation logs backup.

[Workaround] Create a user account in the management server with Username and Password specified during Setup.

KDEX4382-E

Restore operation logs failed.

Could not establish the connection to the operation log backup folder.

[Cause] Anonymous access to shared folders is restricted on the management server.

[Action] Cancel restoration.

[Workaround] Create a user account in the management server with Username and Password specified during Setup.

KDEX4387-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of invalid character input) include the following:

(1) The format of the import file is invalid.

(2) An ASCII control character was specified in the import file.

(3) A surrogate pair was specified in the import file.

(4) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4388-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of invalid update or deletion targets) include the following:

(1) A higher-level value that does not exist was specified for a post-change value. (For example, /A/B is specified for the post-change value, but /A does not exist.)

(2) An attempt was made in the import file to update or delete a value that did not exist before importing the file.

(3) An attempt was made in the import file to delete a value multiple times.

(4) An attempt was made in the import file to delete a value that was added in the same import file.

(5) An attempt was made in the import file to update or delete a management field that did not exist before importing the file. Alternatively, the management field for which an update or deletion attempt was made is not selectable or hierarchical data.

(6) An attempt was made in the import file to delete all values.

(7) A lower-level value that does not exist was specified for the post-change values. (For example, /A/B is specified for the pre-change values and /A/B/C is specified for the post-change values, but because /B will become /C after the change, /B is considered to be nonexistent.)

(8) The update category is D, and no value exists before changing the default language.

(9) The default selection for a management field (asset status, asset type, license status, license type, contract status, contract type) was changed.

(10) The default selection for a management field (asset status, asset type, license status, license type, contract status, contract type) was deleted.

(11) An attempt was made to update the department data applied from data collected from Active Directory.

(12) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4389-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of invalid deletion targets) include the following:

(1) An attempt was made to delete a hierarchical level that contains sublevels.

(2) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4390-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of invalid content input for an item) include the following:

(1) The contents of the import file specified for the command are invalid.

(2) The header of the import file is invalid.

(3) A value that cannot be specified in the import file is specified.

(4) The same language is specified in the multilingual settings.

(5) The number of characters that can be specified exceeded the limit.

(6) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4391-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of an invalid combination) include the following:

(1) The hierarchy settings among multiple languages do not match.

(2) The number of columns separated by commas is insufficient in the header or data of the import file.

(3) For update category U, only the explanation was changed, without changing the set value.

(4) The multilingual settings were changed for a custom item, an additional license item, or an additional contract item.

(5) The multilingual settings do not match among identical management fields.

(6) All pre-change languages were deleted.

(7) For update category A, a pre-change value has been input.

(8) An explanation has been input for a hierarchical item.

(9) For update category U, a pre-change value has been input for a newly added language.

(10) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4392-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of data duplication) include the following:

(1) Multiple lines that add the same selection exist in the import file.

(2) A selection was added that was set before the import of the file.

(3) A selection is specified that was set before the import of the file and that has the same name as a post-change selection.

(4) A line prior to the import file is adding the same selection as after the change.

(5) A line prior to the import file is changing the same selection as after the change.

(6) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4393-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] In the import file specified for the command, /unknown is specified for the root of hierarchical or selectable data.

[Action] Cancels command execution.

[Workaround] Verify that the specified import file is correct, and then retry command execution.

KDEX4394-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error

occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of required items that have not been entered) include the following:

(1) No value is set for a required item.

(2) The multilingual value is set, but no languages corresponding to the multilingual settings are specified.

(3) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Revise the specified import file, and then retry command execution.

KDEX4395-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes (of hierarchical levels exceeding the upper limit) include the following:

(1) In the hierarchical data in the import file specified for the command, the specified data exceeds 40 levels.

(2) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround] Verify that the specified import file is correct, and then retry command execution.

KDEX4396-E

Command execution failed. Processing to apply the import data failed. The data is not reflected in the database. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes include the following:

(1) While the command was being executed, settings for an asset management field were edited from the operations window.

(2) The management server is temporarily experiencing a heavy load.

(3) The character encoding of the import file does not match the character encoding specified by the -encoding option.

[Action] Cancels command execution.

[Workaround]

(1) Retry command execution, and check the input from the import file.

(2) Wait a while, and then retry command execution.

(3) Ensure that the character encoding of the import file matches the character encoding specified by the -encoding option, and then retry command execution.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX4397-E

Command execution failed. The specified file cannot be imported. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, line number at which import check error

occurred = *line-number-at-which-imported-CSV-file-error-occurred*, item at which import check error occurred = *name-of-the-item-for-which-imported-CSV-file-error-occurred*)

[Cause] Possible causes include the following:

(1) An attempt was made to update the additional management items, which have been specified for the user-specified security configuration items, by using the import file that is specified for the command.

(2) An attempt was made to update the additional management items, which have been specified for the user-defined group conditions, by using the import file that is specified for the command.

[Action] Cancels command execution.

[Workaround] Take one of the following actions to prevent user-defined information from being changed by command execution, and then execute the command again:

(1) From the user-defined security setup items, delete the additional management items to be updated by the command.

(2) From the user-defined group conditions, delete the additional management items to be updated by the command.

(3) Make sure that the specified import file is correct.

KDEX4398-W

After the common management fields and additional management fields was successfully imported, an attempt to restart the service failed. (command name = *command-name*, subcommand name = *subcommand-name*, service name = *service-name*)

[Cause] Possible causes include the following:

(1) Processing to link with the service failed.

(2) An error occurred while the service was being restarted.

[Action] Cancels stopping or starting of the service.

[Workaround] Check the public message log file, and follow the instructions in the message output by the service that failed to be restarted. If no such message has been output, try restarting the service again.

KDEX4399-I

The common management fields and additional management fields was successfully imported. On the management server, restart the service indicated in parentheses at the end of this message. (command name = *command-name*, subcommand name = *subcommand-name*, service name = *service-name*)

KDEX4400-E

Import log file output failed. The data is not reflected in the database. (log file name = *import-log-file-name*)

[Cause] Failed to write the log file.

[Action] Cancels processing.

[Workaround] Complete the following steps, and then retry command execution.

(1) Assign write permissions to the folder in which the import file is stored.

(2) Ensure that there is enough free space on the disk on which the import file is stored.

(3) Delete any log files in the folder in which the import file is stored (*import-file-name*.log).

KDEX4401-E

Command execution failed. The specified file cannot be imported. The data is not reflected in the database. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*,

management field name = *name-of-common-management-field-or-additional-management-field*, selection = *selection-set-as-a-common-management-field-or-additional-management-field*)

[Cause] Possible causes include the following:

(1) A selection that is set as an additional management field of hardware asset information was updated or deleted.

(2) A selection that is set as an additional management field of software license information was updated or deleted.

(3) A selection that is set as an additional management field of contract information was updated or deleted.

[Action] Cancels command execution.

[Workaround]

(1) From the hardware asset information, delete the selection that is set as the additional management field of hardware asset information, and then retry command execution.

(2) From the software license information, delete the selection that is set as the additional management field of software license information, and then retry command execution.

(3) From the contract information, delete the selection that is set as the additional management field of contract information, and then retry command execution.

KDEX4402-E

Command execution failed. The specified file cannot be imported. The data is not reflected in the database. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*, management field name = *name-of-common-management-field-or-additional-management-field*, selection = *selection-set-as-a-common-management-field-or-additional-management-field*, filter name = *filter-name*)

[Cause] A selection of an additional management field that is set as a filter condition was updated or deleted.

[Action] Cancels command execution.

[Workaround] Delete the additional management field that is set as a filter condition from the conditions, and then retry command execution.

KDEX4403-E

Command execution failed. Processing to apply the import data failed. The data is not reflected in the database. (command name = *command-name*, subcommand name = *subcommand-name*, import file = *import-file-name*)

[Cause] Possible causes include the following:

(1) The service (JP1_ITDM_DB Service) is stopped.

(2) A network failure occurred.

(3) The authentication information for connecting to the data folder shared between servers is incorrect.

(4) The management server is temporarily experiencing a heavy load.

[Action] Cancels command execution.

[Workaround]

(1) Start the service (JP1_ITDM_DB Service), and then retry command execution.

(2) Resolve the cause of the network failure, and then retry command execution.

(3) Verify that the user name and password for connecting to the data folder shared between servers are correct, and then retry command execution.

(4) Wait a while, and then retry command execution.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5000-I

Starting discovery from IP address range.

KDEX5001-I

IP address range discovery complete.

KDEX5002-I

Searching the range (Start IP address=*start-IP-address*, End IP address=*end-IP-address*).

KDEX5003-I

Completed the search for range (Start IP address=*start-IP-address*, End IP address=*end-IP-address*).

KDEX5004-I

Discovered a new network device and sent an e-mail to the administrator.

KDEX5005-I

Searching the node (IP address=*IP-address*, MAC address=*MAC-address*).

KDEX5006-I

Search for (IP address=*IP-address*, MAC address=*MAC-address*) is complete.

KDEX5007-W

User authentication failed during discovery for this device. IP address=*IP-address*

[Cause] Authentication information is either not set or is not valid.

[Action] Continue the process.

[Workaround] Check if you can log into the target computer as an Administrator with the Windows authentication information specified for discovery. Confirm administrative share is enabled in the target computer, and then retry discovery.

KDEX5008-W

Failed to access the administrative share. IP address=*IP-address*

[Cause] Failed to connect to the administrative share in the target computer.

[Action] Continue the process.

[Workaround] If the power is switched off in target computer, turn it on. If the firewall is enabled, confirm the port for shared files are open and retry discovery.

KDEX5009-E

Failed to access the administrative share. IP address=*IP-address*, Error code=*error-code (maintenance-code)*

[Cause] An error occurred while accessing the administrative share. The error is caused by a factor other than connection, communication, and authentication.

[Action] Continue the process.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5010-W

Failed to discover this device because it is processing another request. (IP address = *IP-address*)

[Cause] Possible causes include the following:

(1) Discovery was executed on a device that was responding to a request from another management server.

(2) Discovery was executed on a device that was responding to a request from the same management server.

[Action] Continues processing.

[Workaround]

(1) Revise the discovery range, and then retry discovery.

(2) Wait a while, and then retry discovery.

If the problem persists, restart the device, and then retry discovery.

KDEX5011-W

Failed to obtain detailed information from the administrative share. IP address=*IP-address*

[Cause] Failed to retrieve detailed information in time, from the administrative share.

[Action] Continue the process.

[Workaround] Check the status of the computer, and retry discovery.

KDEX5012-E

An error occurred while accessing the administrative share in the target computer. IP address=*IP-address*, Error code=*error-code (maintenance-code)*

[Cause] An error occurred while accessing the administrative share in the target computer.

[Action] Continue the process.

[Workaround] Check the operational status of the target computer, and retry discovery. Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5013-E

An error occurred during discovery. Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred during discovery.

[Action] Cancel the process.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5014-W

Failed to update a node due to a brief server error during discovery.

[Cause] (JP1_ITDM_Agent Control) service was either not started or was busy during discovery.

[Action] Continue the process.

[Workaround] Make sure (JP1_ITDM_Agent Control) service is running, and then retry discovery.

KDEX5015-I

Searching for the nodes discovered by Network Access Control.

KDEX5016-I

Search for nodes discovered by Network Access Control is complete.

KDEX5020-I

Collecting device data from agentless devices.

KDEX5021-I

Device data collection from agentless devices is complete.

KDEX5027-W

User authentication failed while collecting device data. IP address=*IP-address*

[Cause] Authentication information is either not set or is invalid.

[Action] Continue the process.

[Workaround] Check if you can log into the target computer as an Administrator with the Windows authentication information specified for discovery. Confirm administrative share is enabled in the target compute, and then retry discovery.

KDEX5040-I

Collecting on-demand device data from agentless devices.

KDEX5041-I

On-demand device data collection from agentless devices is complete.

KDEX5043-I

Collected on-demand device data. IP address=*IP-address*

KDEX5047-W

User authentication failed while collecting on-demand device data. IP address=*IP-address*

[Cause] Authentication information is either not set or is invalid.

[Action] Continue the process.

[Workaround] Check if you can log into the target computer as an Administrator with the Windows authentication information specified for discovery. Confirm administrative share is enabled in the target compute, and then retry discovery.

KDEX5060-I

Delivering agent.

KDEX5061-I

Agent delivery complete.

KDEX5063-I

The agent installer has been started. Access point=*access-point (host-name or IP-address)*, Model name=*model-name*, Version=*version*

KDEX5064-W

Agent delivery failed. The agent is not registered.

[Cause] The agent is not registered.

[Action] Continue the process.

[Workaround] Go to Start>Programs>[JP1_IT Desktop Management - Manager]>Tools>Component Registration to register the agent. Then, retry agent delivery.

KDEX5065-E

An error occurred during agent delivery. Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred during agent delivery.

[Action] Cancel the process.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5067-W

Agent deployment failed because user authentication failed. (access point = *access-point (host-name or IP-address)*)

[Cause] Possible causes are as follows:

(1) No credentials are specified, or the specified credentials are invalid.

(2) The discovery range for when the computer was discovered has been deleted.

[Action] Continues processing.

[Workaround]

(1) Check whether you are able to log on to the access point as an administrator by using the Windows credentials specified for agent deployment, and then retry agent deployment.

(2) Increase the discovery range, and then specify credentials. Perform discovery again, and then retry agent deployment.

KDEX5068-W

Agent delivery failed. Connection failure to the administrative share. Access point=*access-point (host-name or IP-address)*

[Cause] Failed to access the administrative share using the authentication information.

[Action] Continue the process.

[Workaround] Check if the administrative share (ADMIN$) is enabled in the target computer. Check if you can log into the target computer as an Administrator with the Windows authentication information specified for agent delivery. After confirming the settings, retry agent delivery.

KDEX5069-W

An error occurred during agent installation. Access point=*access-point (host-name or IP-address)*, Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred during agent installation.

[Action] Continue the process.

[Workaround] Check if the target computer is prepared for agent installation, and then retry agent delivery. If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5070-W

Started Agent delivery. But Failed to connect to the computer. Access point=*access-point (host-name or IP-address)*

[Cause] Failed to connect to the administrative shared folder in target computer.

[Action] Continue the process.

[Workaround] Turn the power on, if the power of the target computer is switched off. If the firewall is enabled, confirm the port for shared files are open and retry discovery.

KDEX5071-W

A communication error occurred during agent delivery. Access point = *access-point (host-name or IP-address)*

[Cause] Possible causes include the following:

(1) There is a problem in the status of the network between the management server and the computer to which the agent is to be delivered.

(2) The IP address of the computer to which the agent is to be delivered does not exist in the device information.

[Action] Continues processing.

[Workaround]

(1) Verify that there are no problems in the status of the network, and then retry agent delivery.

(2) From the device window, in the [Device List], specify the IP address in the computer device information, and then retry agent delivery.

KDEX5072-E

An error occurred during agent delivery. Access point=*access-point (host-name or IP-address)*, Error code=*error-code (maintenance-code)*

[Cause] An error occurred during agent delivery. The error is caused by a factor other than connection, communication, and authentication.

[Action] Continue the process.

[Workaround] Use the troubleshooting information collection command to collect troubleshooting information and contact support service.

KDEX5073-E

An error occurred on the target computer during agent delivery. Access point=*access-point (host-name or IP-address)*, Error code=*error-code (maintenance-code)*

[Cause] An error occurred on the target computer during agent delivery.

[Action] Continue the process.

[Workaround] Retry agent delivery. If the problem persists, execute troubleshooting information collection command to collect troubleshooting information and contact customer support.

KDEX5074-W

Unabble to deliver agent since the MAC address of the computer differs from the registered MAC address.

[Cause] On agent delivery, the MAC address of the target computer, and that managed by the management server are different. The system had connected to a different computer from the one discovered. Access point=*access-point (host-name or IP-address)*, Registered MAC address=*registered-MAC-address*

[Action] Continue the process.

[Workaround] This may be caused by out-of-date discovery information. Retry agent delivery after re-executing discovery.

KDEX5075-W

Agent delivery was not performed because an agent is already installed. (access point = *access-point (host-name or IP-address)*)

[Cause] An agent is already installed on the target computer.

[Action] Continues processing.

[Workaround] Agent delivery is not required because an agent is already installed on the target computer.

KDEX5076-W

Agent is installed but no communication from the agent. Access point=*access-point (host-name or IP-address)*

[Cause] The management server has not received any confirmation message from the installed agent.

[Action] Continue the process.

[Workaround] Check the operational status of the network between the management server and the target computer, and confirm whether the agent is installed. If the agent is not installed, retry agent delivery. If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5077-W

Failed to deliver agent. Could not resolve management server host name *management-server-host-name* on the target computer. Access point=*access-point (host-name or IP-address)*

[Cause] Could not resolve the management server's host name on the target computer.

[Action] Continue the process.

[Workaround] Configure the agent setting to enable host name resolution on the target computer, if the setting Connecting management server is set to the default host name. Or, you can set the IP address instead of host name, and then retry agent delivery.

KDEX5078-W

Credentials required for agent deployment have not been specified. (access point = *access-point (host-name or IP-address)*)

[Cause] Possible causes are as follows:

(1) You cannot log on to the access point because no Windows credentials have been specified for agent deployment.

(2) The discovery range for when the computer was discovered has been deleted.

[Action] Continues processing.

[Workaround]

(1) Specify Windows credentials to enable logon to the access point as an administrator, and then retry agent deployment.

(2) Increase the discovery range, and then specify credentials. Perform discovery again, and then retry agent deployment.

KDEX5079-E

An error occurred while creating the agent media used for agent delivery. Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred while creating the agent media used for agent delivery.

[Action] Cancel the process.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5080-I

Agent delivery started (retry).

KDEX5081-I

Agent delivery complete (retry).

KDEX5082-W

Failed to deliver agent since the agent is being installed. Access point=*access-point (host-name or IP-address)*

[Cause] Delivered agent to a computer while it was processing another agent delivery.

[Action] Continue the process.

[Workaround] Another agent delivery is in process, so agent delivery is not required.

KDEX5083-W

Failed to complete agent installation within *elapsed-time-in-minutes* minutes. Access point=*access-point (host-name or IP-address)*

[Cause] Failed to complete agent installation within the given time.

[Action] Continue the process.

[Workaround] If the agent is installed after this message display, agent will work normally, no action required. If the agent failed to install for a while, retry agent delivery.

KDEX5084-W

Failed to deliver the agent. User authentication has failed. Access Point=*access-point (host-name or IP-address)*.

[Cause] Authentication information is either not set or is invalid.

[Action] Continue the process.

[Workaround] Check if you can log into the target device as an Administrator with the **Active Directory** information specified for agent delivery.Then, retry agent delivery.

KDEX5085-W

Failed to deliver the agent. Administrative share connection failure. Access point=*access-point (host-name or IP-address)*

[Cause] Failed to access the administrative share using the authentication information.

[Action] Continue the process.

[Workaround] Check if the administrative share (ADMIN$) is enabled in the target computer. Check if you can log into the target device as an Administrator with the **Active Directory** information specified for agent delivery. After confirming the settings, retry agent delivery.

KDEX5086-W

Authentication information required for agent delivery is not specified. Access point=*access-point (host-name or IP-address)*

[Cause] Login has failed because the Active Directory information required for agent delivery was not specified.

[Action] Continue the process.

[Workaround] Specify one or more **Active Directory** information to log in the target computer with Administrator privileges. Retry agent delivery.

KDEX5100-I

Agentless processing was started on the site server.

Access point=*access-point-IP-address*, Operation type=*agentless-operation-type*.

KDEX5101-E

Agentless processing could not be started on the site server.

Access point=*access-point-IP-address*, Operation type=*agentless-operation-type*.

[Cause] The site server service (*site-server-service-name*) has not been started.

[Action] Cancel the process.

[Workaround] Confirm that the site server process (*site-server-service-name*) has been started, and then retry the operation.

KDEX5102-I

Agentless processing on the site server is complete.

Access point=*access-point-IP-address*, Operation type=*agentless-operation-type*.

KDEX5103-E

A request for agentless processing could not be sent to the site server.

Access point=*access-point-IP-address*, Operation type=*agentless-operation-type*.

[Cause] Possible causes are as follows:

(1) The site server service (*site-server-service-name*) has not been started.

(2) The load on the site server has increased.

(3) An error has occurred on the network.

[Action] Cancel processing.

[Workaround] Check whether an error has occurred on the network, and then check whether the site server service (*site-server-service-name*) has been started. To perform discovery, collection of the latest device data, or agent delivery, wait a while, and then retry the operation.

KDEX5104-I

Starting discovery from IP address range. (*n* time around)

KDEX5199-E

A system error has occurred.

[Cause] A critical internal error has occurred in the system.

[Action] Cancel discovery or agent delivery.

[Workaround] Confirm whether configuration environment of the management server is valid and is operating properly. If the problem persists, Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5301-I

Connected to Active Directory.

KDEX5302-E

Active Directory connection failed.

KDEX5305-I

A connection to JP1/NETM/NM - Manager was successfully established.

KDEX5306-E

Failed to connect JP1/NETM/NM - Manager.

KDEX5307-I

Successfully connected to the Support Service site.

KDEX5308-E

Failed to connect the Support Service site.

KDEX5309-I

Updated the security policy.

KDEX5310-E

Failed to update the security policy.

KDEX5311-I

Determined the security status. Performed date=*security-judgment-data*, Safe=*number-of-safe-PCs*, Caution=*number-of-caution-PCs*, Warning=*number-of-warning-PCs*, Danger=*number-of-danger-PCs*, Unknown=*number-of-unknown-PCs*, Out of Target=*number-of-out-of-target-PCs*

KDEX5314-I

Network connection denied. Performed date=*performed-date*, Number of target computers=*number-of-target-computers*

KDEX5315-I

Network connection successful. Performed date=*performed-date*, Number of target computers=*number-of-target-computers*

KDEX5316-E

An error occurred in (JP1_ITDM_Service). Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred in the (JP1_ITDM_Service).

[Action] Stop the (JP1_ITDM_Service).

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5317-E

Improper security status result. Host name=*host-name-or-IP-address*

[Cause] The computer does not have an agent installed.

[Action] Cancel the process for determining security status.

[Workaround] Install an agent on the computer indicated by the host name.

KDEX5319-E

An error occurred while sending e-mail notification to the system administrator. Failed to reach the mail server. Mail server host name=*mail-server-host-name*, Mail server port number=*mail-server-port-number*

[Cause] The host name or port number specified in the settings screen of the mail server is either invalid or the mail server is not in operation.

[Action] Cancel e-mail notification.

[Workaround] Check the host name and port number of the mail server, in the settings screen. Also check the operational status of the mail server. To check the mail server connectivity, send a test mail.

KDEX5320-E

An error occurred while sending e-mail notification to the system administrato. Invalid SMTP authentication information. Mail server host name=*mail-server-host-name*, Mail server port number=*mail-server-port-number*

[Cause] Incorrect SMTP authentication information in the mail server settings screen.

[Action] Cancel e-mail notification.

[Workaround] Check the SMTP authentication information specified in the settings screen of the mail server. To check the mail server connectivity, send a test mail.

KDEX5326-E

Failed to start the (JP1_ITDM_Service). The port number is already in use. Error code=*error-code (maintenance-code)*, Port number=*port-number*

[Cause] The port number is already in use.

[Action] Stop the(JP1_ITDM_Service).

[Workaround] Change the port number and start the service (JP1_ITDM_Service).

KDEX5335-W

Failed to retrieve added device information from the Active Directory server. An irretrievable Active Directory attribute is specified. List of attribute names=*list-of-attribute-names*

[Cause] An irretrievable Active Directory attribute is specified.

[Action] Cancel information retrieval from the added devices.

[Workaround] Check the settings for the added device information.

KDEX5336-I

Started the (JP1_ITDM_Service).

KDEX5337-E

Failed to start the (JP1_ITDM_Service).

KDEX5338-E

Failed to start the (JP1_ITDM_Service). Setup is not complete.

[Cause] JP1/IT Desktop Management - Manager Setup is not complete.

[Action] Cancel starting the(JP1_ITDM_Service).

[Workaround] Retry starting the (JP1_ITDM_Service) after the JP1/IT Desktop Management - Manager Setup is completed.

KDEX5339-E

Failed to start the (JP1_ITDM_Service). Error code=*error-code (maintenance-code)*

[Cause] A critical error has occurred in the service (JP1_ITDM_Service).

[Action] Cancel the launch of the service (JP1_ITDM_Service).

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5340-I

Stopped the (JP1_ITDM_Service).

KDEX5341-E

An error occurred in the (JP1_ITDM_Service). Stopped the (JP1_ITDM_Service).

KDEX5342-E

An error occurred in the (JP1_ITDM_Service). Error code=*error-code (maintenance-code)*

[Cause] A critical error occurred in the (JP1_ITDM_Service).

[Action] Stop the (JP1_ITDM_Service).

[Workaround] Determine the cause of the error and use appropriate workarounds to solve the problem, and restart the (JP1_ITDM_Service). Or, use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5343-W

An error occurred while sending a user notification message. Agent is not installed in the computer. Host name=*host-name-or-IP-address*

[Cause] Agent is not installed in the computer.

[Action] Cancel the notification.

[Workaround] Install an agent to the computer indicated by the host name.

KDEX5344-W

An error occurred while controlling network connection. The computer does not have a network interface card. Host name=*host-name-or-IP-address*

[Cause] The computer does not have a network interface card.

[Action] Cancel the control of network connection.

[Workaround] Install a network interface card on the computer indicated by the host name.

KDEX5346-E

Failed to start the service(JP1_ITDM_Service). The license has expired.

[Cause] Failed to start the service(JP1_ITDM_Service) because the license has expired.

[Action] Cancel starting the service(JP1_ITDM_Service).

[Workaround] Purchase a valid license.

KDEX5347-E

Failed to start the (JP1_ITDM_Service). Setup, the database manager, or a command is in execution.

[Cause] The service (JP1_ITDM_Service) was started while setup, the database manager, or a command was in execution.

[Action] Cancel starting the (JP1_ITDM_Service).

[Workaround] Wait until the executing process (Setup, Database Manager, or command) ends, and then restart the (JP1_ITDM_Service).

KDEX5352-E

An error occurred during e-mail notification to the administrator. The encrypted communication failed. Mail server host name=*mail-server-host-name*, Mail server port number=*mail-server-port-number*

[Cause] The following are possible causes:

(1) The mail certificate is not installed on the mail server.

(2) Incorrect authentication method settings for the mail server.

[Action] Cancel e-mail notification.

[Workaround]
(1) Install the mail certificate on the mail server.
(2) Check the authentication method settings for the mail server.
To check the mail server connectivity, send a test mail.

KDEX5353-I

The system is connected to the mail server.

KDEX5354-E

Failed to connect the system to the mail server.

KDEX5355-E

Failed to e-mail the Administrators.
[Cause] A critical error occurred during e-mail notification.
[Action] Cancel e-mail notification.
[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5359-W

Failed to perform Automatic Windows Update. Agent is not installed. Host name=*host-name-or-IP-address*
[Cause] Agent is not installed.
[Action] Cancel automatic Windows Update.
[Workaround] Install Agent on the computer indicated in the above Host name.

KDEX5360-E

An error occurred in JP1_ITDM_Service.
[Cause] An error occurred in the database.
[Action] Stop JP1_ITDM_Service.
[Workaround] Set up JP1/IT Desktop Management - Manager again.

KDEX5361-E

Failed to connect to the Active Directory server. A connection error has occurred. Error code=*error-code*, Host name=*Active-Directory-server-host-name*, Port number=*port-number*, Connection account=*user-ID*, Route path for information acquisition=*root-OU*
[Cause] The possible causes are given below:
(1) The specified host name is incorrect.
(2) The specified port number is incorrect.
(3) The Active Directory server is not running.
[Action] Cancel the acquisition of device and organizational information.
[Workaround]
(1) Check the specified host name in the Active Directory settings.
(2) Check the specified port number in the Active Directory settings.

(3) Check whether the Active Directory server is running.

To check the Active Directory server connectivity, test the connection to it.

KDEX5362-E

Failed to connect to the Active Directory server. Connection authentication has failed. Error code=*error-code*, Host name=*Active-Directory-server-host-name*, Port number=*port-number*, Connection account=*user-ID*, Route path for information acquisition=*root-OU*

[Cause] The specified account or password is incorrect.

[Action] Cancel the acquisition of device and organizational information.

[Workaround] Check the specified account and password in the Active Directory settings. To check the Active Directory server connectivity, test the connection.

KDEX5363-E

Failed to connect to the Active Directory server.

Could not find the specified domain. Error code=*error-code*, Host name=*Active-Directory-server-host-name*, Port number=*port-number*, Connection account=*user-ID*, Route path for information acquisition=*root-OU*

[Cause] The specified domain in the route path for acquiring Active Directory information is incorrect.

[Action] Cancel the acquisition of device and organizational information.

[Workaround] Check the specified domain in the Active Directory settings. To check the Active Directory server connectivity, test the connection.

KDEX5364-E

Failed to connect to the Active Directory server.

The specified route path for acquiring Active Directory information could not be found. Error code=*error-code*, Host name=*Active-Directory-server-host-name*, Port number=*port-number*, Connection account=*user-ID*, Route path for information acquisition=*root-OU*

[Cause] The specified OU in the route path for acquiring Active Directory information is incorrect.

[Action] Cancel the acquisition of device and organizational information.

[Workaround] Check the specified OU in the Active Directory settings. To check the Active Directory server connectivity, test the connection to it.

KDEX5365-E

Failed to connect to the Active Directory server. Could not establish encrypted communication.

Error code=*error-code*, Host name=*Active-Directory-server-host-name*, Port number=*port-number*, Connection account=*user-ID*, Route path for information acquisition=*root-OU*

[Cause] The possible causes are given below:

(1) The specified port number is incorrect.

(2) The certificate is not installed in the Active Directory server.

[Action] Cancel the acquisition of device and organizational information.

[Workaround]

(1) Check the specified port number in the Active Directory settings.

(2) Check whether the certificate is installed in the Active Directory server.

To check the Active Directory server connectivity, test the connection.

KDEX5366-I

Synchronization between JP1/IT Desktop Management - Manager and Active Directory is complete.

KDEX5367-E

Failed to connect to Product Update. The Product Update URL or The proxy server settings is incorrect. Error code=*error-code (maintenance-code)*

[Cause] The specified Product Update URL or The proxy server settings is incorrect.

[Action] Cancel the Product Update connection.

[Workaround] Check the specified URL or The proxy server settings in the Product Update settings. To check the Product Update connectivity, test the connection to it.

KDEX5368-E

Failed to connect toProduct Update. The user ID or password is incorrect. Error code=*error-code (maintenance-code)*

[Cause] The specified user ID or password is incorrect.

[Action] Cancel the Product Update connection.

[Workaround] Check the specified user ID or password in the Product Update settings.

To check the Product Update connectivity, test the connection.

KDEX5369-E

Failed to connect to Product Update. Error code=*error-code (maintenance-code)*

[Cause] The proxy server settings has an error.

[Action] Cancel the connection to Product Update.

[Workaround] Check the specified proxy server settings. To check the Product Update connectivity, test the connection.

KDEX5370-E

The service(JP1_ITDM_Service) will be terminated. The license has either expired or is invalid.

[Cause] The possible causes are given below:

(1) The license has expired.

(2) The license information is invalid.

[Action] Terminate the service(JP1_ITDM_Service).

[Workaround]

(1) Purchase a valid license.

(2) Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5371-I

Added update programs.

KDEX5372-E

Failed to add update program details.

KDEX5373-I

Added antivirus software information.

KDEX5374-E

Failed to add antivirus software information.

KDEX5375-I

Updated the definition file of Manager behavior.

KDEX5376-E

Failed to update the definition file of Manager behavior.

KDEX5377-I

Updated the agent version.

KDEX5378-E

Failed to update the agent version.

KDEX5379-I

Connected to the Microsoft site successfully.

KDEX5380-E

Failed to connect the Microsoft site.

KDEX5381-I

Based on the settings in securit policy settings, the mandatory Windows Update will be distributed. You can check the task progress status on the distribution screen. Task name=*task-name*

KDEX5382-E

Windows Update distribution task is terminated abnormally. Task name=*task-name*

[Cause] The possible causes are given below:

(1) The Windows Update File download failed.

(2) Windows Update File was not registered when you added Windows Update manually.

[Action] Cancel installation.

[Workaround]

(1) Check the proxy server settings of Product Update in Settings window and network connection status. Execute task again.

(2) Register Windows Update File. Execute task again.

KDEX5383-I

The definition file of Agent behavior was updated.

KDEX5384-E

Failed to update the definition file of Agent behavior.

KDEX5385-I

The JP1_ITDM_Remote Site Service started.

KDEX5386-E

The JP1_ITDM_Remote Site Service failed to start.

KDEX5387-E

The JP1_ITDM_Remote Site Service failed to start. Setup is not complete.

[Cause] Setup of JP1/IT Desktop Management - Manager is not complete.

[Action] Cancel startup of the JP1_ITDM_Remote Site Service.

[Workaround] After setup of JP1/IT Desktop Management - Manager is complete, restart the JP1_ITDM_Remote Site Service.

KDEX5388-E

The JP1_ITDM_Remote Site Service failed to start. (error code = *error-code (maintenance-code)*)

[Cause] A critical error occurred in the JP1_ITDM_Remote Site Service.

[Action] Cancel startup of the JP1_ITDM_Remote Site Service.

[Workaround] Collect troubleshooting information, and contact Customer Support.

KDEX5389-I

The JP1_ITDM_Remote Site Service stopped.

KDEX5390-E

An error occurred in the JP1_ITDM_Remote Site Service. The JP1_ITDM_Remote Site Service will now stop.

KDEX5391-E

An error occurred in the JP1_ITDM_Remote Site Service. (error code = *error-code (maintenance-code)*)

[Cause] A critical error occurred in the JP1_ITDM_Remote Site Service.

[Action] Stop the JP1_ITDM_Remote Site Service.

[Workaround] Following the instructions in the messages output before this message, remove the cause of the error, and then restart the JP1_ITDM_Remote Site Service. If the problem persists, use the troubleshooting information collection command to collect troubleshooting information, and contact Customer Support.

KDEX5392-E

An error occurred in the JP1_ITDM_Remote Site Service. (error code = *error-code (maintenance-code)*)
[Cause] A critical error occurred in the JP1_ITDM_Remote Site Service.
[Action] Stop the JP1_ITDM_Remote Site Service.
[Workaround] Collect troubleshooting information, and contact Customer Support.

KDEX5393-E

The JP1_ITDM_Remote Site Service failed to start. The port number is already in use. (error code = *error-code (maintenance-code)*, port number = *port-number*)
[Cause] The port number is already in use.
[Action] Stop the JP1_ITDM_Remote Site Service.
[Workaround] Change the port number, and then start the JP1_ITDM_Remote Site Service.

KDEX5394-E

The JP1_ITDM_Remote Site Service failed to start. Setup is in progress, or a command is executing.
[Cause] The JP1_ITDM_Remote Site Service started while setup was in progress or a command was executing.
[Action] Cancel startup of the JP1_ITDM_Remote Site Service.
[Workaround] Wait until setup or the command ends, and then restart the JP1_ITDM_Remote Site Service.

KDEX5395-E

Failed to start the service (JP1_ITDM_Service). The license for this product has not been authenticated (registered).
[Cause] The service (JP1_ITDM_Service) could not be started because the license for this product is not registered.
[Action] Cancels startup of the service (JP1_ITDM_Service).
[Workaround] Authenticate (register) the license for this product.

KDEX5396-I

A connection to an MDM server was established. (MDM setting = *MDM-setting-name*)

KDEX5397-E

Failed to connect to an MDM server. (MDM setting = *MDM-setting-name*)

KDEX5399-E

Failed to start the service (JP1_ITDM_Service). The data folder shared between servers cannot be accessed.
[Cause] Possible causes include the following:
(1) The database server is stopped.
(2) A network error occurred.
[Action] Cancels startup of the service (JP1_ITDM_Service).
[Workaround]
(1) Start the database server, and then start the service (JP1_ITDM_Service).
(2) Resolve the cause of the network failure, and then start the service (JP1_ITDM_Service).

KDEX5400-E

Failed to start the service (JP1_ITDM_Service). The data folder shared between servers cannot be accessed.

[Cause] The user name or password for connecting to the data folder shared between servers is incorrect.

[Action] Cancels startup of the service (JP1_ITDM_Service).

[Workaround] Verify that the user name and password for connecting to the data folder shared between servers are correct. (This user name and password were specified during management server setup.) Then, start the service (JP1_ITDM_Service).

KDEX5401-E

Failed to collect device information and organization information from the Active Directory server. (error code = *error-code*)

[Cause] An error occurred during collection of device information and organization information from the Active Directory server.

[Action] Cancels collection of device information and organization information.

[Workaround] Use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX5402-I

A smart device will be locked.

KDEX5403-E

Failed to lock a smart device.

KDEX5404-E

Failed to lock a smart device. (error code = *error-code*, MDM server host name = *MDM-server-host-name*, MDM server port number = *MDM-server-port-number*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*)

[Cause] Possible causes include the following:

(1) Connection to the MDM server failed.

(2) Connection to the proxy server failed.

(3) The MDM server is not running.

[Action] Cancels locking of the smart device.

[Workaround]

(1) Check the host name and port number of the MDM server that were set in the settings window for MDM linkage.

(2) Check the IP address and port number of the proxy server that were set in the settings window for MDM linkage.

(3) Check whether the MDM server is running.

KDEX5405-E

Failed to lock a smart device. (error code = *error-code*, MDM server user ID = *MDM-server-user-ID*)

[Cause] Authentication for connection to the MDM server failed.

[Action] Cancels locking of the smart device.

[Workaround] Check the user ID and password for the MDM server that were set in the settings window for MDM linkage.

KDEX5406-E

Failed to lock a smart device. (error code = *error-code*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*, proxy server user ID = *proxy-server-user-ID*)

[Cause] Authentication for connection to the proxy server failed.

[Action] Cancels locking of the smart device.

[Workaround] Check the IP address, port number, user ID, and password for the proxy server that were set in the settings window for MDM linkage.

KDEX5407-E

Failed to lock a smart device. (error code = *error-code*)

[Cause] Possible causes include the following:

(1) The applicable smart device is not being managed by the MDM system.

(2) The profile of the MDM system has been deleted from the smart device.

[Action] Cancels the locking of the smart device.

[Workaround] Verify the following, and then try collecting smart device information from the MDM server again.

(1) Has the smart device been specified as a managed device of the MDM system?

(2) Has the profile of the MDM system been installed on the smart device?

KDEX5409-E

Failed to lock a smart device. (error code = *error-code*)

[Cause] An MDM linkage error occurred.

[Action] Cancels locking of the smart device.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5410-I

The password of a smart device will be reset.

KDEX5411-E

Failed to reset the password of a smart device.

KDEX5412-E

Failed to reset the password of a smart device. (error code = *error-code*, MDM server host name = *MDM-server-host-name*, MDM server port number = *MDM-server-port-number*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*)

[Cause] Possible causes include the following:

(1) Connection to the MDM server failed.

(2) Connection to the proxy server failed.

(3) The MDM server is not running.

[Action] Cancels the reset of the smart device password.

[Workaround]

(1) Check the host name and port number of the MDM server that were set in the settings window for MDM linkage.

(2) Check the IP address and port number of the proxy server that were set in the settings window for MDM linkage.

(3) Check whether the MDM server is running.

KDEX5413-E

Failed to reset the password of a smart device. (error code = *error-code*, MDM server user ID = *MDM-server-user-ID*)

[Cause] Authentication for the MDM server failed.

[Action] Cancels the reset of the smart device password.

[Workaround] Check the user ID and password for the MDM server that were set in the settings window for MDM linkage.

KDEX5414-E

Failed to reset the passcode of a smart device. (error code = *error-code*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*, proxy server user ID = *proxy-server-user-ID*)

[Cause] Authentication for connection to the proxy server failed.

[Action] Cancels the reset of the smart device passcode.

[Workaround] Check the IP address, port number, user ID, and password for the proxy server that were set in the settings window for MDM linkage.

KDEX5415-E

Failed to reset the password of a smart device. (error code = *error-code*)

[Cause] The target smart device is not managed by the MDM system.

[Action] Cancels the reset of the smart device password.

[Workaround] Obtain device information from the MDM server.

KDEX5417-E

Failed to reset the password of a smart device. (error code = *error-code*)

[Cause] An MDM linkage error occurred.

[Action] Cancels the reset of the smart device password.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5418-I

A smart device will be initialized.

KDEX5419-E

Failed to initialize a smart device.

KDEX5420-E

Failed to initialize a smart device. (error code = *error-code*, MDM server host name = *MDM-server-host-name*, MDM server port number = *MDM-server-port-number*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*)

[Cause] Possible causes include the following:
(1) Connection to the MDM server failed.
(2) Connection to the proxy server failed.
(3) The MDM server is not running.
[Action] Cancels initialization of the smart device.
[Workaround]
(1) Check the host name and port number of the MDM server that were set in the settings window for MDM linkage.
(2) Check the IP address and port number of the proxy server that were set in the settings window for MDM linkage.
(3) Check whether the MDM server is running.

KDEX5421-E

Failed to initialize a smart device. (error code = *error-code*, MDM server user ID = *MDM-server-user-ID*)
[Cause] Authentication for connection to the MDM server failed.
[Action] Cancels initialization of the smart device.
[Workaround] Check the user ID and password for the MDM server that were set in the settings window for MDM linkage.

KDEX5422-E

Failed to initialize a smart device. (error code = *error-code*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*, proxy server user ID = *proxy-server-user-ID*)
[Cause] Authentication for connection to the proxy server failed.
[Action] Cancels initialization of the smart device.
[Workaround] Check the IP address, port number, user ID, and password for the proxy server that were set in the settings window for MDM linkage.

KDEX5423-E

Failed to initialize a smart device. (error code = *error-code*)
[Cause] Possible causes include the following:
(1) The applicable smart device is not being managed by the MDM system.
(2) The profile of the MDM system has been deleted from the smart device.
[Action] Cancels initialization of the smart device.
[Workaround] Verify the following, and then try collecting smart device information from the MDM server again.
(1) Has the smart device been specified as a managed device of the MDM system?
(2) Has the profile of the MDM system been installed on the smart device?

KDEX5425-E

Failed to initialize a smart device. (error code = *error-code*)
[Cause] An MDM linkage error occurred.
[Action] Cancels initialization of the smart device.
[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5426-E

Failed to synchronize device information with the MDM system. (MDM setting name = *MDM-setting-name*, error code = *error-code*, MDM server host name = *MDM-server-host-name*, MDM server port number = *MDM-server-port-number*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*)

[Cause] Possible causes include the following:

(1) Connection to the MDM server failed.

(2) Connection to the proxy server failed.

(3) The MDM server is not running.

[Action] Cancels synchronization of device information with the MDM system.

[Workaround]

(1) Check the host name and port number of the MDM server that were specified in the settings window for MDM linkage.

(2) Check the IP address and port number of the proxy server that were specified in the settings window for MDM linkage.

(3) Check whether the MDM server is running.

KDEX5427-E

Failed to synchronize device information with the MDM system. (MDM setting name = *MDM-setting-name*, error code = *error-code*, MDM server user ID = *MDM-server-user-ID*)

[Cause] Authentication for connection to the MDM server failed.

[Action] Cancels synchronization of device information with the MDM system.

[Workaround] Check the user ID and password for the MDM server that were specified in the settings window for MDM linkage.

KDEX5428-E

Failed to synchronize device information with the MDM system. (MDM setting name = *MDM-setting-name*, error code = *error-code*, proxy server IP address = *proxy-server-IP-address*, proxy server port number = *proxy-server-port-number*, proxy server user ID = *proxy-server-user-ID*)

[Cause] Authentication for connection to the proxy server failed.

[Action] Cancels synchronization of device information with the MDM system.

[Workaround] Check the IP address, port number, user ID, and password for the proxy server that were set in the settings window for MDM linkage.

KDEX5430-E

Failed to synchronize device information with the MDM system. (error code = *error-code*)

[Cause] An MDM linkage error occurred.

[Action] Cancels synchronization of device information with the MDM system.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5431-I

Synchronization of device information with the MDM system was completed. (MDM setting name = *MDM-setting-name*)

KDEX5432-I

Synchronization of device information with the MDM system will now start. (MDM setting name = *MDM-setting-name*)

KDEX5433-E

Failed to start the service (JP1_ITDM_Remote Site Service). The command for deleting operation log data (deletelog) is not finished.

[Cause] The command for deleting operation log data is not finished or has failed.

[Action] Cancels the start of the service (JP1_ITDM_Remote Site Service).

[Workaround] After the command for deleting operation log data ends normally, start the service (JP1_ITDM_Remote Site Service).

KDEX5434-E

Failed to delete a smart device. (host name = *host-name*, error code = *error-code*)

[Cause] A database access error might have occurred.

[Action] Cancels the deletion of the smart device.

[Workaround]In the settings window, select [Discover Devices], [Check Discovery History], and [Managed Devices]. Then, select the devices that you want to delete, and delete them.

KDEX5435-E

An error occurred in the service (JP1_ITDM_Service). The data folder shared between servers cannot be accessed.

[Cause] Possible causes include the following:

(1) The database server is not running.

(2) A network failure occurred.

[Action] Continues processing of the service (JP1_ITDM_Service).

[Workaround] If the error occurs repeatedly, take the following actions:

(1) Start the database server.

(2) Resolve the cause of the network failure.

KDEX5436-E

An error occurred in the service (JP1_ITDM_Service). The data folder shared between servers cannot be accessed.

[Cause] The user name or password for connecting to the data folder shared between servers is incorrect.

[Action] Continues processing of the service (JP1_ITDM_Service).

[Workaround] If the error occurs repeatedly, verify that the user name and password for connecting to the data folder shared between servers are correct. (This user name and password were specified during management server setup.)

KDEX5440-E

Failed to synchronize device information with the MDM system. (MDM setting name = *MDM-setting-name*, error code = *error-code*)

[Cause] An MDM linkage error occurred.

[Action] Cancels synchronization of device information with the MDM system.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5450-E

Failed to lock a smart device.

[Cause] The server certificate of the MDM server is invalid.

[Action] Cancels the locking of the smart device.

[Workaround] Execute the keytool command to check whether the server certificate has been imported. If it has not, execute the keytool command to import the server certificate. For details about the keytool command, see the relevant documentation.

KDEX5451-E

Failed to lock a smart device. (error code = *error-code*)

[Cause] The applicable smart device is excluded from management by the MDM system.

[Action] Cancels the locking of the smart device.

[Workaround] From the MDM system, specify the applicable smart device as a managed device.

KDEX5452-E

Failed to unlock the pass code of a smart device.

[Cause] The server certificate of the MDM server is invalid.

[Action] Cancels the unlocking of the pass code of the smart device.

[Workaround] Execute the keytool command to check whether the server certificate has been imported. If it has not, execute the keytool command to import the server certificate. For details about the keytool command, see the relevant documentation.

KDEX5453-E

Failed to unlock the pass code of a smart device. (error code = *error-code*)

[Cause] The applicable smart device is excluded from management by the MDM system.

[Action] Cancels the unlocking of the pass code of the smart device.

[Workaround] From the MDM system, specify the applicable smart device as a managed device.

KDEX5454-E

Failed to initialize a smart device.

[Cause] The server certificate of the MDM server is invalid.

[Action] Cancels initialization of the smart device.

[Workaround] Execute the keytool command to check whether the server certificate has been imported. If it has not, execute the keytool command to import the server certificate. For details about the keytool command, see the relevant documentation.

KDEX5455-E

Failed to initialize a smart device. (error code = *error-code*)

[Cause] The applicable smart device is excluded from management by the MDM system.

[Action] Cancels initialization of the smart device.

[Workaround] From the MDM system, specify the applicable smart device as a managed device.

KDEX5456-E

Failed to synchronize device information with the MDM system. (MDM setting name = *MDM-setting-name*)

[Cause] The server certificate of the MDM server is invalid.

[Action] Cancels synchronization of device information with the MDM system.

[Workaround] Execute the keytool command to check whether the server certificate has been imported. If it has not, execute the keytool command to import the server certificate. For details about the keytool command, see the relevant documentation.

KDEX5460-I

Collection of the revision history started.

KDEX5461-I

Collection of the revision history ended.

KDEX5462-E

Collection of the revision history failed.

[Cause] A fatal error occurred during collection of the revision history.

[Action] Cancels collection of the revision history.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5463-E

Failed to output the file for saving the revision history.

[Cause] Possible causes include the following:

(1) You do not have access rights for the output folder for saving the revision history.

(2) An I/O error occurred.

[Action] Cancels output of the file for saving the revision history.

[Workaround]

(1) Verify that you have access rights for the output folder for saving the revision history.

(2) Verify that no disk failure has occurred.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5464-I

A request to allow connections to the network was sent to JP1/NETM/NM - Manager.

KDEX5465-I

A request to reject connections to the network was sent to JP1/NETM/NM - Manager.

KDEX5466-E

The request to JP1/NETM/NM - Manager to allow connections to the network failed.

[Cause] The JP1/NETM/NM - Manager service has not been started on the management server.

[Action] Stops allowing connections to the network.

[Workaround] Start the JP1/NETM/NM - Manager service on the management server.

KDEX5467-E

The request to JP1/NETM/NM - Manager to reject connections to the network failed.

[Cause] The JP1/NETM/NM - Manager service has not been started on the management server.

[Action] Stops rejecting connections to the network.

[Workaround] Start the JP1/NETM/NM - Manager service on the management server.

KDEX5468-E

The request to JP1/NETM/NM - Manager to allow connections to the network failed.

[Cause] JP1/NETM/NM - Manager has not been installed on the management server.

[Action] Stops allowing connections to the network.

[Workaround] Install JP1/NETM/NM - Manager on the management server.

KDEX5469-E

The request to JP1/NETM/NM - Manager to reject connections to the network failed.

[Cause] JP1/NETM/NM - Manager has not been installed on the management server.

[Action] Stops rejecting connections to the network.

[Workaround] Install JP1/NETM/NM - Manager on the management server.

KDEX5470-E

The request to JP1/NETM/NM - Manager to allow connections to the network failed. (error code = *error-code (maintenance-code)*)

[Cause] A fatal error occurred while connections to the network were being allowed.

[Action] Stops allowing connections to the network.

[Workaround] If this error occurs repeatedly, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5471-E

The request to JP1/NETM/NM - Manager to reject connections to the network failed. (error code = *error-code (maintenance-code)*)

[Cause] A fatal error occurred while connections to the network were being rejected.

[Action] Stops rejecting connections to the network.

[Workaround] If this error occurs repeatedly, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX5700-W

Insufficient hard disk space for *Database, Data, Operation Log Database, or Operation Log Backup*.

[Cause] Insufficient hard disk space for *Database, Data, Operation Log Database, or Operation Log Backup*.

[Action] None.

[Workaround] Increase hard disk space, or specify any other path for *Database, Data, Operation Log Database, or Operation Log Backup* on a hard disk with sufficient space.

KDEX5701-W

Insufficient hard disk space for *Database, Data, Operation Log Database, or Operation Log Backup*. A database failure might occur.

[Cause] Insufficient hard disk space for *Database, Data, Operation Log Database, or Operation Log Backup*.

[Action] None.

[Workaround] Increase hard disk space, or specify any other path for *Database, Data, Operation Log Database, or Operation Log Backup* on a hard disk with sufficient space.

KDEX6110-I

The (JP1_ITDM_Agent Control) service will be started.

KDEX6111-E

Failed to start the (JP1_ITDM_Agent Control) service.

KDEX6112-E

Failed to start the (JP1_ITDM_Agent Control) service.

[Cause] Failed to start the (JP1_ITDM_Agent Control) service.

[Action] Stop the (JP1_ITDM_Agent Control) service.

[Workaround] Start the (JP1_ITDM_Agent Control) service again. If the problem persists, use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX6113-E

Because JP1/IT Desktop Management - Manager setup is incomplete, startup of the (JP1_ITDM_Agent Control) service failed.

[Cause] Because JP1/IT Desktop Management - Manager setup is incomplete, the (JP1_ITDM_Agent Control) service could not be started.

[Action] Stops the (JP1_ITDM_Agent Control) service.

[Workaround] After JP1/IT Desktop Management - Manager setup is complete, start the (JP1_ITDM_Agent Control) service.

KDEX6114-E

Failed to start the (JP1_ITDM_Agent Control) service. The license has expired.

[Cause] Failed to start the (JP1_ITDM_Agent Control) service because the license has expired.

[Action] Cancels starting the (JP1_ITDM_Agent Control) service.

[Workaround] Purchase a valid license.

KDEX6115-E

Failed to start the (JP1_ITDM_Agent Control) service. Setup, the database manager, or a command is in execution.

[Cause] The (JP1_ITDM_Agent Control) service was started while setup, the database manager, or a command was in execution.

[Action] Cancel starting the (JP1_ITDM_Agent Control) service.

[Workaround] Wait until the executing process (Setup, Database Manager, or command) ends, and then restart the (JP1_ITDM_Agent Control) service.

KDEX6116-E

Service (JP1_ITDM_Agent Control) error occurred.

[Cause] The RD area has blocked the service.

[Action] Service (JP1_ITDM_Agent Control) has stopped.

[Workaround] JP1_ITDM_Agent Control has been set up again.

KDEX6117-E

The (JP1_ITDM_Agent Control) service will be terminated. The license has either expired or is invalid.

[Cause] Possible causes include the following:

(1) The license has expired.

(2) The license information is invalid.

[Action] Stops the (JP1_ITDM_Agent Control) service.

[Workaround]

(1) If the license has expired, purchase a valid license.

(2) If the license information is invalid, collect troubleshooting information by using troubleshooting information collection command, and then contact customer support.

KDEX6118-E

Failed to start the (JP1_ITDM_Agent Control) service. The license is not registered.

[Cause] Failed to start the (JP1_ITDM_Agent Control) service because the license is not registered.

[Action] Cancels starting the (JP1_ITDM_Agent Control) service.

[Workaround] Register a valid license.

KDEX6119-E

Failed to start the service (JP1_ITDM_Agent Control).

[Cause] An attempt was made to start the service (JP1_ITDM_Agent Control) on the database server.

[Action] Cancels startup of the service (JP1_ITDM_Agent Control).

[Workaround] Check whether the service (JP1_ITDM_Agent Control) is running on the management server. If it is not, start the service on the management server.

KDEX6120-I

The (JP1_ITDM_Agent Control) service is complete.

KDEX6121-E

Failed to stop the (JP1_ITDM_Agent Control) service.

KDEX6122-E

Failed to stop the (JP1_ITDM_Agent Control) service.

[Cause] Failed to stop (JP1_ITDM_Agent Control) service due to an error.

[Action] Stop the (JP1_ITDM_Agent Control) service.

[Workaround] If the service fails to stop after a while, use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX6131-E

(JP1_ITDM_Agent Control) service has stopped abnormally.

KDEX6132-E

(JP1_ITDM_Agent Control) service has stopped abnormally.

[Cause] Due to a failure, (JP1_ITDM_Agent Control) service has stopped abnormally.

[Action] Stop the (JP1_ITDM_Agent Control) service.

[Workaround] Restart the service (JP1_ITDM_Agent Control). If the problem persists, use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX6140-I

Notified the user with a message. Performed date=*performed-date*, Notification destination=*notification-destination-host-name*

KDEX6141-I

The database was expanded because of capacity shortage in the operation log storage area.

KDEX6151-E

Failed to start the service (JP1_ITDM_Agent Control). The data folder shared between servers cannot be accessed.

[Cause] Possible causes include the following:

(1) The database server is stopped.

(2) A network failure occurred.

[Action] Cancels startup of the service (JP1_ITDM_Agent Control).

[Workaround]

(1) Start the database server, and then start the service (JP1_ITDM_Agent Control).

(2) Resolve the cause of the network failure, and then start the service (JP1_ITDM_Agent Control).

KDEX6152-E

Failed to start the service (JP1_ITDM_Agent Control). The data folder shared between servers cannot be accessed.

[Cause] The user name or password for connecting to the data folder shared between servers is incorrect.

[Action] Cancels startup of the service (JP1_ITDM_Agent Control).

[Workaround] Verify that the user name and password for connecting to the data folder shared between servers are correct. (This user name and password were specified during management server setup.) Then, start the service (JP1_ITDM_Agent Control).

KDEX6211-E

An error occurred while initializing audit logs of the (JP1_ITDM_Agent Control) service.

[Cause] Due to a failure, an error occurred while initializing audit logs of the (JP1_ITDM_Agent Control) service.

[Action] None.

[Workaround] Restart the (JP1_ITDM_Agent Control) service. If the problem persists, use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX6221-E

An error occurred while processing the audit logs of the (JP1_ITDM_Agent Control) service.

[Cause] Due to a failure, an error occurred during the output processing of audit logs of the (JP1_ITDM_Agent Control) service.

[Action] None.

[Workaround] Restart the (JP1_ITDM_Agent Control) service. If the problem persists, use troubleshooting information collection command to collect troubleshooting information and contact Customer Support.

KDEX6411-I

The on-demand task is complete. (task name = *task-name*, number of error nodes = *number-of-error-nodes*)

KDEX6412-E

The installation task was terminated because of an error. Target computer name=*target-computer-name*, Task name=*task-name*

[Cause] *cause-of-error*

[Action] Cancel installation.

[Workaround] *workaround*

KDEX6413-E

The uninstallation task was terminated because of an error. Target computer name=*target-computer-name*, Task name=*task-name*

[Cause] *cause-of-error*

[Action] Cancel uninstallation.

[Workaround] *workaround*

KDEX6511-E

An error occurred during event notification to JP1/IM. (error code = *error-code*)

[Cause] A database access error occurred.

[Action] Cancels event notification to JP1/IM.

[Workaround] Check whether the service (JP1_ITDM_DB Service) is running. If it is not, start it. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8000-E

Failed to execute the command. The specified arguments are invalid. (command name = *command-name*)

[Cause] The specified arguments are invalid.

[Action] Cancel command execution.

[Workaround] Confirm the command arguments, and retry execution.

KDEX8001-E

Failed to execute the command. You do not have the required permissions. (command name = *command-name*)

[Cause] The command was executed by a user without Administrator permissions.

[Action] Cancel command execution.

[Workaround] Re-execute the command as a user with Administrator permissions.

KDEX8002-E

Failed to execute the command. Setup is in progress, or a command is executing. (command name = *command-name*)

[Cause] The command was executed while setup was in progress or a command was executing.

[Action] Cancel command execution.

[Workaround] Wait until the process or command ends, and then re-execute the command.

KDEX8003-I

Re-creation of the operation log database has started.

KDEX8004-E

Failed to execute the command. Setup is not complete. (command name = *command-name*)

[Cause] Setup of JP1/IT Desktop Management - Remote Site Server is not complete.

[Action] Cancel command execution.

[Workaround] Complete setup of JP1/IT Desktop Management - Remote Site Server, and then re-execute the command.

KDEX8005-E

Failed to execute the command. (command name = *command-name*, error code = *error-code (maintenance-code)*)

[Cause] A critical error occurred during command execution.

[Action] Cancel command execution.

[Workaround] Use the troubleshooting information collection command to collect troubleshooting information, and contact Customer Support.

KDEX8006-E

Failed to execute the command. A database access error occurred. (details = *DBMS-message*, command name = *command-name*)

[Cause] The service (JP1_ITDM_DB Service) has stopped, or the error described in "details" occurred.

[Action] Cancels command execution.

[Workaround] Start the service (JP1_ITDM_DB Service) or resolve the error described in "details", and then re-execute the command. If the problem persists, collect troubleshooting information on the site server by using the troubleshooting information collection command, and then contact Customer Support.

KDEX8007-I

The operation log was moved successfully.

KDEX8008-E

Failed to execute the command. A file access error occurred. (command name = *command-name*)

[Cause] Possible causes include the following:

(1) You do not have access permission for the specified folder.

(2) There is not enough free disk space for the specified folder.

(3) An I/O error occurred.

[Action] Cancel command execution.

[Workaround]

(1) Make sure you have access permission for the specified folder.

(2) Make sure there is enough free disk space for the specified folder.

(3) Make sure that a disk error did not occur.

If the problem persists, use the troubleshooting information collection command to collect troubleshooting information, and contact Customer Support.

KDEX8009-E

Failed to execute the command. The specified folder is invalid. (command name = *command-name*)

[Cause] Possible causes include the following:

(1) The operation log folder currently in use or a folder that does not contain an operation log is specified for the migration-source folder.

(2) The migration-destination folder is not empty.

[Action] Cancels command execution.

[Workaround] Make sure the specified folder is correct, and then re-execute the command. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8010-I

Storage of the operation logs is complete.

KDEX8011-W

Free space on the disk containing the operation log backup folder has become scarce. Increase the free disk space, or change to a disk that has enough free disk.

KDEX8012-W

Storage of the operations logs stopped because there is almost no free space on the disk containing the operation log backup folder. Increase the free disk space, or change to a disk that has enough free disk.

KDEX8013-W

Free space on the disk containing the operation log database has become scarce.

KDEX8014-W

Storage of the operation logs stopped because there is almost no free disk space for the operation log database.

KDEX8015-I

The operation log database was expanded because its capacity was insufficient.

KDEX8016-I

Command execution was canceled. (command name = *command-name*)

KDEX8017-W

Free space on the disk containing the folder that stores content has become scarce. Increase the free disk space, or change to a disk that has enough free space.

KDEX8018-W

Downloading of content to the site server was stopped because there is almost no free space on the disk containing the folder that stores content. Increase the free disk space, or change to a disk that has enough free space.

KDEX8019-E

Failed to execute the command. The JP1_ITDM_Remote Site Service service failed to stop. (command name = *command-name*)

[Cause] The command was executed during processing to start or stop the JP1_ITDM_Remote Site Service service.

[Action] Cancels command execution.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8020-E

Failed to execute the command. Failed to connect to the management server. (command name = *command-name*)

[Cause] Possible causes are as follows:

(1) The management server service is not running.

(2) A failure occurred on the network of the management server.

[Action] Cancels command execution.

[Workaround]

(1) Execute the startservice command to start the management server service, and then re-execute the command.

(2) Eliminate the cause of the network failure, and then re-execute the command.

KDEX8021-I

The list of agents managing operation logs was reported to the managing server.

KDEX8022-W

Re-creation of the operation log database started normally, but the JP1_ITDM_Remote Site Service service could not start. (command name = *command-name*)

[Cause] A critical error occurred during command execution.

[Action] Cancels command execution.

[Workaround] Collect troubleshooting information on the site server by using the troubleshooting information collection command, and then contact Customer Support.

KDEX8023-W

The operation log was moved successfully, but deletion of the move-source folder failed. (command name = *command-name*)

[Cause] A file in the move-source folder is being used.

[Action] Cancels command execution.

[Workaround] Stop any application using the move-source folder, and then delete the folder.

KDEX8024-W

The operation log was moved successfully, but the service (JP1_ITDM_Remote Site Service) could not be started. (command name = *command-name*)

[Cause] A fatal error occurred in the command.

[Action] Cancel command execution.

[Workaround] Collect troubleshooting information on the site server by using the troubleshooting information collection command, and then contact Customer Support.

KDEX8025-I

The communication service of the site server was started.

KDEX8026-E

An attempt to start the communication service of the site server failed.

KDEX8027-I

The communication service of the site server was stopped.

KDEX8028-E

A database access error occurred in the communication service of the site server. (details = *DBMS-message*)

[Cause] The service (JP1_ITDM_DB Service) has not started, or the error described in "details" occurred.

[Action] Restart the communication service of the site server.

[Workaround] Start the service (JP1_ITDM_DB Service), or resolve the error described in "details" and restart the service (JP1_ITDM_Remote Site Service). If the problem persists, collect troubleshooting information on the site server by using the troubleshooting information collection command, and then contact Customer Support.

KDEX8029-E

An error occurred in the communication service of the site server. (error code = *internal-error-code*)

[Cause] An internal error occurred.

[Action] Restart the communication service of the site server.

[Workaround] Collect troubleshooting information on the site server by using the troubleshooting information collection command, and then contact Customer Support.

KDEX8030-E

Re-creation of the operation log database has failed.

KDEX8031-I

Deletion of operation log data ended normally. (number of operation log items before deletion = *number-of-operation-log-items*, number of operation log items after deletion = *number-of-operation-log-items*)

KDEX8032-W

Deletion of operation log data ended normally, but the service (JP1_ITDM_Remote Site Service) could not be started. (command name = *command-name*)

[Cause] A fatal error occurred in the command.

[Action] Cancels execution of the command.

[Workaround] Collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8033-E

Command execution failed. There is not enough free space in the work folder. (command name = *command-name*, required space = *required-space*)

[Cause] Possible causes include the following:

(1) There is not enough free space on the disk that contains the specified folder.

(2) If no work folder has been specified, there is not enough free space on the disk that contains the data folder.

[Action] Cancels execution of the command.

[Workaround] Increase the free space on the disk or specify a folder on a disk that has enough free space, and then re-execute the command. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8034-E

Deletion of operation log data failed.

KDEX8035-W

Operation log data to be deleted does not exist.

KDEX8036-E

Command execution failed. The specified date is invalid. (command name = *command-name*)

[Cause] A date that does not exist was specified.

[Action] Cancels execution of the command.

[Workaround] Check the specified date, and then re-execute the command. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8037-E

Command execution failed. The specified folder is invalid. (command name = *command-name*)

[Cause] Possible causes include the following:

(1) The folder is not specified using an absolute path.

(2) A path exceeding 120 bytes is specified for the folder.

(3) The folder contains characters that cannot be entered. Characters that can be entered are halfwidth spaces and the following halfwidth characters:

A-Z a-z 0-9 # @ \ : . ( )

(4) A folder that is not on a local disk is specified.

[Action] Cancels execution of the command.

[Workaround] Check the specified folder, and then re-execute the command. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8038-E

Command execution failed. The site server was unable to notify the management server of the list of agents managing operation logs. (command name = *command-name*)

[Cause] Possible causes include the following:

(1) The management server service has not started.

(2) A failure has occurred on the network connection to the management server.

[Action] Cancels execution of the command.

[Workaround]

(1) Execute the startservice command to start the management server service, and then re-execute the command.

(2) Remove the cause of the network failure, and then re-execute the command.

If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.

KDEX8039-E

Command execution failed. (command name = *command-name*)

[Cause] The command for deleting operation log data is not finished or has failed.

[Action] Cancels execution of the command.

[Workaround] After the command for deleting operation log data ends normally, re-execute the command.

19.3 List of events

Event number	Severity	Event
0	Information	The device has been discovered. Device type=*device-type* The following is displayed for *device-type*. • PC • Server • Network Device • Printer • Smart Device • Storage • USB Device • Display • Peripheral Device • Other Device • Unknown • (User definition)
1	Information	The device has been added as a managed node. Device type=*device-type* The following is displayed for *device-type*. • PC • Server • Network Device • Printer • Smart Device • Storage • USB Device • Display • Peripheral Device • Other Device • Unknown • (User definition)
2	Information	The status of the device has been changed to Ignored.
3	Information	The device has been deleted.
4	Warning	Failed to register the device as a managed node. You have already reached the limit of licenses available for managed devices. Purchase licenses based on the number of managed devices. Device type=*device-type* The following is displayed for *device-type*. • PC • Server • Network Device • Printer • Smart Device • Storage • USB Device • Display • Peripheral Device • Other Device

Event number	Severity	Event
4	Warning	• Unknown • (User definition)
5	Warning	The agent has been uninstalled. Confirm if agent uninstallation (from the computer) is allowed.
6	Information	The agent settings have been updated. Agent setting name=*agent-setting-name*
7	Information	Memory capacity has been changed. Before change=*memory-capacity* After change=*memory-capacity*
8	Information	Hardware has been added. Interface type=*interface-type* Model name=*model-name* Capacity=*capacity*
9	Information	Hardware has been deleted. Interface type=*interface-type* Model name=*model-name* Capacity=*capacity*
19	Warning	Failed to obtain detailed information from *function-name*. Confirm the settings (authentication information, discovery range) and the operational status of the service (JP1_ITDM_Agent Control). Or confirm the machine status of the target client. After confirmation, retry device discovery and inventory collection. If the problem persists, collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service. Cause of error=*cause-of-error* IP address=*IP-address* The following is displayed for *function-name*. • Device Discovery • Inventory Collection • On-demand inventory collection The following is displayed for *cause-of-error*. • User authentication failed • Administrative share is not accessible • An error occurred in administrative share • The client is not accessible • A communication error occurred • An error occurred in the client • Discovery program is running on the client • Discovery program did not finish
22	Information	The agent installer has been launched. Model name=*model-name* Version=*version* IP address=*IP-address*
50	Critical	The security status has been judged. The judgment result is *violation-level*. Security policy name=*security-policy-name* Update program=*violation-level-of-update-program* Antivirus software=*violation-level-of-antivirus-software* Unauthorized software=*violation-level-of-unauthorized-software* Mandatory software=*violation-level-of-mandatory-software*

Event number	Severity	Event
50	Critical	Unauthorized Windows service=*violation-level-of-unauthorized- windows-service* Security settings=*violation-level-of-security-settings* The following is displayed for *violation-level*. • Critical • Warning • Important • Safe • Unknown • Out of Target The following is displayed for *violation-level* of the target item. • Guest account settings • Vulnerable password • Password that never expires • Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services • Windows Firewall settings • Settings for Windows automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
51	Warning	The security status has been judged. The judgment result is *violation-level*. Security policy name=*security-policy-name* Update program=*violation-level-of-update-program* Antivirus software=*violation-level-of-antivirus-software* Unauthorized software=*violation-level-of-unauthorized-software* Mandatory software=*violation-level-of-mandatory-software* Unauthorized Windows service=*violation-level-of-unauthorized- windows-service* Security settings=*violation-level-of-security-settings* The following is displayed for *violation-level*. • Critical • Warning • Important • Safe • Unknown • Out of Target The following is displayed for *violation-level* of the target item. • Guest account settings • Vulnerable password • Password that never expires • Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services

Event number	Severity	Event
51	Warning	• Windows Firewall settings • Settings for Windows automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
52	Information	The security status has been judged. The judgment result is *violation-level*. Security policy name=*security-policy-name* Update program=*violation-level-of-update-program* Antivirus software=*violation-level-of-antivirus-software* Unauthorized software=*violation-level-of-unauthorized-software* Mandatory software=*violation-level-of-mandatory-software* Unauthorized Windows service=*violation-level-of-unauthorized- windows-service* Security settings=*violation-level-of-security-settings* The following is displayed for *violation-level*. • Critical • Warning • Important • Safe • Unknown • Out of Target The following is displayed for *violation-level* of the target item. • Guest account settings • Vulnerable password • Password that never expires • Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services • Windows Firewall settings • Settings for Windows automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
56	Information	Message notification to the user has been sent.
57	Warning	Failed to send a message notification to the user. Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
58	Information	Connection to the network has been denied.
60	Information	Network connection has been allowed.
62	Information	Antivirus software settings have been changed. Product name=*product-name* Engine version=*engine-version* File definition version=*file-definition-version*

Event number	Severity	Event
63	Information	Update information has been added. Update information=*update-information*
69	Information	Security policy has been added. Security policy name=*security-policy-name*
70	Information	Security policy content has been updated. Security policy name=*security-policy-name*
71	Information	Security policy has been deleted. Security policy name=*security-policy-name*
72	Information	Security policy assignment has been changed. Security policy name=*security-policy-name* Assigned group=*assigned-group*
75	Information	Software start-up has been blocked. Account name=*account-name* Account login=*account-login* Product name=*product-name* Product version=*product-version* File name=*file-name*
76	Information	Printing operation has been blocked. Account login=*account-login* Printer name=*printer-name* Printing job name=*printing-job-name*
77	Information	Printing operation has been unblocked. Account login=*account-login*
78	Warning	Failed to unblock the printing operation. Confirm whether the password is correct, and then retry unblocking the printing task. Account login=*account-login*
200#	Critical	An error occurred in the operation (JP1_ITDM_Service). The operation (JP1_ITDM_Service) will be stopped. Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service. ErrCode=*error-code*
208	Warning	An error occurred while updating received files. A temporary error occurred while received files were being updated. The update to the received files will be retried.
209	Warning	An error occurred in *function-name*. An internal error occurred in *function-name* process. If the error is repeated, then collect troubleshooting information and contact Support Service. Error code=*error-code* IP address=*IP-address* The following is displayed for *function-name*. • Device Discovery • Inventory Collection • On-demand inventory collection • Agent Deployment
210	Warning	Failed to update. Error occurred while updating received files. Failed to update file information because of an error, which occurred during file update. Temporary resource insufficiency might have occurred.

Event number	Severity	Event
210	Warning	If the error is repeated, then collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
211	Warning	Failed to update the file. The file format was invalid. Failed to update file information because of invalid file format. There is a possibility of special characters (control code etc.) in the data of the acquisition origin. Please remove special characters if you can edit the data of the acquisition origin, and acquire information again. If the error is repeated, then collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
212	Warning	Failed to update the file. The file size exceeds the database update limit. Failed to update information due to huge data. If the error is repeated, then collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
1003	Warning	The agent's operation has been stopped. The agent's operation has been stopped. The agent files might have been deleted (by the user).
1004	Information	New software has been discovered. Software name=*software-name* Version=*version*
1006	Warning	Failed to stop the prohibited operation. Service name=*service-name*
1007	Information	Antivirus software information has been added.
1008	Information	Agent patch has been updated. Agent version=*agent-version*
1009	Information	Action definition file (manager) has been updated.
1010	Information	The unregistered USB device has been disconnected. Login account name=*login-account-name* Drive name=*drive-name* Drive type=*drive-type* Device name=*device-name* Instance id=*instance-ID* The following is displayed for *device-name*. • Unknown • Local Disk • Network Drive • Removable Disk • CD-ROM Drive • RAM disk
1016	Information	Mandatory software will be distributed. Mandatory software is not installed. Distribution of the software has been requested based on the policy settings. The execution status of the task can be confirmed through *task-name*.
1017	Information	Prohibited software will be deleted. The detected software is an unauthorized software, and will be deleted based on the policy settings. Execution status of the task can be confirmed through *task-name*.
1018	Warning	Package distribution task has been terminated abnormally. Task *task-name* for agent *target-agent-host-name* has been terminated abnormally. Cause of error: *cause-of-error*

Event number	Severity	Event
1018	Warning	The following is displayed for *cause-of-error*. • Insufficient hard disk free space. • Failed to access the file or folder. • Specified computer was excluded from task execution target. • An internal error has occurred. • Failed to start the command. • Command processing has stopped. • Execution command has terminated abnormally.
1019	Warning	Unistallation task has been terminated. Task *task-name* for agent *target-agent-host-name* has been terminated abnormally. Cause of error: *cause-of-error* The following is displayed for *cause-of-error*. • Insufficient hard disk free space. • Failed to access the file or folder. • Specified computer was excluded from task execution target. • An internal error has occurred. • Failed to start the command. • Command processing has stopped. • Execution command has terminated abnormally.
1020	Information	Task *task-name* has been started according to the schedule. Task *task-name* has been started at its scheduled starting time *scheduled-starting-time*.
1021	Information	On-demand tasks has ended. On-Demand Task *task-name* has been completed. Please refer the result. Number of Error Nodes=*number-of-error-nodes*
1022	Information	An unconfirmed hardware asset (*device-type*) has been recognized. An unconfirmed hardware asset (*device-type*) has been recognized. Please register the asset. The following is displayed for *device-type*. • PC • Server • Network Device • Printer • Smart Device • Storage • USB Device • Display • Peripheral Device • Other Device • Unknown • (User definition)
1028	Information	IP Discovery is complete.
1029	Information	Active Directory synchronization is complete.
1031	Information	Operations logs backup (automatic) is complete.
1032#	Warning	An error occurred while backing up (automatic) the Operations logs. *cause-of-error*
1033	Information	Operations log restoration is complete. Restore period: *start-date-and-time-end-date-and-time*
1034	Warning	An error occurred while restoring Operations logs.

Event number	Severity	Event
1034	Warning	*cause-of-error*
1035	Warning	The Operations logs restoration may have missed some data. Skipped period: *start-date-and-time-end-date-and-time*
1036#	Critical	Failed to expand database files for Operations logs. Insufficient folder space for operation logs database. Please allocate available disk space for the folder, and then restart the service. If the error is repeated even when there is enough disk space, then collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
1037#	Warning	Failed to retrieve inventory and organizational information from Active Directory Server. *cause* Check Active Directory configurations (from AD server settings screen), using test connection. Error code=*error-code* Active Directory server hostname=*host-name* Connected port=*connected-port* Account=*account* Root path=*root-path*
1038	Information	Action definition file (agent) has been updated.
1039	Information	The Windows update will be distributed. The Windows update is not installed. Distribution of the Windows update has been requested based on the policy settings. The execution status can be confirmed through *task-name*.
1041	Warning	Because the error occurred during a distribution task to update a program, the task was ended. The downloading Windows update file failed or Windows Update File was not registered when you added Windows Update manually. Task name=*task-name*
1048	Warning	E-mail transmission with attachments has been detected. Login account name=*login-account-name* File count=*file-count* File destination information=*file-destination-information (email)*
1049	Warning	File upload to Web Server/FTP Server was detected. Login account name=*login-account-name* File count=*file-count* File destination information=*file-destination-information (destination-URL, server-name)*
1050	Warning	File Copy or File Move to a unregistered removable drive has been detected. Login account name=*login-account-name* File count=*file-count* File destination information=*file-destination-information (file-path)*
1051	Warning	Mass-Printing has been detected. Login account name=*login-account-name* Print pages=*print-pages*
1055#	Warning	Failed to collect product update information. An error occurred while connecting to the Product Update server.*cause-of-error* Please check the Product Update settings, by using Test mode.
1056#	Critical	Failed to notify System Administrators by e-mail. *cause-of-error*

Event number	Severity	Event
1056#	Critical	Please use Test Mode to check the SMTP server settings.
1057#	Warning	Available disk space is limited. Please increase available space or change the path to a disk with sufficient space. *FolderType* (*Specified folder*) Available disk space=*available disk space of the drive*
1058#	Critical	Available disk space is limited. A database failure might occur due to limited disk space. Please increase available space or change the path to a disk with sufficient space. *FolderType* (*Specified folder*) Available disk space=*available disk space of the drive*
1059	Warning	The product license will expire soon. Expiration date: *expiration-date* Please purchase a new license key.
1060	Information	Software has been added. Software=*software-name version*
1061	Information	Software has been either deleted or the software retrieval condition was changed. Software=*software-name version*
1062	Information	Software has been updated. Before change Software=*software-name version* After change Software=*software-name* Version=*version*
1063	Information	Security measures of account (*account-name*) has been applied. Item name=*item-name* The following is displayed for *item-name*. • Disable Password Never Expires • Enable Password (Screen Saver) • Set Startup Time (Screen Saver)
1064	Information	Failed to apply security measures for account (*account-name*). Item name=*item-name* The following is displayed for *item-name*. • Disable Password Never Expires • Enable Password (Screen Saver) • Set Startup Time (Screen Saver)
1065	Warning	Failed to apply security measures for the device (Account *account-name*). Violated the assigned group policy. Confirm the policy and security measure contents. Item name=*item-name* The following is displayed for *item-name*. • Disable Password Never Expires • Enable Password (Screen Saver) • Set Startup Time (Screen Saver)
1066	Information	Security settings have been changed. Item=*item-name* Before change=*value* After change=*value* The following is displayed for *item-name*. • Power-on password • Guest account • Automatic logon • Shared folder • Administrative sharing • DCOM

Event number	Severity	Event
1066	Information	• Restriction of anonymous connections • Windows Firewall settings • Windows automatic updates • Remote desktop The following is displayed for *value*. • Disabled • Enabled • None • Exist • Unknown • Permit • Not permit
1067	Information	A computer account (*account-name*) has been added. Number of days elapsed since password change=*number-of-days-elapsed* Days Unprotected password=*unprotected-password* Password never expires setting=*password-never-expires-setting* Screensaver settings=*screensaver-settings* Screensaver password settings=*screensaver-password-settings* Screensaver waiting period=*screensaver-waiting-period* The following is displayed for *unprotected-password*. • Compliant • Not Compliant The following is displayed for *password-never-expires-setting*, *screensaver-settings*, and *screensaver-password-settings*. • Disabled • Enabled
1068	Information	A computer account (*account-name*) has been deleted. Number of days elapsed since password update=*number-of-days-elapsed* Days Unprotected password=*unprotected-password* Password never expires setting=*password-never-expires- setting* Screensaver settings=*screensaver-settings* Screensaver password settings=*screensaver-password-settings* Screensaver waiting period=*screensaver-waiting-period* The following is displayed for *unprotected-password*. • Compliant • Not Compliant The following is displayed for *password-never-expiressetting*, *screensaver-settings*, and *screensaver-password-settings*. • Disabled • Enabled
1069	Information	A computer account (*account-name*) has been changed. Item=*item-name* Before change=*value-before-change* After change=*value-after-change* The following is displayed for *item-name*. • Password Strength • Password Never Expires • Screensaver settings • Password (Screen Saver) • Startup Time (Screen Saver)

Event number	Severity	Event
1069	Information	The following is displayed for *value-before-change* and *value-after-change*. • Password Strength Compliant Not Compliant • Password Never Expires, Screensaver settings, Password (Screen Saver) Disabled Enabled • Startup Time (Screen Saver)
1070	Information	Security measures has been applied. Item name=*item-name* The following is displayed for *item-name*. • Disable Guest Account • Disable Password Never Expires • Disable Auto Logon • Disable Shared Folder • Disable Anonymous Access • Enable Windows Firewall • Enable Automatic Windows Update • Disable Administrative Share • Disable DCOM • Disable Remote Desktop • Execute Windows Update • Stop and Disable Windows services
1071	Warning	Failed to apply security measures. Apply security measures after the System Administrator collects troubleshooting information and eliminates the cause of error. Item name=*item-name* The following is displayed for *item-name*. • Disable Guest Account • Disable Password Never Expires • Disable Auto Logon • Disable Shared Folder • Disable Anonymous Access • Enable Windows Firewall • Enable Automatic Windows Update • Disable Administrative Share • Disable DCOM • Disable Remote Desktop • Execute Windows Update • Stop and Disable Windows services
1072	Warning	Failed to apply security measures for the device. Violated the assigned group policy. Item name=*item-name* The following is displayed for *item-name*. • Enable Windows Firewall • Enable Automatic Windows Update • Execute Windows Update • Disable Remote Desktop
1073	Information	The start of a prohibited operation has been detected. Service name=*service-name*
1074	Information	The completion of a prohibited operation has been detected. Service name=*service-name*

Event number	Severity	Event
1075	Information	An entry to the Software List has been added.
1076	Warning	The Operations log was deleted. The operation log was deleted because the data storage duration has exceeded. Errors due to incorrect registration date or connection failure between manager and agent.
1077	Information	The network access control is enabled. Network address=*network-address*
1078	Information	The network access control is disabled. Network address=*network-address*
1079	Warning	The device has been disconnected. MAC address=*MAC-address* IPaddress=*IP-address*
1081	Information	The network access control has started.
1082	Warning	The network access control has stopped running.
1085	Warning	Failed to enable network access control. Check the error message output to the installer trace log file, and take action according to that error message. The installer trace log file is output to *%WINDIR%*\Temp\JDNNMA\JDNINS01.log on the source host. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support. (network address = *network-address*)
1086	Warning	The attempt to disable the network access control failed. Check the error message output to the installer trace log file, and then take action according to that error message. The installer trace log file is output to *%WINDIR%*\Temp\JDNNMA\JDNINS01.log on the source host. Network address=*network-address*
1087	Information	Asset information import is complete. The asset information was imported. Asset Type=*asset-type* add=*number-of-information-items* update=*number-of-information-items* error=*number-of-information-items*
1088	Warning	AMT authentication failed. (AMT power control) [AMT Settings] - [User ID] Authentication failed. To access the settings, please change the AMT credentials. http://*host-name*:16992
1089	Warning	AMT authentication failed. (AMT Settings) [AMT Settings] - [admin Password] to access the settings, please change the AMT credentials. http://*host-name*:16992
1090	Warning	Free space on the disk containing the operation log data folder has become scarce. Increase the free disk space, or change to a disk that has enough free space. Free disk space = *free-disk-space* MB
1091#	Critical	The operation log collection service stopped because there is almost no free space on the disk containing the operation log data folder. Increase the free disk space, or change to a disk that has enough free space.

Event number	Severity	Event
1091#	Critical	Free disk space =*free-disk-space* MB
1092	Warning	Free space for the site server database has become scarce. % of database used = *database-usage*%
1093#	Critical	The operation log collection service stopped because there is almost no free space for the site server database. % of database used = *database-usage*%
1094	Warning	Free space on the disk containing the data folder has become scarce. Increase the free disk space, or change to a disk that has enough free space. Free disk space = *free-disk-space* MB
1095#	Critical	A package cannot be downloaded to the site server because there is almost no free space on the disk containing the data folder. Increase the free disk space, or change to a disk that has enough free space. Free disk space = *free-disk-space* MB
1096	Information	The site server has been installed.
1097	Information	The site server has been uninstalled.
1098	Information	The site server service has started.
1099	Information	The site server service has stopped.
1100	Critical	Installation of the site server program failed. Check the error message output to the installer trace log file, and take action according to that error message. The installer trace log file is output to *%WINDIR%*\Temp\JDNINST\JDNINS01.log on the source host. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.
1101	Critical	Uninstallation of the site server program failed. Check the error message output to the installer trace log file, and take action according to that error message. The installer trace log file is output to *%WINDIR%*\Temp\JDNINST\JDNINS01.log on the source host. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support.
1103#	Critical	A database access error occurred on the site server. The database service (JP1_ITDM_DB Service) might have not started. On the site server, start the database service if it has stopped. If the problem persists, collect troubleshooting information on the site server by using the appropriate command, and then contact Customer Support. (cause = *DBMS-message*)
1104#	Critical	A fatal error occurred on the site server. The site server environment might be corrupted. If the problem persists, collect troubleshooting information on the site server by using the appropriate command, and then contact Customer Support. (error code = *internal-error-code*)
1105	Warning	Failed to enable network access control. *cause-of-error* network address = *network-address*
1106	Critical	Installation of the site server program failed. *cause-of-error*

Event number	Severity	Event
1110	Information	A smart device was locked. MDM setting name = *MDM-setting-name*
1111	Warning	Failed to lock a smart device. cause = *cause-of-error* MDM setting name = *MDM-setting-name* MDM server host name = *host-name* MDM server port number = *port number* MDM server user ID = *user-ID* proxy server IP address = *IP-address* proxy server port number = *port-number* proxy server user ID = *user-ID*
1112	Information	The password of a smart device was reset. MDM setting name = *MDM-setting-name*
1113	Warning	Failed to reset the password of a smart device. cause = *cause-of-error* MDM setting name = *MDM-setting-name* MDM server host name = *host-name* MDM server port number = *port number* MDM server user ID = *user-ID* proxy server IP address = *IP-address* proxy server port number = *port-number* proxy server user ID = *user-ID*
1114	Information	A smart device was initialized. MDM setting name = *MDM-setting-name*
1115	Warning	Failed to initialize a smart device. cause = *cause-of-error* MDM setting name = *MDM-setting-name* MDM server host name = *host-name* MDM server port number = *port number* MDM server user ID = *user-ID* proxy server IP address = *IP-address* proxy server port number = *port-number* proxy server user ID = *user-ID*
1116	Warning	Failed to delete a smart device. A database access error might have occurred. In the settings window, select [Discover Devices], [Check Discovery History], and [Managed Devices]. Then, select the devices that you want to delete, and delete them. (error code = *error-code*)
1117	Information	Synchronization of device information with the MDM system (*MDM-system-name*) is complete. MDM setting = *MDM-setting-name*
1118#	Warning	Synchronization of device information with the MDM system (*MDM-system-name*) failed. cause = *cause-of-error* MDM setting = *MDM-setting-name* MDM server host name = *host-name* MDM server port number = *port-number* user ID = *user-ID* proxy server IP address = *IP-address*

Event number	Severity	Event
1118#	Warning	proxy server port number = *port-number* proxy server user ID = *user-ID*
1120	Warning	Event notification to JP1/IM failed. Verify that JP1/Base is installed. The JP1/Base software is required for linkage with JP1/IM. If JP1/Base is installed, verify that its settings are correct. If the problem persists, collect troubleshooting information by using the appropriate command, and then contact customer support. (error code = *error-code*)
1121#	Critical	An error occurred in the service (JP1_ITDM_Service). Could not access the data folder shared between servers. *cause-of-error*
1122	Warning	The size of the collected device information exceeds the maximum size that can be sent to the management server. Device information of the maximum size that can be sent to the management server was sent to the management server. The device information that exceeded the maximum size could not be sent to the management server. When network access control is enabled, the network connection of a network adapter that meets the following conditions might be disconnected: • No network adapter information (hardware information) was sent. • The network adapter has an IP address that is not registered in the network control list. If the above conditions are met, register the adapter in the network control list by setting [Network connections] to [Permit] for all relevant IP addresses. Do not enter MAC addresses.
1123	Warning	Failed to collect device information and organization information from the Active Directory server. An error occurred during collection of device information and organization information from the Active Directory server. Collect troubleshooting information by using the appropriate command, and then contact customer support. (error code = *error-code*)
1127	Critical	The security status has been judged. The judgment result is *violation level*. Security policy name=*security-policy-name* Update program=*violation-level-of-update-program* Antivirus software=*violation-level-of-antivirus-software* Unauthorized software=*violation-level-of-unauthorized-software* Mandatory software=*violation-level-of-mandatory-software* Unauthorized Windows service=*violation-level-of-unauthorized-Windows-service* Security settings=*violation-level-of-security-settings* User-Defined Security Settings=*violation-level-of-user-defined-security-settings* The following shows the *violation levels*: • Critical • Important • Warning • Safe • Unknown • Out of Target The following shows the target items of the *violation levels*: • Guest account settings • Vulnerable password • Password that never expires

Event number	Severity	Event
1127	Critical	• Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services • Windows Firewall settings • Settings for Windows automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
1128	Warning	The security status has been judged. The judgment result is *violation level*. Security policy name=*security-policy-name* Update program=*violation-level-of-update-program* Antivirus software=*violation-level-of-antivirus-software* Unauthorized software=*violation-level-of-unauthorized-software* Mandatory software=*violation-level-of-mandatory-software* Unauthorized Windows service=*violation-level-of-unauthorized-Windows-service* Security settings=*violation-level-of-security-settings* User-Defined Security Settings=*violation-level-of-user-defined-security-settings* The following shows the *violation levels*: • Critical • Important • Warning • Safe • Unknown • Out of Target The following shows the target items of the *violation levels*: • Guest account settings • Vulnerable password • Password that never expires • Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services • Windows Firewall settings • Settings for Windows automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
1129	Information	The security status has been judged. The judgment result is *violation level*. Security policy name=*security-policy-name* Update program=*violation-level-of-update-program* Antivirus software=*violation-level-of-antivirus-software* Unauthorized software=*violation-level-of-unauthorized-software*

Event number	Severity	Event
1129	Information	Mandatory software=*violation-level-of-mandatory-software* Unauthorized Windows service=*violation-level-of-unauthorized-Windows-service* Security settings=*violation-level-of-security-settings* User-Defined Security Settings=*violation-level-of-user-defined-security-settings* The following shows the *violation levels*: • Critical • Important • Warning • Safe • Unknown • Out of Target The following shows the target items of the *violation levels*: • Guest account settings • Vulnerable password • Password that never expires • Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services • Windows Firewall settings • Settings for Windows automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
1130	Information	Processing to collect the revision history started.
1131	Information	Processing to collect the revision history is complete.
1132#	Warning	A fatal error occurred during collection of the revision history. Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
1133#	Warning	Failed to output the file for saving the revision history. *cause-of-error* For *cause-of-error*, the cause of the error is displayed depending on the situation.
1134	Information	A request to allow connections to the network was sent to JP1/NETM/NM - Manager.
1135	Warning	A request to reject connections to the network was sent to JP1/NETM/NM - Manager.
1136	Warning	Failed to reject connections to the network. *cause-of-error* The following shows the content displayed for *cause-of-error*: • JP1/NETM/NM - Manager is not installed. Make sure that JP1/NETM/NM - Manager is installed on the management server. • The JP1/NETM/NM - Manager service has not been started. Make sure that the JP1/NETM/NM - Manager service is running on the management server. • Processing stopped because an internal error occurred. If this error occurs repeatedly, contact customer support.
1137	Warning	Failed to allow connections to the network.

Event number	Severity	Event
1137	Warning	*cause-of-error* The following shows the content displayed for *cause-of-error*. • JP1/NETM/NM - Manager is not installed. Make sure that JP1/NETM/NM - Manager is installed on the management server. • The JP1/NETM/NM - Manager service has not been started. Make sure that the JP1/NETM/NM - Manager service is running on the management server. • Processing stopped because an internal error occurred. If this error occurs repeatedly, contact customer support.

#: When linked to JP1/IM, the ID displayed in JP1/IM for the JP1 event.

19.3.1 JP1 event attributes

JP1 events have two types of attributes: *basic attributes* and *extended attributes*. Basic attributes contain an event ID and a message. Extended attributes contain common information (such as the severity and user name) and program-specific information (the message details).

The table below lists the JP1 event attributes. (Note that the following legend applies to all tables in this section.)

(Legend) --: Not applicable

For event number 200

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006902
		message	--	An error occurred in the operation (JP1_ITDM_Service). The operation (JP1_ITDM_Service) will be stopped.
extended attributes	common information	severity	SERVERITY	Emergency
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service. ErrCode=*error-code*

For event number 1032

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006901
		message	--	An error occurred while backing up (automatic) the Operations logs.
extended attributes	common information	severity	SERVERITY	Alert
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR

Attribute type		Item	Attribute name	Content
extended attributes	common information	start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause-of-error*

For event number 1036

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006905
		message	--	Failed to expand database files for Operations logs.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	Insufficient folder space for operation logs database. Please allocate available disk space for the folder, and then restart the service. If the error is repeated even when there is enough disk space, then collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.

For event number 1037

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006906
		message	--	Failed to retrieve inventory and organizational information from Active Directory Server.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause* Check Active Directory configurations (from AD server settings screen), using test connection. Error code=*error-code* Active Directory server hostname=*host-name* Connected port=*connected-port* Account=*account* Root path=*root-path*

For event number 1055

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006907
		message	--	Failed to collect product update information.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	An error occurred while connecting to the Product Update server.*cause-of-error* Please check the Product Update settings, by using Test mode.

For event number 1056

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006908
		message	--	Failed to notify System Administrators by e-mail.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause-of-error* Please use Test Mode to check the SMTP server settings.

For event number 1057

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006909
		message	--	Available disk space is limited. Please increase available space or change the path to a disk with sufficient space.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time

Attribute type		Item	Attribute name	Content
extended attributes	program-specific information	message details	--	*FolderType* (*Specified folder*) Available disk space=*available disk space of the drive*

For event number 1058

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000690A
		message	--	Available disk space is limited. A database failure might occur due to limited disk space. Please increase available space or change the path to a disk with sufficient space.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*FolderType* (*Specified folder*) Available disk space=*available disk space of the drive*

For event number 1079

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006913
		message	--	The device has been disconnected.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	No setting
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_SECURITY
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	MAC address=*MAC-address* IP address=*IP-address*

For event number 1082

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006914
		message	--	The network access control has stopped running.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	NM host name

Attribute type		Item	Attribute name	Content
extended attributes	common information	product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_SECURITY
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	--

For event number 1091

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000690B
		message	--	The operation log collection service stopped because there is almost no free space on the disk containing the operation log data folder. Increase the free disk space, or change to a disk that has enough free space.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the site server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	Free disk space =*free-disk-space* MB

For event number 1093

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000690C
		message	--	The operation log collection service stopped because there is almost no free space for the site server database.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the site server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	% of database used = *database-usage*%

For event number 1095

Attribute type	Item	Attribute name	Content
basic attributes	event ID	--	0000690D

Attribute type		Item	Attribute name	Content
basic attributes		message	--	A package cannot be downloaded to the site server because there is almost no free space on the disk containing the data folder. Increase the free disk space, or change to a disk that has enough free space.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the site server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	Free disk space = *free-disk-space* MB

For event number 1103

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000690E
		message	--	A database access error occurred on the site server.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the site server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	The database service (JP1_ITDM_DB Service) might have not started. On the site server, start the database service if it has stopped. If the problem persists, collect troubleshooting information on the site server by using the appropriate command, and then contact Customer Support. (cause = *DBMS-message*)

For event number 1104

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000690F
		message	--	A fatal error occurred on the site server.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the site server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time

Attribute type		Item	Attribute name	Content
extended attributes	program-specific information	message details	--	The site server environment might be corrupted. If the problem persists, collect troubleshooting information on the site server by using the appropriate command, and then contact Customer Support. (error code = *internal-error-code*)

For event number 1118

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006912
		message	--	Synchronization of device information with the MDM system (*MDM-product-name*) failed.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	cause = *cause-of-error* MDM setting = *MDM-setting-name* MDM server host name = *host-name* MDM server port number = *port-number* user ID = *user-ID* proxy server IP address = *IP-address* proxy server port number = *port-number* proxy server user ID = *user-ID*

For event number 1121

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006911
		message	--	An error occurred in the service (JP1_ITDM_Service). Could not access the data folder shared between servers.
extended attributes	common information	severity	SERVERITY	Emergency
		issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause-of-error*

For event number 1132

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006915
		message	--	A fatal error occurred during collection of the revision history.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.

For event number 1133

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006916
		message	--	Failed to output the file for saving the revision history.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause-of-error* For *cause-of-error*, the cause of the error is displayed depending on the situation.

For event number 1135

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006917
		message	--	A request to reject connections to the network was sent to JP1/NETM/NM - Manager.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_SECURITY
		start time	START_TIME	event occurrence time

Attribute type		Item	Attribute name	Content
extended attributes	program-specific information	message details	--	--

For event number 1136

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006918
		message	--	Failed to reject connections to the network.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause-of-error* For *cause-of-error*, the cause of the error is displayed depending on the situation.

For event number 1137

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	00006919
		message	--	Failed to allow connections to the network.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	*cause-of-error* For *cause-of-error*, the cause of the error is displayed depending on the situation.

Appendix

A. Miscellaneous Information

This appendix provides miscellaneous information about using JP1/IT Desktop Management.

A.1 Port number list

This section describes the port numbers used by JP1/IT Desktop Management.

JP1/IT Desktop Management - Manager port number list

Single-server configuration:

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
31080	←	Administrator computer [ephemeral]	TCP	Used for communication from an administrator computer to a management server when the operation window is either referenced or used
31000	←	• Agent [ephemeral] • Site server [ephemeral]	TCP	Used for communication from either an agent or a site server to a management server
31006 to 31012	None	None	TCP	Used for internal processing of JP1/IT Desktop Management.

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 JP1/IT Desktop Management - Manager 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).

Multi-server configuration:

Management server

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
31080	←	Administrator computer [ephemeral]	TCP	Used for communication from an administrator computer to a management server when the operation window is either referenced or used
31000	←	• Agent [ephemeral] • Site server [ephemeral]	TCP	Used for communication from either an agent or a site server to a management server
31006	←	Database server [ephemeral]	TCP	Used for communication from a database server to a management server
31007 to 31009, 31011, 31012	None	None	TCP	Used for internal processing of JP1/IT Desktop Management.

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 JP1/IT Desktop Management - Manager 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).

Database server

Port number for database server	Connection direction	Connected to [port number]	Protocol	Use
31010		Management server [ephemeral]	TCP	Used for communication from a management server to a database server
31007	None	None	TCP	Used for internal processing of JP1/IT Desktop Management.

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 database server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if JP1/IT Desktop Management - Manager 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).

Specify settings to enable the following ports for networks between JP1/IT Desktop Management - Manager and agentless computers.

Ports used for shared files and printers:

- Protocol: TCP and UDP, Port number: 445
- Protocol: TCP, Port number: 139
- Protocol: UDP, Port number: 137 and 138

Ports used for SNMP protocol:

- Protocol: UDP, Port number: 161

Follow the steps below to specify protocol ports.

1. From the Windows Control Panel, select **Windows Firewall** and then **Advanced**.
2. In the displayed dialog box, select **Inbound Rules**, and then in the operation window, select **New Rule**.
   Follow the displayed **New Inbound Rule Wizard** to specify protocol ports.

Port number list for a site server

Port number for site server	Connection direction	Connected to [Port number]	Protocol	Use
31000		Agent or management server [ephemeral]	TCP	Used for a communication from an agent or management server to a site server
31010	None	None	TCP	Used for internal processing of a site server

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 site server, change them to port numbers that are not used.

If a site server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if a site server program 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).

Specify settings to enable the following ports for the networks between JP1/IT Desktop Management - Remote Site Server and agentless computers.

Ports used for shared files and printers:

- Protocol: TCP and UDP, port number: 445
- Protocol: TCP, port number: 139
- Protocol: UDP, port number: 137 and 138

Ports used for SNMP protocol:

- Protocol: UDP, port number: 161

Follow the steps below to specify the protocol ports.

1. From the Windows Control Panel, select **Windows Firewall** and then **Advanced**.
2. In the dialog box that appears, select **Inbound Rules**, and then in the operation window, select **New Rule**.
   Follow the displayed **New Inbound Rule Wizard** to specify the protocol ports.

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 **Remote Control Settings** in the agent configurations.
- 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 - 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

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 - Manager and JP1/IT Desktop Management - 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.2 Communication between a management server and an agent

A management server and a computer with an agent installed communicate to send or receive data. The following table describes when this communication occurs.

Category	Major actions that trigger communication
Notification about a change in the computer management status	• When the agent is installed (The information for registering the device on which the agent is installed as a managed device and changing the management type to agent management is sent immediately after installation.) • When the agent is uninstalled (The information for changing the management status to agentless management is sent.)
Automatic acquisition of inventory information	• If any changes are found in the security information, which the agent obtains according to the monitoring interval (security items), when compared to the information acquired last time. • If any changes are found in the information that excludes security information, which the agent obtains according to the monitoring interval (items excluding the security items), compared to the information obtained the last time. • When a USB device that is permitted to be used is connected to a PC (When a USB device is disconnected, or a PC is turned off with a USB device connected, the file list information is sent the next time the PC is started.) • When a USB device is disconnected, or a PC is turned off with a USB device connected (File list information is sent the next time the PC is started.)

Category	Major actions that trigger communication
Automatic acquisition of inventory information	• When the agent is stopped, such as when a PC is turned off (The information about stopping is sent.)
Application or change of agent settings information	• When the settings to be applied to the agent, such as the security policy or agent configurations, are assigned • When the settings to be applied to the agent, such as the security policy or agent configurations, are changed • When the agent is started (The agent receives the security policy or agent configurations.)
Action by an administrator	• When an administrator performs **Update Device Details** (The agent sends inventory information.) • When an administrator turns on, turns off, or restarts a user computer • When an administrator performs **Send User Notification** • When an administrator performs distribution or uninstallation • When an administrator performs remotely controlled actions
Security measures	• When security is judged (Automatically executes security measures) • When security is judged (Automatically distributes update programs that have not been applied)
Entry on the agent	• When user information is entered • When a USB device is registered • When the device information collected from a computer managed offline is sent as a notification
Operation logs or prohibited operations	• When operation logs or prohibited operations are uploaded (sent once per hour)#

#: You cannot change the interval at which operation logs or prohibited operations are uploaded. If an upload is performed while a computer with the agent installed is off, the upload finishes after the computer is turned on.

A.3 Communication between a management server and site server

The following describes when a management server and site server communicate.

Device management

- When a device is discovered

Security management

- When a security policy is created or edited
- When a security policy is assigned
- When operation logs stored on a site server is searched or referenced

Distribution management

- When a package is created
- When software is installed or files are distributed

Others

- When agent configurations are changed
- When agent programs are registered on a management server
- When an agent is delivered to a computer
- When site server programs are registered on a management server

- When a site server is installed on a computer from the operation window
- When server configuration management settings are changed
- When network monitoring agent programs are registered on a management server
- When a network monitoring agent is installed on a computer from the operation window

A.4 Communication between a site server and an agent

The following describes when a site server and an agent communicate.

Security management

- When the security policy is assigned
- When operation logs are obtained

Distribution management

When software is installed or files are distributed

Others

- When an agent is delivered to a computer
- When a site server is installed on a computer from the operation window
- When a network monitoring agent is installed on a computer from the operation window

A.5 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.

A.6 Output format of exported operation logs

The following table shows the output format of a CSV file that is output when operation logs are exported by using the `ioutils exportoplog` command.

Output item	Output format	Maximum number of bytes of the output character string[#1]
Suspicious Operation	Either Warning or FALSE is output.	8
Operation Date/Time	The date and time are output in the following format: YYYY/MM/DD hh:mm:ss[#2]	19
Source	A character string of 256 or fewer characters is output.	1,024
User Name	A character string of 1,024 or fewer characters is output.	4,096
Operation Type	One of the following is output: • Power On/Shutdown/Logon/Logoff • Process/Program Operation • File Operation • Print Operation • External Media Operation • Web Access • Shut Down	88
Operation Type (Detail)	One of the following is output: • Power On • Shutdown • Log On • Log Off • Block Program Activation • Process Execution • Process Termination • Copy file • Move file • Rename file • Create file • Delete file • Copy folder • Move folder • Rename folder • Create folder • Delete folder • Web Access (Upload) • Web Access (Download) • FTP (Send File) • FTP (Receive File) • Send Mail (Attachment File) • Receive Mail (Attachment File) • Save Attached File • Print • Block Printing • Attach External Device • Detach External Device • Block Attached External Device	56

Output item	Output format	Maximum number of bytes of the output character string[#1]
Operation Type (Detail)	• Web Access • Change active window	56
File Created Date/Time	The date and time are output in the following format: YYYY/MM/DD hh:mm:ss[#2]	19
File Last Modified Date/Time	The date and time are output in the following format: YYYY/MM/DD hh:mm:ss[#2]	19
File Size	A number is output that includes a decimal point and to which one of the following units is added: B, KB, MB, GB, TB, or PB. The maximum value is 8,191 PB.	6
Original File Drive Type	One of the following is output: • Local Disk • Network Drive • Removable Disk • CD-ROM • RAM Disk • Web • FTP • Email • Other	40
Original File Created Date/Time	The date and time are output in the following format: YYYY/MM/DD hh:mm:ss[#2]	19
Source File Information[#3]	A character string of 2,083 or fewer characters is output.	8,332
Source File Drive Type	One of the following is output: • Local Disk • Network Drive • Removable Disk • CD-ROM • RAM Disk • Web • FTP • Email • Other	40
Destination File Information[#3]	A character string of 2,083 or fewer characters is output.	8,332
Destination File Drive Type	One of the following is output: • Local Disk • Network Drive • Removable Disk • CD-ROM • RAM Disk • Web • FTP • Email • Other	40
User Name (Run As)	A character string of 1,024 or fewer characters is output.	4,096

Output item	Output format	Maximum number of bytes of the output character string[#1]
File Name	A character string of 520 or fewer characters is output.	2,080
Software Name	A character string of 512 or fewer characters is output.	2,048
Software Version	A character string of 128 or fewer characters is output.	512
File Version	A character string of 20 or fewer characters is output.	80
Process Name	A character string of 520 or fewer characters is output.	2,080
External Drive Type	One of the following is output: • Local Disk • Network Drive • Removable Disk • CD-ROM • RAM Disk • Other	40
External Drive Name	A drive name in the range from `A:\` to `Z:\` is output.	3
Serial #	A character string of 256 or fewer characters is output.	1,024
External Device Type	A character string of 1,024 or fewer characters is output.	4,096
External Device Name	A character string of 1,024 or fewer characters is output.	4,096
External Device Instance ID	A character string of 1,024 or fewer characters is output.	4,096
Printed Document Name	A character string of 1,024 or fewer characters is output.	4,096
Printer Name	A character string of 1,024 or fewer characters is output.	4,096
Printed Page Count	An integer that is equal to or less than 2,147,483,647 is output.	10
URL	A character string of 2,083 or fewer characters is output.	8,332
Web Page Title	A character string of 1,024 or fewer characters is output.	4,096
Window Title	A character string of 512 or fewer characters is output.	2,048

#1: This is the maximum number of bytes if either UTF-8 or UTF-16 is specified for the character encoding during execution of the `ioutils exportoplog` command. A half-width alphanumeric character or symbol is counted as 1 byte. For other characters, a character is counted as 4 bytes.

#2: YYYY: year, MM: month, DD: day, hh: hour, mm: minute, ss: second

#3: If Operation Type (Detail) is Send Mail (Attachment File), Receive Mail (Attachment File), or Save Attachment File, `\r\n` (return code) is converted to \n, and then the data is output.

Related Topics:

- 17.16 ioutils exportoplog (exporting operation logs)

A.7 Setting fields in the import file for the definitions of common management fields and additional management fields

When you edit the import file for the definitions of common management fields and additional management fields, you need to enter a value for certain fields according to the purpose of the edit. The following table shows such fields for each purpose of an edit.

Purpose of the edit	Update category#1	Asset management field type	Update-field language key	Update field	Multilingual settings	*nn* - Setting value (before change)#2	*nn* - Setting value (after change)#2	*nn* - Explanation#2
Add a hierarchical field	Y	Y	Y	Y	Y	N	A#3	N
Change a hierarchical field	Y	Y	Y	Y	Y	Y	Y	A
Delete a hierarchical field	Y	Y	Y	Y	--	Y	--	--
Add an enumeration field	Y	Y	Y	Y	Y	N	A#3	A#4
Change an enumeration field	Y	Y	Y	Y	Y	Y	Y	A
Delete an enumeration field	Y	Y	Y	Y	--	Y	--	--

Legend: Y: You must enter a value. A: Enter a value as necessary. N: You must not enter a value. --: The entered value is ignored.

#1: For the update category, enter a value as follows:

- If adding an item: A
- If changing an item: U
- If deleting an item: D

#2: The import file is output with these 3 columns added as many times as the number of language types that are set in the **Edit Other Language Settings** dialog box. *nn* is an abbreviation for the specified language type. For example, ja and en.

#3: You cannot omit a value for the default language. If you omit a value for a language other than the default language, the same value as the default language is set for that language.

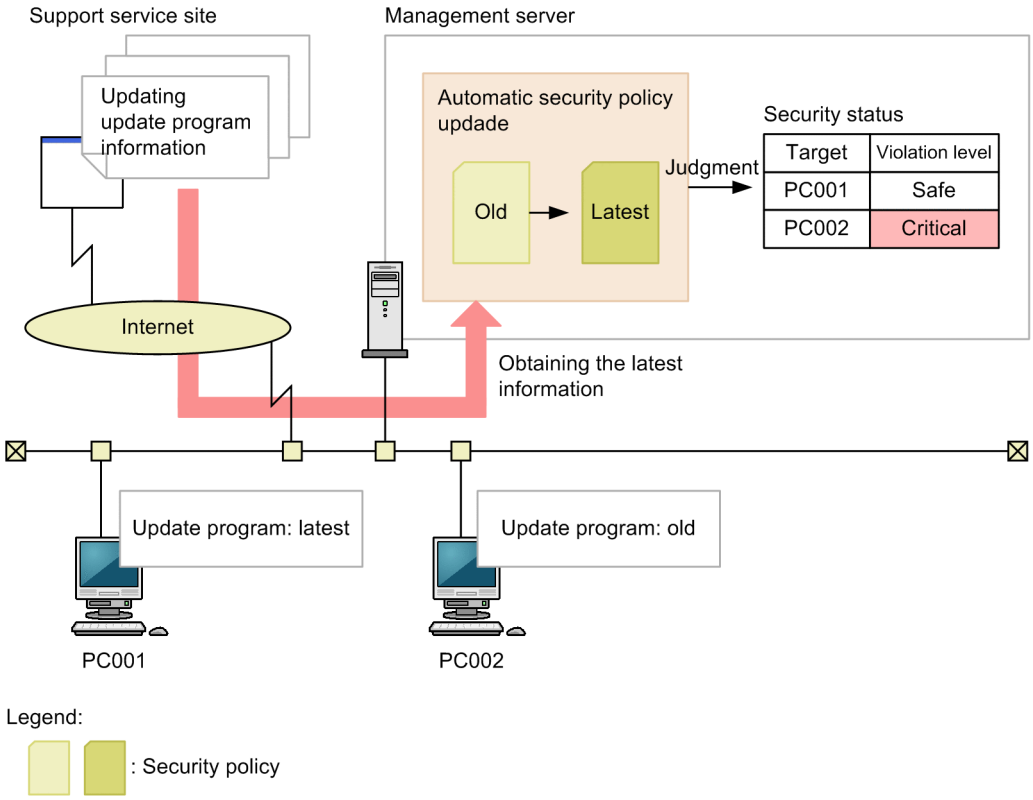
#4: If you omit a value for the default language, a null character is set. If you omit a value for a language other than the default language, the same value as the default language is set for that language.

A.8 Obtaining information from the support service

If you have a contract with the support service, you can obtain information about update programs from the support service to update the information within JP1/IT Desktop Management.

(1) Automatically obtaining information from the support service

A management server regularly (once a day by default) checks whether information about update programs has been updated. The following figure describes the workflow from acquisition of update program information to the update of the security policy after the update program information has been updated.



Important note

To automatically obtain update information from the support service, the following conditions must be met:

- You have a contract with the support service.
- A management server can connect to the Internet.

(2) Updating information from the support service offline

If a management server cannot connect to the Internet, an administrator connects to the support service by using a computer that can be externally connected, and then downloads information from the support service. Registering the downloaded information on the management server updates the information of the management server. Check the support service site regularly, and if there is any new information available, perform an offline update.

There are two ways of updated information from the support service offline.

Updating offline from the operation window

Perform an update from the operation menu of one of the following: the **Update List** view in the Security module, the **Managed Software List** view in the Assets module, or the **Software List** view in the Device module.

Updating offline by executing a command

Execute the `updatesupportinfo` command to update. For details, see 17.22 updatesupportinfo (uploading support service information).

(3) Information obtainable from the support service

The following table describes the information you can obtain from the support service.

Obtainable information		Description
Update program information	Update program name	The name of an update program
	Security information number	The security information number of an update program
	Security severity	The importance of an update program. It is either "Critical" or "Important".
	Update type	The type of an update program
	URL	A URL of Microsoft Japan. You can find details about update programs here.
	Description	A description of an update program
	Release date	The date on which an update program was released
	Target product	Names of products affected by the update program
	Service pack	An OS service pack selected in **Support OS**
	Target type	Target products, versions, and service packs
	Execution file download URL	The URL from which the update program is downloaded

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. A restart is required in the following cases:

- When JP1/IT Desktop Management - Manager is installed (in Windows XP Professional Service Pack 2 or 3)
- When a security policy is edited or assigned
- When security measures are manually performed

When JP1/IT Desktop Management - Manager is installed (in Windows XP Professional Service Pack 2 or 3)

Restart the computer on which JP1/IT Desktop Management - Manager is installed. Installation is complete after the restart. If, however, the functionality to trace the flow of processing for other Hitachi products (HNTRLib2) is installed on the computer, you do not need to restart the computer.

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, Windows XP, and Windows 2000.
- Auto enforce of Disable DCOM (OS Security)
- Auto enforce of Disable Remote Desktop (OS Security)
- External Device Restriction (Other Access Restrictions)
- Enable or disable Acquisition of Operations Logs (including acquisition of Suspicious Operations to be Notified) (Operation Logs)

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.

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, Windows XP, and Windows 2000.
- Disable DCOM (OS Security)
- Disable Remote Desktop (OS Security)

A.10 Displayed date and time

The date and time displayed in JP1/IT Desktop Management differ by function. The following table shows the types of local time used for display.

Local time displayed for functions that are not described in this table is based on the following: If a function is performed or used by a management server, the local time of the management server is used. If a function is performed or used by a computer with the agent installed, the local time of the computer with the agent installed is used.

Function		Displayed date and time		Description
		Local time of management server	Local time of computer with agent installed	
Device management	Registered Date/Time	Y	N	Registered Date/Time is the date and time at which device information is registered on the management server. This date and time is not updated.

Function		Displayed date and time		Description
		Local time of management server	Local time of computer with agent installed	
Device management	Managed Date/Time	Y	N	Managed Date/Time is the date and time at which a computer becomes subject to management.
	Last Modified Date/Time	Y	Y	Last Modified Date/Time is the date and time at which device information is updated. For the date and time at which device information of a management server is updated, the local time of the management server is displayed. For the date and time at which device information of a computer with an agent installed is updated, the local time of that computer is displayed. If device information is last updated via information notification by external storage media, the date and time at which the information notification is collected is displayed. The local time of a computer with an agent installed that is managed offline is displayed.
	Last Alive Confirmation Date/Time	Y	N	Last Alive Confirmation Date/Time is the date and time at which you last confirmed a connection from a computer to a management server. The local time of the management server is displayed here. If the last connection was used for an information notification by external storage media, the date and time is not updated. The date and time before the notification remain.
Calculate	Operation Date/Time	N	Y	The local time of a computer with an agent installed is used for, for example, software startup blocking or operation logs for the computer with an agent installed.
	Calculate Date/Time	Y	N	Calculations are performed at the local time of a management server.
Events	Registered Date/Time	Y	N	Registered Date/Time indicates the date and time at which an event occurrence is registered on a management server. The local time of the management server is displayed here.
Schedule executed by a management server	The following schedules, which you can specify by selecting **Configurations** from **Discovery** in the Settings module: • Active Directory • IP Address Range	Y	N	A search is performed at the local time of a management server.
	The schedules that you specify by selecting **Security Schedule** from	Y	N	The security status is judged at the local time of a management server.

Function		Displayed date and time		Description
		Local time of management server	Local time of computer with agent installed	
Schedule executed by a management server	**Security management** in the Settings module.	Y	N	The security status is judged at the local time of a management server.

Legend: Y: Displayed, N: Not displayed

Important note

While JP1/IT Desktop Management is running, do not revert the date and time on any of the computers that make up a JP1/IT Desktop Management system. Changing the date and time might cause a failure in functions that work according to the set date and time.

A.11 Outputting audit logs

Audit logs in JP1/IT Desktop Management indicate who executed what operations, as well as when and from where those operations were executed. You can use audit logs to evaluate and assess internal controls. Note that the information necessary for running JP1/IT Desktop Management is stored in the audit logs.

(1) Types of events output to audit logs

The following table describes the types of events that are output to audit logs and when JP1/IT Desktop Management outputs audit logs. Events to be output to audit logs are classified by an event type identifier.

Event type	Description	When JP1/IT Desktop Management outputs audit logs
StartStop	This event type indicates that this is an audit log related to the start and end of software.	• Start and end of the JP1/IT Desktop Management - Manager service • Startup failure of the JP1/IT Desktop Management - Manager service • Abnormal end of the JP1/IT Desktop Management - Manager service
Authentication	This event type indicates that this is an audit log related to the authentication results of a JP1/IT Desktop Management - Manager user.	• Success or failure in login to JP1/IT Desktop Management - Manager • Logout from JP1/IT Desktop Management - Manager
ConfigurationAccess	This event type indicates that this is an audit log related to operations performed by an administrator, such as a user account registration or agent setup.	• Registration or removal of user accounts • Locking or unlocking of user accounts • Permission changes • Normal or abnormal end during setup of JP1/IT Desktop Management - Manager • Normal or abnormal end to agent setup • Normal or abnormal end in license information registration

Event type	Description	When JP1/IT Desktop Management outputs audit logs
ConfigurationAccess	This event type indicates that this is an audit log related to operations performed by an administrator, such as a user account registration or agent setup.	• Success or failure in setting an ID and password for the support service site • Success in setting or removing a search authentication ID and password • Success or failure in setting an ID and password for AMT linkage • Success in setting or removing an ID and password for connecting to Active Directory • Success or failure in setting an ID and password for connecting to a mail server • Success in setting an ID and password for connecting to an operation log storage folder when the folder is located on a network • Success or failure in adding MDM settings • Success or failure in changing an ID or password for a MDM settings server or proxy • Success or failure in removing MDM settings • Normal or abnormal end to configuration of revision history • Success or failure in setting an ID and password for connecting to the output folder for saving the revision history • Success or failure in changing the automatic update of the network filter list • Success or failure in setting the JP1/NETM/NM - Manager linkage
ExternalService	This event type indicates that this is an audit log related to the results of communication with external services such as Active Directory, mail sending, and the support service site.	• Success or failure in connecting to Active Directory • Success or failure in connecting to JP1/NETM/NM • Success or failure in sending mail • Success or failure in connecting to the support service site • Success or failure in connecting to MDM products
ContentAccess	This event type indicates that this is an audit log related to operations such as changing the security policy, exporting device information, or collecting information from the support service.	• Normal or abnormal end of the security policy change • Success or failure in exporting device information • Success in importing and exporting asset information • Failure in importing and exporting asset information • Success or failure in adding update programs

Event type	Description	When JP1/IT Desktop Management outputs audit logs
ContentAccess	This event type indicates that this is an audit log related to operations such as changing the security policy, exporting device information, or collecting information from the support service.	• Success or failure in adding antivirus software information • Success or failure in updating action definition files by an administrator • Success or failure in updating the agent • Success or failure in recreating the site server database • Success or failure in removing operation logs
Maintenance	This event type indicates that this is an audit log related to database operation.	• Success or failure in backing up databases • Success or failure in restoring databases • Success or failure in reorganizing databases
ManagementAction	This event type indicates that this is an audit log related to the following: the results of judgment and of executing action items for security status, and the results of executing action items for smart devices.	• The results of judgment and of executing action items for security status • Results of executing action items for smart devices

(2) Audit log output format

The items of an audit log are output in the following order: "CALFHM", which indicates the output is in the audit log format, the revision number of the audit logs, and related output items. The following table describes the values and details of items output to audit logs.

Output item		Value	Description
Item name	Output attribute name		
Common specification identifier	--	CALFHM	This identifier indicates that the output is in audit log format.
Common specification revision number	--	1.0	The revision number is used to manage audit logs.
Sequence number	seqnum	Sequence number	Sequence number for audit logs
Message ID	msgid	An ID of a message that has been made public	A message ID for each product
Date and time	date	Log output date and time	*YYYY-MM-DDThh:mm:ss.sssTZD* • *YYYY*: year (4-byte number) • *MM*: month (2-byte number) • *DD*: date (2-byte number) • *T*: delimiter (fixed) • *hh*: hour (2-byte number) • *mm*: minute (2-byte number) • *ss*: second (2-byte number) • *sss*: millisecond (3-byte number)

Output item		Value	Description
Item name	Output attribute name		
Date and time	date	Log output date and time	• *TZD*: time zone
Program name	progid	JP1/ITDM	The name of the product in which an event occurred
Component name	compid	One of the following is output: • Installer • Setup • Gui • Api • ManagerService • Utility • AgentControl • Agent	The name of the component in which an event occurred
Process ID	pid	An ID of a process	The process ID that detected the occurrence of an event
Location	ocp:ipv4 or ocp:host	The IP address or computer name of a management server	An IP address or host computer name of the server on which an event occurred
Audit event type	ctgry	One of the following is output: • StartStop • Authentication • ConfigurationAccess • ExternalService • ContentAccess • Maintenance • ManagementAction	This identifier classifies events to be output to audit logs.
Audit event results	result	One of the following is output: • Success • Failure • Occurrence (other than success or failure)	Results of events that occurred
Subject identifier	subj:uid or subj:euid	A user account or Administrator	Information about the user who caused an event to occur
Object information	obj	One of the following is output: • User (user account) • Role (permissions) • Setup (JP1/IT Desktop Management - Manager setup) • Config (agent configuration) • Policy (security policy) • DeviceInfo (device information) • DataBase (database) • UpdateInfo (update program information) • AntivirusInfo (antivirus software information) • ActionDefinition (JP1/IT Desktop Management - Manager action definition file)	Information about the object that caused an event to occur

Output item		Value	Description
Item name	Output attribute name		
Object information	obj	• Agent • AssetInfo (asset information)	Information about the object that caused an event to occur
Action information	op	One of the following is output: • Start • Stop • Login • Logout • Add • Update • Delete • Request • Response • Import • Export • Install • Uninstall • Backup • Maintain (reorganization) • Recovery (restore)	Action information about the user who caused an event to occur
Permissions information	auth	Either of the following is output: • User permissions for JP1/IT Desktop Management • Administrator (OS permissions)	Permissions information is not output if permissions have not been obtained.
Request source	from:ipv4	An IP address of a computer that performs operations in an operation window	The IP address of the server on which an event occurred
Message text	msg	Any message	A message that describes an event in detail

Legend: --: Not applicable

(3) Audit log save format

This section describes the save format for audit logs. Audit logs are output to JDNAUDTn.LOG (where n is a number in the range from 1 through 9).

When the size of a given log file (JDNAUDTn.LOG) reaches a certain level, audit logs are output to a different output file. For example, when the size of JDNAUDT1.LOG reaches a certain level, audit logs are then output to JDNAUDT2.LOG. In this way, output files for audit logs change sequentially. When the size of JDNAUDT9.LOG reaches a certain level, the existing audit logs stored in JDNAUDT1.LOG are deleted, and new audit logs are output to JDNAUDT1.LOG, restarting the sequence.

A.12 Amendments for each version

Amendments for version 10.01

- The following information was combined into the Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management Overview and System Design Guide:

- A description of Microsoft products
- Icons and formats used in the manual
- Online Help
- Related manuals
- Related documents
- Notations used in the manual
- Abbreviations used in the manual
- Conventions, e.g., KB (kilobyte)
- Glossary

- Windows 8 and Windows Server 2012 were added as applicable OSs for JP1/IT Desktop Management - Agent.
- Description about using Autorun.inf to enable an installation to start automatically when a CD-R is used as the media for installing the agent was added.
- Computers that are not connected to the management server via a network can now be managed by using the offline management functionality.
- Descriptions about suspicious operations such as taking out files without permission or printing out files causing windows to be displayed differently and requiring different ways to investigate the issue were added.
- Notes about the `recreatelogdb` command were corrected.
- Notes about operating JP1/IT Desktop Management windows in Internet Explorer 9 were added.
- Methods for taking action when messages such as "Abnormal request" or "Unexpected error" is displayed when the user logs in or opens the operation window were added.
- Procedures for editing the agent configurations for the computer that enables the site server or network monitoring were added.
- JP1/IT Desktop Management information can now be updated by obtaining the support service information.
- Methods for setting MDM system linkage information were corrected.
- Reference information when registering JP1/IT Desktop Management commands as Windows tasks was corrected.
- Description about the server that can execute the `ioutils exportoplog` command was corrected.
- Software types, the purchasing status for some installed software, and product IDs can now be managed while managing assets.
- Notes about an error message (KDEX4041-E) that is output when executing the `getlogs` command was added.
- A description about reference information when installing the agent by copying a disk without executing the `resetnid.vbs` command was improved.
- The following messages were added:
  KDEX1005-W, KDEX1036-W, KDEX1076-E, KDEX1077-E, KDEX1078-W, KDEX1543-E, KDEX1581-E, KDEX1582-W, KDEX1583-W, KDEX1584-E, KDEX1587-Q, KDEX1588-Q, KDEX1589-Q, KDEX1590-E, KDEX1591-W, KDEX1592-E, KDEX1593-E, KDEX1594-E, KDEX3029-E, KDEX3030-I, KDEX3299-I, KDEX3300-E, KDEX3301-I, KDEX3302-E, KDEX3303-I, KDEX3304-E, KDEX4074-E, KDEX4075-E, KDEX4076-E, KDEX4202-E, KDEX4203-E, KDEX4215-Q, KDEX4216-Q, KDEX4233-E, KDEX4270-I, KDEX4287-E, KDEX5104-I, KDEX5396-I, KDEX5397-E, KDEX5399-E, KDEX5400-E, KDEX5401-E, KDEX5402-I, KDEX5403-E, KDEX5404-E, KDEX5405-E, KDEX5406-E, KDEX5407-E, KDEX5409-E, KDEX5410-I, KDEX5411-E, KDEX5412-E, KDEX5413-E, KDEX5414-E, KDEX5415-E, KDEX5417-E, KDEX5418-I, KDEX5419-E, KDEX5420-E, KDEX5421-E, KDEX5422-E, KDEX5423-E, KDEX5425-E, KDEX5426-E, KDEX5427-E, KDEX5428-E, KDEX5430-E, KDEX5431-I, KDEX5432-I, KDEX5434-E, KDEX5435-E, KDEX5436-E, KDEX5440-E, KDEX5450-E, KDEX5451-E, KDEX5452-E, KDEX5453-E,

KDEX5454-E, KDEX5455-E, KDEX5456-E, KDEX6119-E, KDEX6151-E, KDEX6152-E, KDEX6511-E, KDEX8031-I, KDEX8032-W, KDEX8033-E, KDEX8034-E, KDEX8035-W, KDEX8036-E, KDEX8037-E, KDEX8038-E, and KDEX8039-E.

- The following messages were changed:
  KDEX1505-E, KDEX1506-E, KDEX4020-E, KDEX4023-E, KDEX4073-I, KDEX4085-I, KDEX4100-E, KDEX4204-E, KDEX4220-E, KDEX4221-E, KDEX4295-E, KDEX4378-Q, KDEX5000-I, KDEX5010-W, KDEX5071-W, KDEX5336-I, KDEX5337-E, KDEX5338-E, KDEX5339-E, KDEX5340-I, KDEX5341-E, KDEX5342-E, KDEX5346-E, KDEX5385-I, KDEX5386-E, KDEX5387-E, KDEX5388-E, KDEX5389-I, KDEX5390-E, KDEX5391-E, KDEX5392-E, KDEX5393-E, KDEX5394-E, KDEX6112-E, KDEX6113-E, KDEX6115-E, KDEX6132-E, KDEX8003-I, KDEX8006-E, KDEX8019-E, KDEX8022-W, KDEX8024-W, KDEX8028-E, and KDEX8030-E.
- The following events were added:
  1105, 1106, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1120, 1121, 1122, and 1123.
- IDs that are displayed in JP1/IM as JP1 events when linked with JP1/IM were added.
- Event 1118 is now output to JP1/IM as a JP1 event when linked with JP1/IM.
- Attributes for JP1 events were added.
- Port numbers that are used in JP1/IT Desktop Management - Manager are described separately for single-server and multi-server configurations.
- A description was added about the fact that when the power of a computer with an agent installed is turned off while operation logs about prohibited operations are being uploaded, the operation logs are uploaded after the computer is turned on.
- You can now manage a maximum of 50,000 devices when operating a system in a multi-server configuration.
- Information to be displayed or operations to be executed can now be controlled in accordance with work responsibilities specified for user accounts.
- Writing to FD drives and removable disks can now be suppressed.
- You can now link with JP1/IM to send notifications concerning JP1 events.
- The list in the operation window can now be displayed on each page.
- The methods for applying and canceling simple filters were changed.
- The following was added: A procedure to revert the security configuration items of a managed computer, which had been changed due to application of a security policy or security auto enforce, to the state before the change.
- A solution for the following was added: When installing an agent by copying a disk, multiple devices are recognized as a single device.
- A method was added to remove a device from the network control list that was automatically added to the list.
- A description of the following was added: If you removed a device discovered by the network monitoring functionality, to rediscover the device, you must disconnect from and then reconnect to the network.
- The targets of the network monitoring functionality were added.
- The following description was added: If you install an agent in Windows 2000, Windows XP, or Windows Server 2003, in the **Agent Configurations** view, which you can select from **Agent** in the Settings module, the settings for **Set the account to install Agent.** are enabled.
- Notes on device discovery and agent delivery were changed for the following case: The network settings prevent unregistered devices from connecting to the network.
- The URL of the login window for JP1/IT Desktop Management was added.

- The following description was added: A timeout occurs if you have not clicked the **OK** button in the JP1/IT Desktop Management dialog box after 60 minutes or more.
- The following description was added: Changing the **Host Name** of device information linked to hardware asset information does not automatically change **Device Name** in the hardware asset information.
- The following description was added: Among the asset status or contract status information added by a system administrator, the asset status or contract status information that was saved as filter conditions cannot be removed.
- The following description was added: Serial numbers that can become mapping keys when imported are classified as BIOS information.
- The following description was added: The data type of **Department** or **Location** can be changed, but the data type of other added asset management items cannot be changed after it is specified.
- The following was added: The time required to generate a new host name after the `resetnid.vbs` is executed.
- Device information can now be exported by using the `ioutils exportdevice` command.
- Detailed device information can now be exported by using the `ioutils exportdevicedetail` command.
- Notes on IP addresses and MAC addresses to be registered in the network control list were added.
- Port numbers of the controller and remote control agent were modified.
- Situations in which communication between a management server and an agent occur were corrected.
- The description of the following was corrected: Timing at which a management server checks whether the update program information has been updated.
- The conditions for automatically obtaining update information from the support service site were corrected.
- The following description was added: If you edit **External Device Restriction** in **Other Access Restrictions** in the security policy, you must restart the computer to which the security policy is assigned.
- The following was corrected: Details of event types output to audit logs, and the timing at which JP1/IT Desktop Management outputs audit logs.
- The following items were added to the values output as object information in audit logs:
  - UpdateInfo (update program information)
  - AntivirusInfo (antivirus software information)
  - ActionDefinition (JP1/IT Desktop Management - Manager action definition file)
  - Agent
  - AssetInfo (asset information)
- The values output as the request source for an audit log were corrected.
- The description of the audit log save format was corrected.
- You can now link with an MDM product to manage smart devices.
- The total number of devices with software installed (Number of Used Licenses) is now displayed in the managed software information.
- The timing at which you are asked to change your password at login was added. In addition, the following description was added: You must change your password at login after 180 days of setting it.
- A procedure for logging out was added.
- A procedure for releasing a user account lock was added.
- The icon for editing definitions for departments and locations from the menu area was changed. In addition, procedures for adding, editing, and removing definitions for departments and locations were added.

- Names of departments and locations can now be changed from the menu area. In addition, a procedure for changing the names of departments and locations was added.
- A procedure for removing departments and locations was added.
- The following note was added: In a network segment for which network monitoring is disabled, even if **Deny** is displayed for **Connection to Network**, the network connection is not blocked.
- The following description was added: When action items for network control are specified, reconnecting to a network from a computer with an agent installed is controlled according to the security judgment.
- A description about registration of USB devices was added for the following cases: Registering USB devices that are recognized by vendors and registering USB devices that are recognized individually.
- Unnecessary operation logs can now be removed by using the `deletelog` command.
- The following description was added: If a CSV file for hardware asset information contains blank values, items with blank values are not updated after import.
- The following description was added: If a hyphen (-) is displayed in the information area, blank values are output after export.
- The following description was added: a user ID used in authentication for Windows administrative share must be specified in the following format if the ID is to be authenticated as a domain user: User ID@FQDN (fully qualified domain name), or Domain name\user ID.
- A procedure for specifying display names of departments and locations for each language was added.
- The following description was added: the `ioutils importfield` command can add items only by importing. Events with event numbers from 1085 through 1116 were added to the events for which action needs to be taken.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W