HITACHI
Inspire the Next

JP1 Version 12

JP1/IT Desktop Management 2 Administration Guide

3021-3-E14-30(E)

Notices

■ Relevant program products

For details about the supported operating systems and the service packs or patches that are required by JP1/IT Desktop Management 2, see the *Release Notes*.

P-2A42-78CL JP1/IT Desktop Management 2 - Manager 12-60

The above product includes the following:

• P-CC2A42-7ACL JP1/IT Desktop Management 2 - Manager (for Windows Server 2019, Windows Server 2016, Windows Server 2012)

• P-CC2A42-7BCL JP1/IT Desktop Management 2 - Agent (for Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

• P-CC2A42-7CCL JP1/IT Desktop Management 2 - Network Monitor (for Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1 Enterprise, Windows 8.1 Pro, Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate)

• P-CC2A42-7DCL JP1/IT Desktop Management 2 - Asset Console (for Windows Server 2019, Windows Server 2016, Windows Server 2012)

• P-CC2A42-7PCL JP1/IT Desktop Management 2 - Internet Gateway (for Windows Server 2019, Windows Server 2016, Windows Server 2012)

P-2A42-7KCL JP1/IT Desktop Management 2 - Operations Director 12-60

The above product includes the following:

• P-CC2A42-7ACL JP1/IT Desktop Management 2 - Manager (for Windows Server 2019, Windows Server 2016, Windows Server 2012)

• P-CC2A42-7BCL JP1/IT Desktop Management 2 - Agent (for Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

• P-CC2A42-7CCL JP1/IT Desktop Management 2 - Network Monitor (for Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1 Enterprise, Windows 8.1 Pro, Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate)

• P-CC2A42-7PCL JP1/IT Desktop Management 2 - Internet Gateway (for Windows Server 2019, Windows Server 2016, Windows Server 2012)

■ Trademarks

HITACHI, HiRDB, Job Management Partner 1, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

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

BSAFE is a trademark or registered trademark of Dell Inc. in the United States and other countries.

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

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

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

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

Windows Media 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.

XenApp is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

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.

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/).

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

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

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

This product includes software developed by Andy Clark.

This product bundles Dell BSAFE™ software developed by Dell Inc. in the United States.

Java is a registered trademark of Oracle and/or its affiliates.

Java is a registered trademark of Oracle and/or its affiliates.

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

```
LICENSE ISSUES
==============
The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.
OpenSSL License
---------------
/* ====================================================================
* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
```

```
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----------------------
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
```

```
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given
attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
```

```
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

■ 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

January 2022: 3021-3-E14-30(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-E14-30(E)) and product changes related to this manual.

Changes	Location
The **All Assets Cost** report, which totals the cost values of hardware assets, software license, and other, was added to **Asset Detail Reports**.	1.12.1, 11.3.1
Maximum of 300,000 devices can be managed.	1.17, 6.39
Software information can now be searched for at any time with the `softwaresearch` command.	17.3, 17.46
Operation Date/Time (UTC) was added to the information items to be collected in the operation log.	17.20, Appendix A.4

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

Preface

This manual explains and gives examples of how to use JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Operations Director. Herineafter, JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Operations Director are abbreviated to JP1/IT Desktop Management 2 .

Compared with JP1/IT Desktop Management 2 - Manager, some of the functions of JP1/IT Desktop Management 2 - Operations Director are restricted. For details about functional restrictions, see the description about the functional restrictions of JP1/IT Desktop Management 2 - Operations Director in the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

For details about the latest notes, see the Release Notes.

■ Intended readers

This manual is intended for:

- Administrators who manage security and assets in an organization using JP1/IT Desktop Management 2.
- Readers who want to know how to use and operate JP1/IT Desktop Management 2.

■ Organization of this manual

This manual is organized into the following chapters and appendix:

1. Managing Computers by Using JP1/IT Desktop Management 2

   This chapter explains how to operate and utilize JP1/IT Desktop Management 2.

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 of JP1/IT Desktop Management 2.

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 2.

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 2.

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 2 commands.

18. Troubleshooting

This chapter describes the actions to be taken when a problem occurs during operation of JP1/IT Desktop Management 2.

19. Events

This chapter lists and describes the JP1/IT Desktop Management 2 events.

Appendix A. Miscellaneous Information

Appendix A provides reference material for using JP1/IT Desktop Management 2.

For reference materials when reading this manual, see the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

Contents

1 Managing Computers by Using JP1/IT Desktop Management 2

This chapter describes how to manage computers by using JP1/IT Desktop Management 2.

1.1 Installing agents

Install agents on computers to be managed by JP1/IT Desktop Management 2.

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.

On agents for UNIX, you cannot determine the security status or automatically correct any detected security problems. On agents for Mac, problems cannot be corrected automatically.

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.

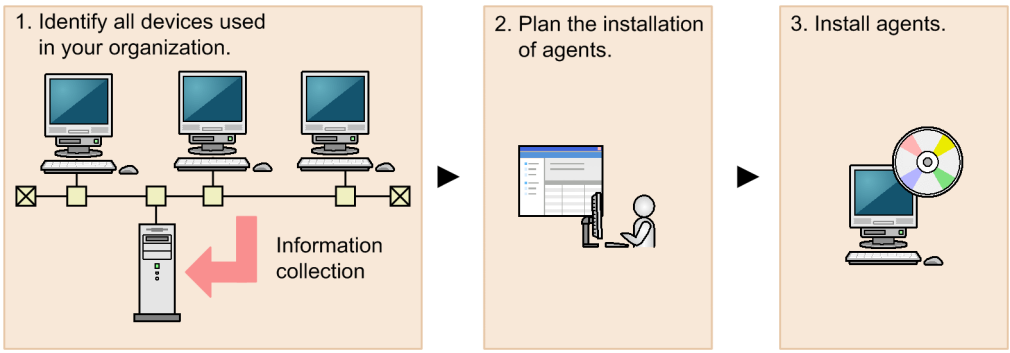
For distribution of software or files to agents for UNIX or Mac, use the Remote Install Manager.

If you are using JP1/IT Desktop Management 2 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 2 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 2, 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 2 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. You can search for devices registered in Active Directory.

In the Settings module, select **General**, and then **Active Directory**. In the **Active Directory** view that appears, specify the domain information for the Active Directory you want to search. Then, in the Settings module, select **Discovery**, **Configuration**, and then **Active Directory**. In the **Active Directory** view that appears, specify the search condition

and other necessary information. When you click the **Start Discovery** button, the search begins according to the specified schedule.

To search for devices registered in Active Directory:

1. In the Settings module, select **General**, and then **Active Directory** to display the **Active Directory** view.
2. Set the domain information of the Active Directory you want to access.
   To make sure that you can access the set Active Directory, click the **Test** button.

   > **Important**
   >
   > In a multi-server configuration, do not specify the same Active Directory domain information for different management servers. If you do so, you might not be able to manage device information normally because the server that manages the information about a device might be changed unintentionally each time the device is detected.

3. In the Settings module, select **Discovery**, **Configuration**, and then **Active Directory** to display the **Active Directory** view.
4. In **Auto Discovery Schedule**, specify the search schedule.
5. In **Edit Discovery Option**, specify whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them.
6. To send a notification email to yourself (administrator) after completion of the search, specify the notification destination in **Notification of Discovery Completion**.
7. Click the **Start Discovery** button in the upper right corner of the window.

The display changes to the **Active Directory** view (which is displayed by selecting **Discovery**, **Discovery Log**, and then **Active Directory** in the Settings module), and then the search is performed according to the specified search schedule.

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. You can search for devices connected to the network.

In the Settings module, select **Discovery**, **Configuration**, and then **IP Address Range**. In the **IP Address Range** view that appears, set the range of IP addresses to be searched and the authentication information to be used during the search. When you click the **Start Discovery** button, the search begins according to the specified schedule.

To search for devices connected to the network:

1. In the Settings module, select **Discovery**, **Configuration**, and then **IP Address Range** to display the **IP Address Range** view.
2. In **Search Node Locations**, set the range of IP addresses to be searched.

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

> **Important**
>
> 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.
>
> If you discover more than 50,000 IP addresses, disable the **Intensive Discovery** option.

> **Important**
>
> In a multi-server configuration, do not specify the same search range for different management servers. If you do so, you might not be able to manage device information normally because the server that manages the information about a device might be changed unintentionally each time the device is detected.

3. In **Credentials Used**, set the authentication information to be used during the search.
4. In **Search Node Locations**, set the authentication information to be used for each IP address range.

> **Important**
>
> 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 might cause some users to be unexpectedly locked out of their accounts.

> **Important**
>
> 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.

5. In **Auto Discovery Schedule**, specify the search schedule.
6. In **Edit Discovery Option**, specify whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them.
7. To send a notification email to yourself (administrator) after completion of the search, specify the notification destination in **Notification of Discovery Completion**.
8. Click the **Start Discovery** button in the upper right corner of the window.
9. In the dialog box that opens, confirm the search settings, and then click the **OK** button.

   If you select the **Intensive Discovery** check box, a network search is repeated without a break in the specified period of time. Therefore, we recommend that you select this check box if you want to discover as many devices as possible at the initial stage of operation. For example, if you repeat a search, devices that were turned off and could not be discovered during the first search are more likely to be discovered during the second and subsequent searches.

Important

With the **Intensive Discovery** check box selected, a search that is continuously repeated imposes a heavy load on the network during the specified period of time. Select this check box after due consideration of the load on the network.

The display changes to the **IP Address Range** view (that is displayed by selecting, **Discovery**, **Discovery Log**, and then **IP Address Range** in the Settings module), and then the search is performed according to the specified search schedule.

Tip

When performing Discovery from IP Address Range to network devices that are in a redundant configuration, a device may be registered as two devices. If you do not want to manage one of devices, set either device to Ignored Node.

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 Inventory 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

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.

Important

The network monitoring function is not available for shared VDI-based virtual computers.

Tip

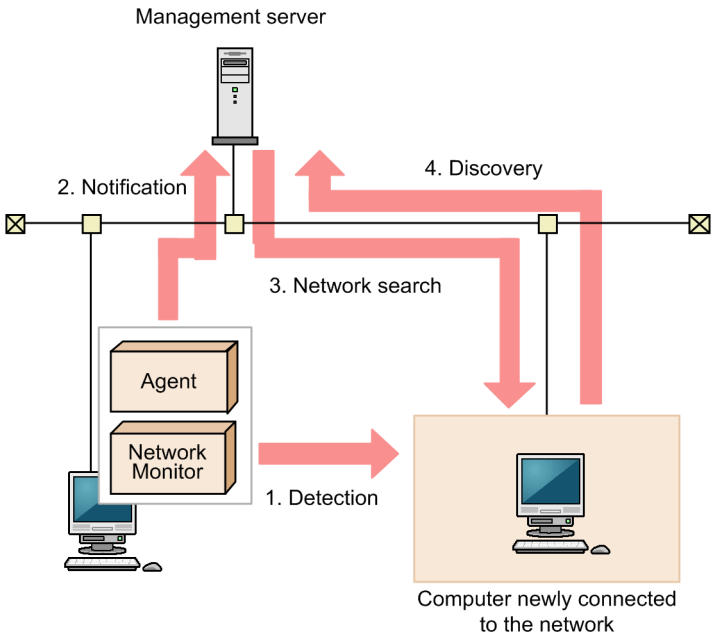
You cannot use network control to disconnect connections with a management server, a relay system, or a computer on which network access control is enabled.

Tip

To detect devices, enable the network monitor for a single computer on which an agent is installed per network segment. By installing an agent on and enabling the network monitor for a computer capable of

accessing multiple networks using multiple network cards, you can monitor multiple network segments using just one computer. Set an appropriate IP address range for the network segment and assign the corresponding authentication information. If a detected device has a network address that is outside the IP address range, a search is performed without using the authentication information. In this case, only the MAC address and IP address information is acquired from that device.

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



Legend:

Agent: JP1/IT Desktop Management 2 - Agent

Network Monitor: 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.

Important

If a search for devices (network search) is already running, the system waits until the search ends. If the network monitoring function is taking long time to detect devices, implement countermeasures such as narrowing the search range of the device search (network search).

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

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.

To use the network monitoring functions in a network connected via NAT, you must build a multi-server configuration system where a management server is installed for each network segment.

Important

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

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.
- Only computers that use standard TCP/IP can be monitored.
- 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 2, and then install agents on them.

Computers with agents installed automatically become the management target of JP1/IT Desktop Management 2. A JP1/IT Desktop Management 2 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.

Tip

In JP1/IT Desktop Management 2, the number of licenses held is managed for each OS type (Windows, Linux, or UNIX), but the number of licenses used is managed collectively regardless of the OS types. Note that Mac OS computers use licenses for Windows. (You can assign licenses for Windows to Mac OS computers.) Assigning a license to a Mac OS computer reduces the number of licenses that can be assigned to Windows computers.

For example, assume that a total of 520 licenses are registered as follows:

- Licenses for Windows agents: 500
- Licenses for Linux agents: 10
- Licenses for UNIX agents: 10

If you specify 510 Windows computers as management targets, the limit on the number of licenses held (520) is not exceeded, but the limit on the number of licenses for Windows agents (500) is exceeded. In such as case, you need to take one of the following measures:

- Register 10 or more additional licenses for Windows agents.
- Exclude the excessive (10 or more) Windows computers.

To check whether the maximum number of licenses used is exceeded for each OS, from the Settings module, click **Product Licenses** and then **License Details** to display **Maximum number of managed nodes**. Compare the number displayed with the number of computers managed for each OS displayed in **Device List** in the Inventory module.

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.

Note that you need to use the installation set to install an agent on the Citrix XenApp and Microsoft RDS server.

(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 wizard, click the **Next** button.
3. Create the installation set you want to apply to each computer by following the instructions in the wizard.

   Configure the following items. Click the **Next** button when you set the item:

   Selecting agent settings

   From **Agent Configuration Name**, select the agent configuration you want to apply to the computer.

   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 **Windows Agent Configurations and Create Agent Installers**.

   When you select an agent configuration, you can change the folder in which the agent is installed.

   To change the installation folder, enter the new installation folder for an agent in **Installation Folder**.

   In addition, when you install agents on shared VDI-based virtual computers, you have to specify **Settings when generating the host ID**.

   Account settings

   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 when you install agents on computers running 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 specify an account that has Administrator privileges, users who do not have Administrator privileges can use the specified account to install agents. 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.

   Settings for the components to be installed

   Specify the type of components to be installed (select whether to install them as agents or relay systems), and whether to install remote control agents, which are subcomponents.

Settings for the registration-destination ID

Specify the ID (ID group used for receiving jobs from the managing server) to which the agent is to be registered.

Settings for the file to be deployed

Specify the file that is deployed when the agent is installed and the folder in which the file is to be deployed.

Settings for the file to be automatically executed

Specify the files that are automatically executed after the agent is installed, and the files and arguments necessary for the automatic execution.

> **Tip**
>
> To automatically install Hibun (Hibun DC or Hibun DE) or some other related product on an agent, first prepare (create) installation media containing the related product in a folder in `C:\DATA` on the administrator's computer. Compress the entire folder or all of the files in the folder to a ZIP file. Then, to automatically install the related product on an agent, specify this ZIP file as a file to be automatically executed after agent installation. For details about how to create installation media for Hibun, see the *JP1/HIBUN Installation and Setup (for Administrators)*.

Settings for an overwrite installation

Specify whether to perform an overwrite installation if the agent has already been installed.

4. Check the settings, and then click the **Create** button.
   The **Create Agent Installer** dialog box appears.

5. In the **Create Agent Installer** dialog box, click the **Save** button.
   The default file name of the saved installation set is `ITDM2Agt.exe`.

6. The **Completed** screen is displayed, click the **Close** button and exit the wizard.

The installation set is created, and then downloading of the installation set begins.

> **Tip**
>
> You can also create an installation set in the **Windows Agent Configurations and Create Agent Installers** view. To display this view, in the Settings module, select **Agent** and then **Windows Agent Configurations and Create Agent Installers**. 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 **Create** button. The installation set is created, and then downloading of the installation set begins.

> **Tip**
>
> You can create the file for connection destinations (`itdmhost.conf`) or the information file for higher connection destinations (`dmhost.txt`) and store it in the JP1/IT Desktop Management 2 - Manager data folder. When you create the installation data set, the file you created is incorporated into the installation data set. For details about the file for connection destinations (`itdmhost.conf`), see the description about automatically setting the connection destinations of agents in the *JP1/IT Desktop Management 2 Configuration Guide*. For details about the information file for higher connection destinations, see the description of automatic change of connection destinations for agents in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

Important

You cannot use an installation set to install an agent on UNIX computers or Mac OS computers.

Related Topics:

- 15.1.2 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.

Note that you can use an installation set to install agents only on computers that are directly managed by the management server on which you created the installation set.

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.

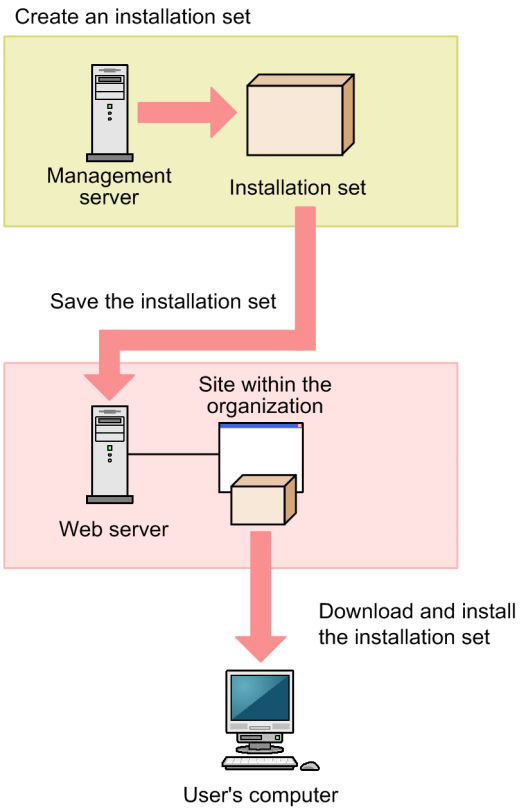
Advantage:

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.

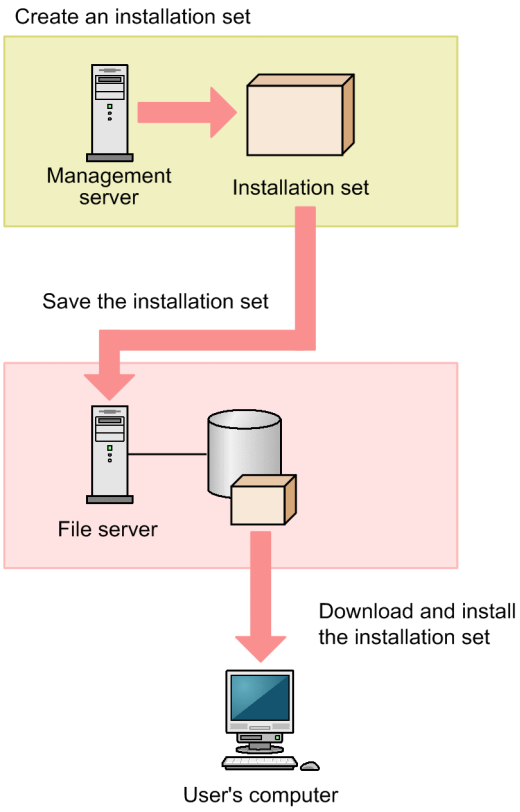
Advantage:

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:



Tip

If you execute an offline installation media on a network drive, you're required to log on with administrator permissions.

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.

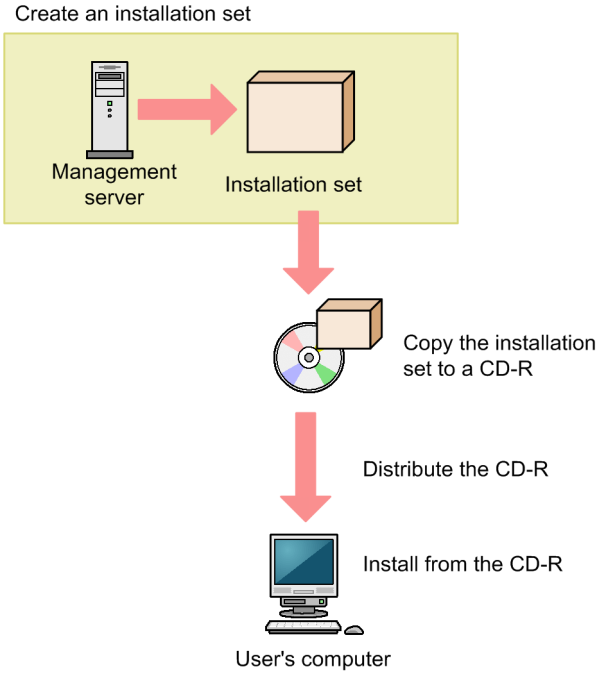
Advantage:

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 `ITDM2Agt.exe` is the name of the file storing the installation set:

```
[Autorun]
open=ITDM2Agt.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.

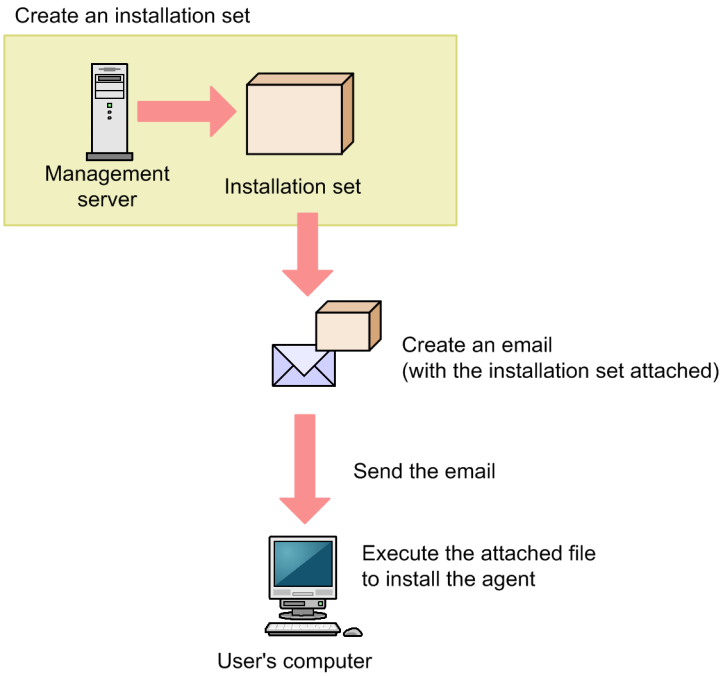
Advantage:

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

Disadvantage:

The minimum size of an installation set is approximately 80 MB, which varies according to the settings. 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\ITDM2Agt.exe
)
) else (
if not exist "%ProgramFiles%\Hitachi\jp1itdma\bin\jdnglogon.exe" (
start /w \\server-name\shared-folder-name\ITDM2Agt.exe)
)
```

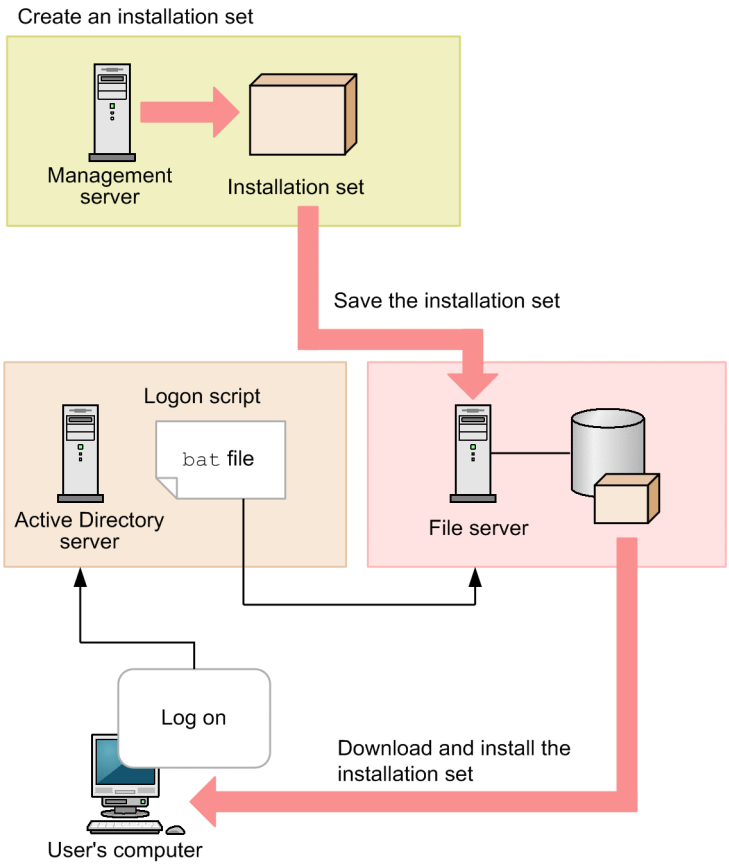
Advantage:

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

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.

If you duplicate an agent-installed virtual environment such as a VMWare environment, execute the `resetnid.vbs` command.

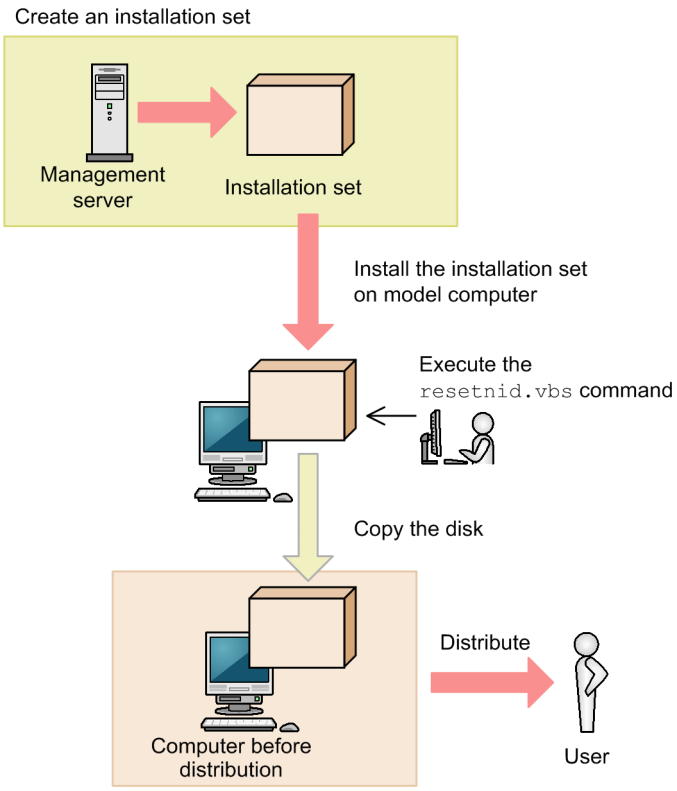
Advantage:

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
- 17.33 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.

Important

You cannot deploy agents to computers running UNIX or Mac OS. (If you select multiple Windows computers together with UNIX or Mac OS computers as deployment destinations at the same time, deployment to any selected UNIX and Mac OS computers will fail.)

Tip

If the display language of OS of the agent is not Japanese, English, Chinese, when execute remote installation to the agent itself, even if Interactive Services Detection dialog from OS might be displayed on agent, installation is successfully completed so ignore it.

Check the display language of OS at **Control Panel** - **Regional and Language Options** - **Keyboards and Languages** tab. In Windows 8 and Windows Server 2012 or later, check **Control Panel** - **Language**

(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 80 MB of data (installation set) is sent to each computer. The size of an installation set varies according to the settings.

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 **Windows Agent Deployment** to display the Agent Deployment view.

(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 80 MB of data (installation set) is sent to each computer. The size of an installation set varies according to the settings.

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.
   If the agents to be deployed include a remote control agent, go to step 5. If the agents to be deployed do not include a remote control agent, go to step 10.

5. Under **Agent** in the Settings module, click **Windows Agent Deployment** to display the Windows Agent Deployment window.

6. In **Settings of the Components of the Agents to Be Deployed**, click **Edit**.

7. In the displayed dialog box, select the **Include remote control agents** check box.

8. Click **OK** to close the dialog box.

9. Under **Discovery** in the Settings module, click **Configurations** to display the **IP Address Range** window.

10. Click the **Start Discovery** button.

11. 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 **Windows Agent Deployment** to display the Agent Deployment view.

(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 80 MB of data (installation set) is sent 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.

   If you want to include remote control agents as agents to be deployed, go to the next step. If you do not want to include remote control agents, skip the remaining steps.
5. In the Settings module, select **Agent** to display the **Windows Agent Deployment** view.
6. In **Settings of the Components of the Agents to Be Deployed**, click the **Edit** button.
7. In the dialog box that appears, select **Include remote control agents**.
8. Click the **OK** button to close the dialog box.

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 2, 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 2. 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 2. 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 2 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 2 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 80 MB of data is sent to each computer.

To deploy agents to selected groups of computers:

1. In the Settings module, select **Agent** and then **Windows Agent Deployment** to display the **Windows Agent Deployment** view.

2. In **Settings of the Components of the Agents to Be Deployed**, click **Edit**.
   If the agents to be deployed include a remote control agent, select the **Include remote control agents** check box in the displayed dialog box. If the agents to be deployed do not include a remote control agent, uncheck it.
3. Click **OK** to close the dialog box.
4. Select the computers to which you want to deploy agents.
5. Click the **Deploy Agent** button.
6. In the displayed dialog box, select an agent configuration you want to apply to computers.
   In the **Agent Configuration**, displayed the agent configurations which are added in the **Windows Agent Configurations and Create Agent Installers** from the **Agent** in the Settings module. For details about adding agent configurations, see the description of managing agent configurations in the manual *JP1/IT Desktop Management 2 Administration Guide*.
7. Click the **OK** button.

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

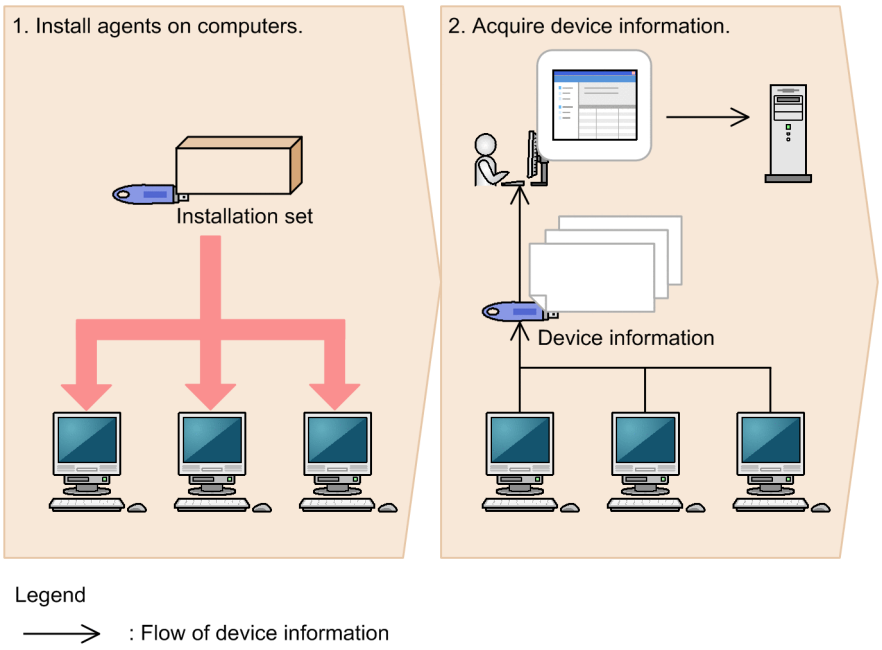
If you find any computers on which agents have not yet be installed, inform the applicable users to install an agent on their computers as soon as possible. If you have configured automatic agent deployment, agent deployment might have failed. In this case, check the deployment status in the **Windows 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 2, you can manage computers not connected to the management server in the same way as you manage online computers.

Note that this function is not supported on the Citrix XenApp and Microsoft RDS server.

To manage devices offline:



1. Install agents on computers.

   To manage computers offline by using JP1/IT Desktop Management 2, 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:

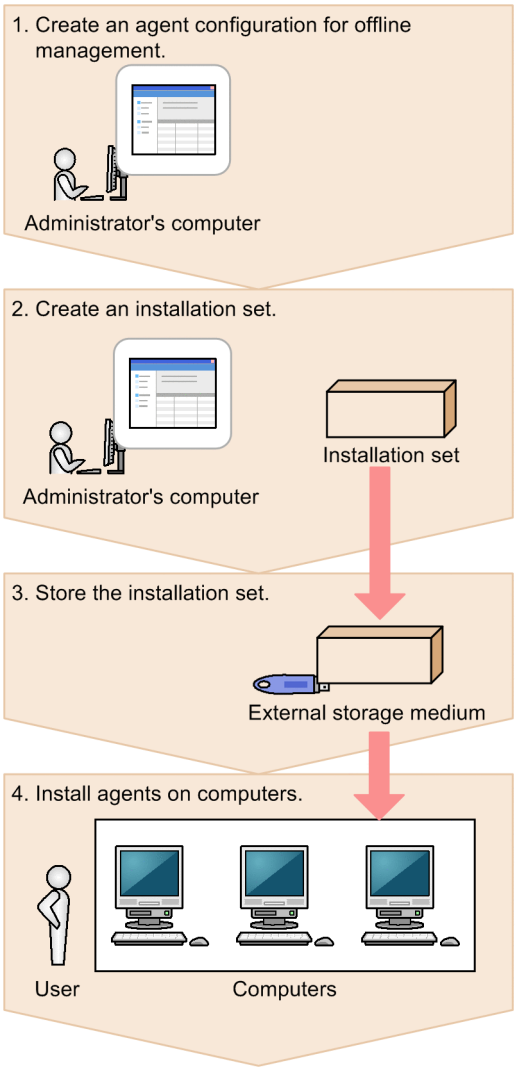
- 1.2.1 General procedure for installing agents on computers to be managed offline
- 1.2.2 General procedure for acquiring device information from computers managed offline by using an external storage medium

- 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 2, 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 **Communicate with the higher system** check box is cleared in the **Basic settings** view 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.If you want to apply a security policy, you can create an installation set with a security policy.

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.

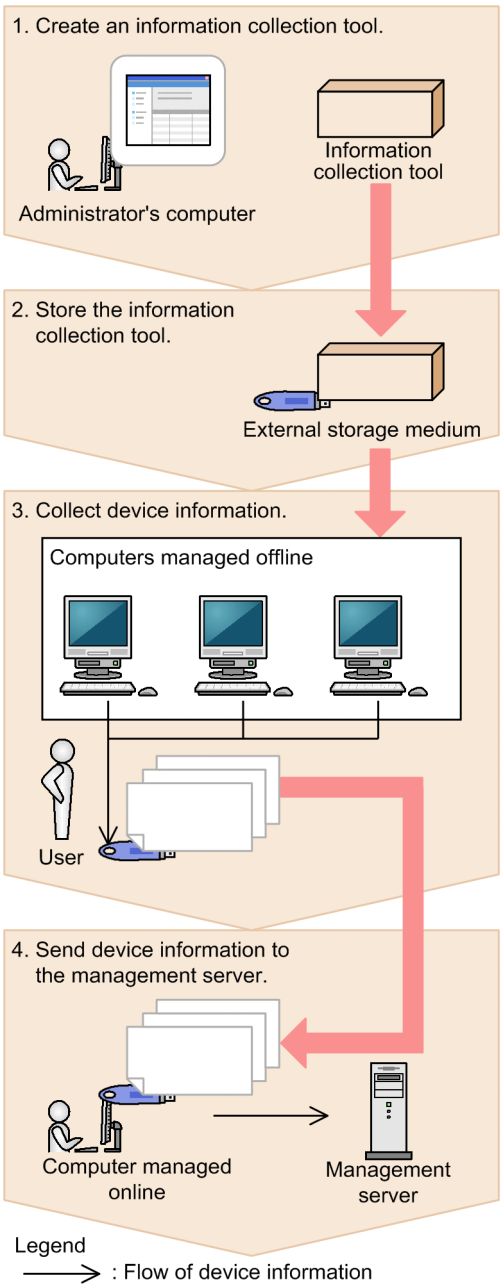
Agents are installed on all computers. When the agent installation task is complete, acquire device information from the computers to be managed offline to include them as the management targets of JP1/IT Desktop Management 2.

> **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.

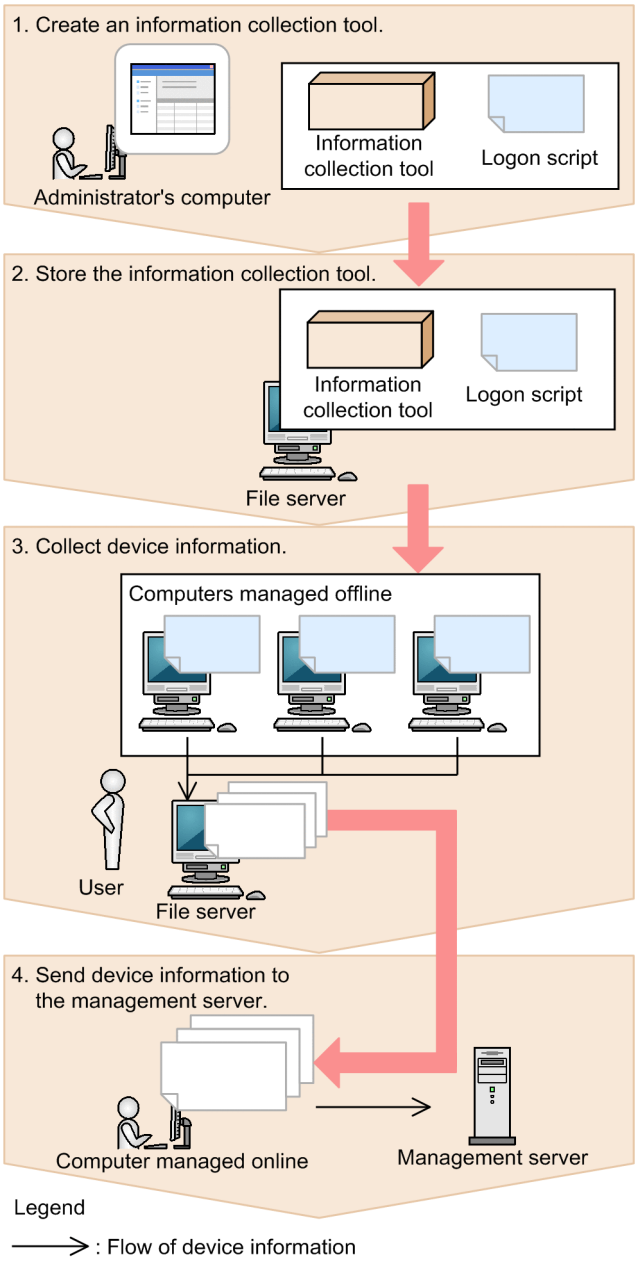
Device information of computers managed offline is acquired.

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.

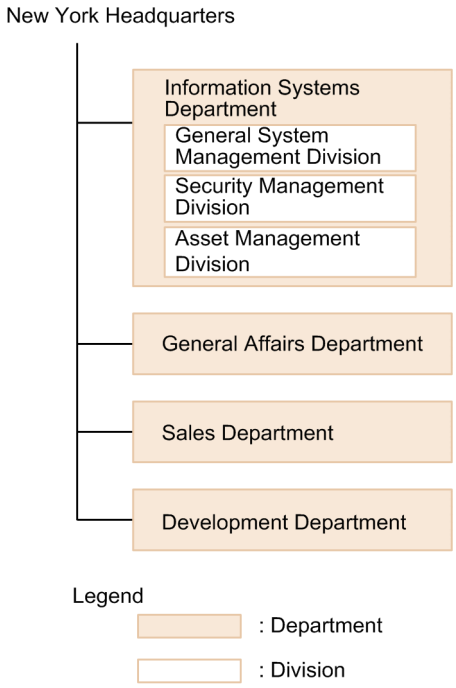
   Determine the system management tasks to be assigned to each administrator. For example, there are various system management tasks that include creating and assigning a security policy to computers, managing devices, managing software licenses, distributing software to computers, and managing user accounts. 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 2, 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 2.

   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 2.

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 2. 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 2. 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

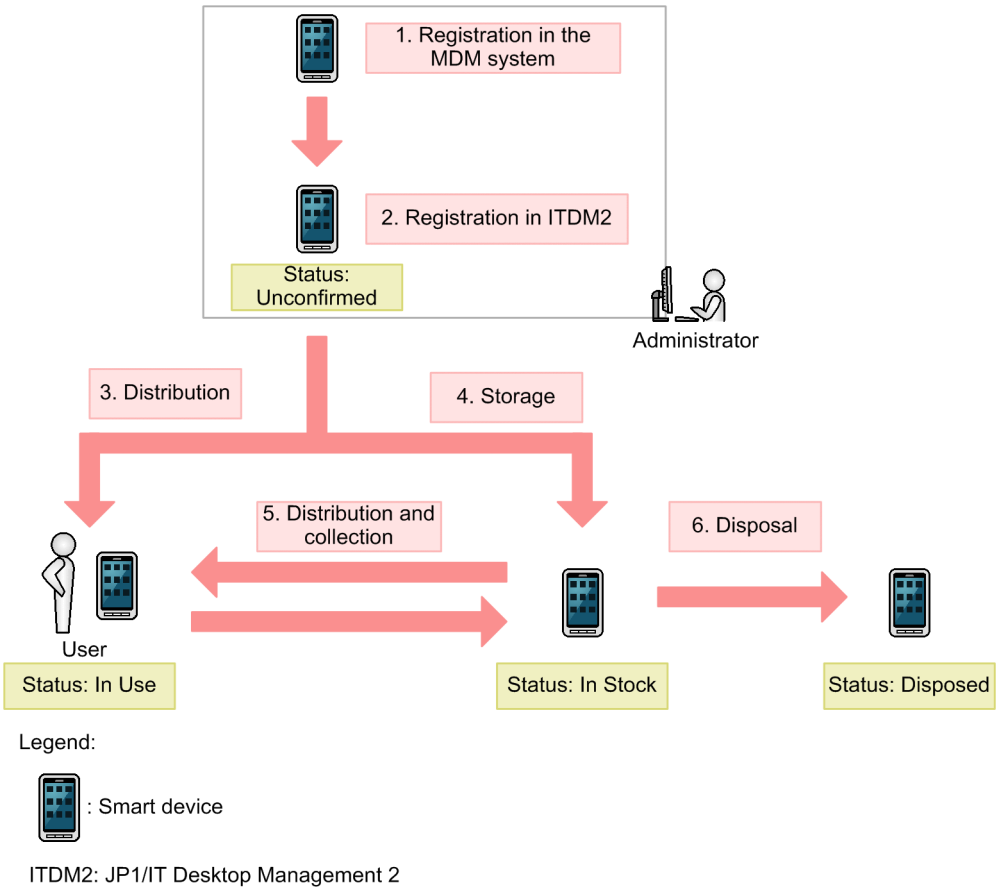
As smart devices become increasingly popular, many more companies are incorporating smart devices into their business operations. Although incorporation of smart devices into business operations is expected to improve business efficiency, such incorporation raises the risk of information leakage. To 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 2, you can efficiently manage smart devices as follows:

- Using JP1/IT Desktop Management 2, 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 2, you can manage the device information, asset information, and security of the smart devices.
- Using JP1/IT Desktop Management 2, you can lock and initialize smart devices, as well as reset their passcodes.

You can manage smart devices by using the Inventory 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 2.

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 2, 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 2 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 2, 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 2 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 2.

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 2, 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 2, 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 2, 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 2, 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 2 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 2, 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 2, 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 2, 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 2, 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 2.

   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 2.

   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 Inventory 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 2 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) Including smart device software as a management target

To include smart device software as a management target, acquire information about the smart device software from the MDM system, and then add the software as managed software.

The following table lists and describes the search words to be specified when you acquire the software information needed to add managed software.

Smart device OS	Search word to be specified	Application name to be specified
Android	`Android-`*`application-name`*	Specify the application name displayed on the **Software** tab of the **Managed Smart Device List** view of JP1/ITDM2 - SDM#, or the application name displayed by the device when you select **Settings** and then **Apps (Application Manager)**.
iOS	`iOS-`*`application-name`*	Specify the application name displayed on the **Software** tab of the **Managed Smart Device List** view of JP1/ITDM2 - SDM#, or the application name displayed by the device when you select **Settings**, **General**, **Storage & iCloud Usage** and then **Manage Storage**.

#: JP1/IT Desktop Management 2 - Smart Device Manager

(4) 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 2. 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 2. 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 2 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 2 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 2, 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 2, 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 2, 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 **Planned Hardware Asset Status** 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:

- 15.6.2 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 **Planned Hardware Asset Status** 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:

- 15.6.2 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 Inventory module. Then, from **Action**, select **Initialize Smart Device**.

   To retain the smart device information in JP1/IT Desktop Management 2, 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 2, 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:

- 6.31 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 2. 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 2. 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 Inventory module. Use the filtering function to facilitate this processing.

4. Initialize the identified smart device.

   In the **Device List** view of the Inventory 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 2, 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:

- 6.31 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 2 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 Inventory module. Use the filtering function to facilitate this processing.

3. Lock the identified smart device.

   In the **Device List** view of the Inventory 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:

- 6.29 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 2.

(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 Inventory 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:

- 6.30 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 2.

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 2, 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 Inventory 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.

   > **Important**
   >
   > If the network monitor is enabled on a device to be disposed of, you need to disable the network monitor before disposing of the device.

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

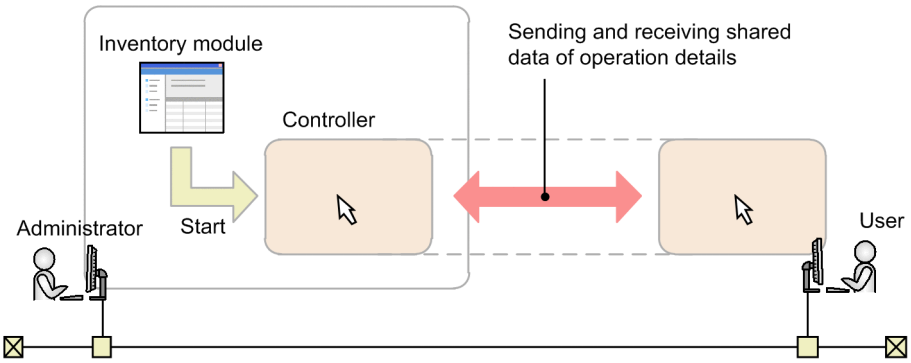
1.5 Remote controlling devices

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 Inventory 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 2. The following figure shows how an administrator can remote control a device:



From the Inventory 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 2 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 Inventory 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 Inventory 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
- 15.1.1 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 2, 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.
- Use a command to block or enable network access of devices.
  Use this function when you want to execute a command from the management server or an environment other than that of the management server to block network access.

Important

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

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 2 (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

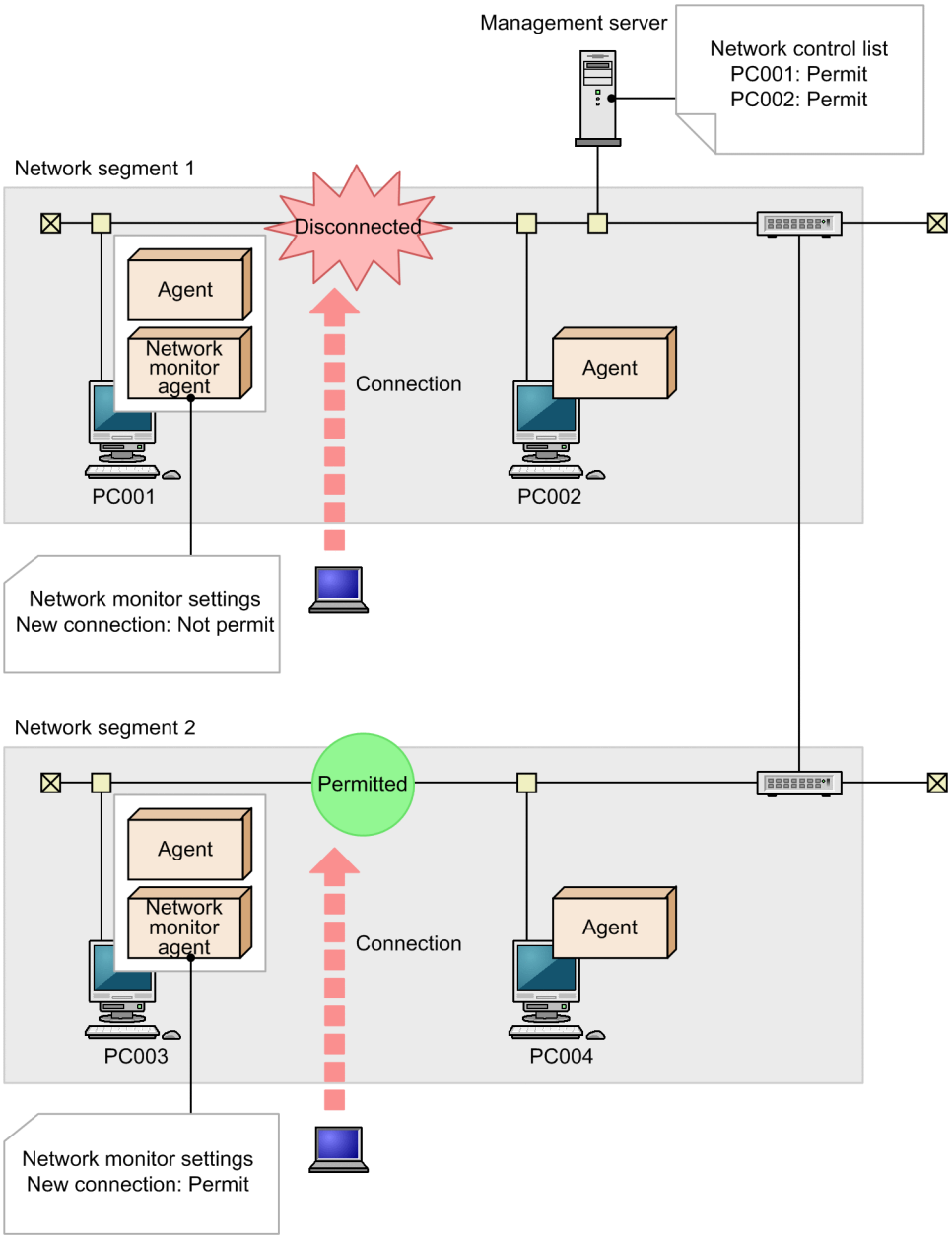
We recommend that you manually register, in a network control list, the IP addresses of devices that are important for business operations, including routers, printers, and servers. In this way, you can prevent these devices' network access from being disabled due to automatic updating of the network 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.

Important

Network devices such as routers, switches, and network printers are less likely to communicate with the devices, so it may not be detected by the network monitor immediately after start of operations with enabled network monitor.

Control network access of devices by using the Inventory 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, relay systems, or the computers on which network monitor agents are installed.

Note that you cannot disable network access for management servers

This section explains how to use JP1/IT Desktop Management 2 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.

Use a command to block network access of devices.

By executing a network access control command from the management server or an environment other than that of the management server, you can automatically block or enable network access of devices.

Important

On agents for UNIX, automatic control of enabling or disabling network access cannot be used because the network monitor cannot be enabled and the security status cannot be determined. You need to enable or disable network access on demand.

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**
>
> 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 2

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 2

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**
>
> 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

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 Inventory 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:

- 1.7.6 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 Inventory 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 Inventory 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.

Important

On agents for UNIX, automatic control of enabling or disabling network access cannot be used because the security status cannot be determined. You need to enable or disable network access on demand.

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

  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 settings** 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.

1.6.5 Controlling network access of devices by using a command

By using a network control command provided by JP1/IT Desktop Management 2, you can block or enable network access of devices. The network control command can be executed from any environment other than that of the management server.

To control network access of devices by using a network control command:

1. Set up an environment to execute the network control command.
   Set up an environment to execute the network control command.
2. Execute the network control command.
   Execute the network control command to block or enable network access of the devices.

(1) Setting up an environment to execute the network control command

To set up an environment to execute the network control command:

1. Create a dedicated user for executing the network control command (recommended).
   The network control command requires the execution user to be authenticated. The command must be executed while a user ID and password managed in JP1/IT Desktop Management 2 are specified in the command.
   The user account to execute the network control command must be configured as described below. We recommend that you create a dedicated user for executing the network control command in an operational environment.
   - Permission: System Administrator
   - Task allocation: Security management and System settings management
   - Administration scope : All
2. Deploy the network control command.#
   To execute the network control command in an environment other than that of the management server, copy the following files to any folder in that environment:
   Executable of the network control command
   JP1/IT Desktop Management 2 -Manager-installation-folder\mgr\remote\jdnrnetctrl.exe
   Network control command configuration file (template)
   JP1/IT Desktop Management 2 -Manager-installation-folder\mgr\remote\jdnrnetctrl.ini
   The jdnrnetctrl.ini file (network control command configuration file) can be copied with any name you want.

In a multi-server configuration, you can create different network control command configuration files for different management servers you want to interact with.

3. Edit the network control command configuration file.

Edit the following values for your environment:

- The host name or IP address of a management server
- The connection port number on the management server
- The ID of the JP1/IT Desktop Management 2 user who can execute the command
- The password of the JP1/IT Desktop Management 2 user ID

#: To execute the network control command on a management server, use the executable and configuration file listed below. The network control command configuration file must be edited for your environment. Note that you must specify localhost for the host name.

Executable of the network control command

JP1/IT Desktop Management 2 -Manager-installation-folder\mgr\bin\jdnrnetctrl.exe

Network control command configuration file (template)

JP1/IT Desktop Management 2 -Manager-installation-folder\mgr\conf\jdnrnetctrl.ini

(2) Controlling network access of devices

1. Execute the network control command.

Execute the network control command (jdnrnetctrl command). When you execute the command, set an option to specify whether to block or enable network access. Specify either or both of the host name and IP address of the device whose network access you want to control. When both of the host name and IP address are specified, the system uses the AND condition to find a device that matches both of the host name and IP address. The command can control the network access of any devices that are managed in JP1/IT Desktop Management 2 (managed devices, discovered devices, and ignored devices).

Network access is blocked or enabled for the devices specified with the command.

For a multi-server configuration

In a multi-server configuration, the network control command must be issued to a management server that manages a device whose network access you want to control. A management server can control the network access of devices that are located directly under the management server. When you cannot identify which management server manages your target device, you can issue the same command to multiple management servers. To do so, ensure that the device information (host name and IP address) specified with the command does not conflict between management servers.

In a configuration where the primary management server works with JP1/NETM/NM - Manager to manage all network accesses, the network access of a device is controlled after the primary management server receives a notification from the management relay server. A notification to a higher server is sent at the specified interval (set to five minutes by default).

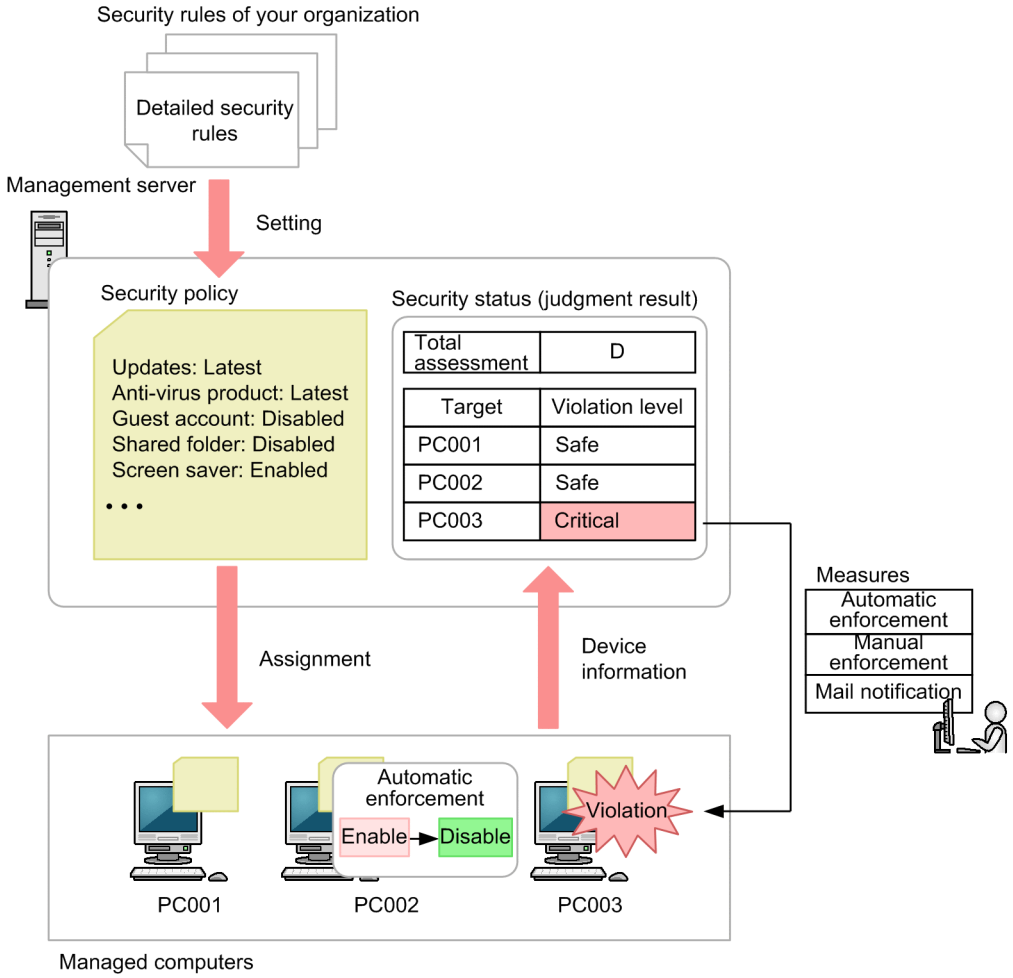
1.7 Managing the security status

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 2, 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 2.

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.

You can also use the security policy settings to deter the use of some software or devices or obtain an operation log from each computer to detect a suspicious operation.

This section explains how to use JP1/IT Desktop Management 2 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 2 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 2 obtains updates released by Microsoft and automatically distributes and applies them to computers. It takes a certain period time for JP1/IT Desktop Management 2 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 2 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 devices.

You can permit data to be read from and written to authorized 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.

Important

The following notes apply to agents for UNIX or Mac:

For agents for UNIX

- Because security status determination is not provided, (Unknown) is always displayed as the violation level.
- Neither automatic correction of security problems (automatic distribution of OS patches) nor email security notification is provided.

- Automatic control of enabling or disabling network access is not provided. You need to enable or disable network access on demand.
- You need to use Remote Install Manager to distribute and apply OS patches.

For agents for Mac OS

- Security status determination is provided for items listed below. For excluded items, **Out of Target** is displayed as the violation level.
  - Windows Update (Automatic Update)
  - Software use
  - OS Security (**Guest Account, Days Since Last Password Change, Auto Logon, Firewall**, and **Password (Screen Saver)**)
  - User-Defined Security Settings
- Neither automatic correction of security problems (automatic distribution of OS patches) nor email security notification is provided.
- Network access can be enabled or disabled automatically depending on the results of security status evaluation.
- To distribute or apply OS patches, you must use distribution with Remote Installation Manager.

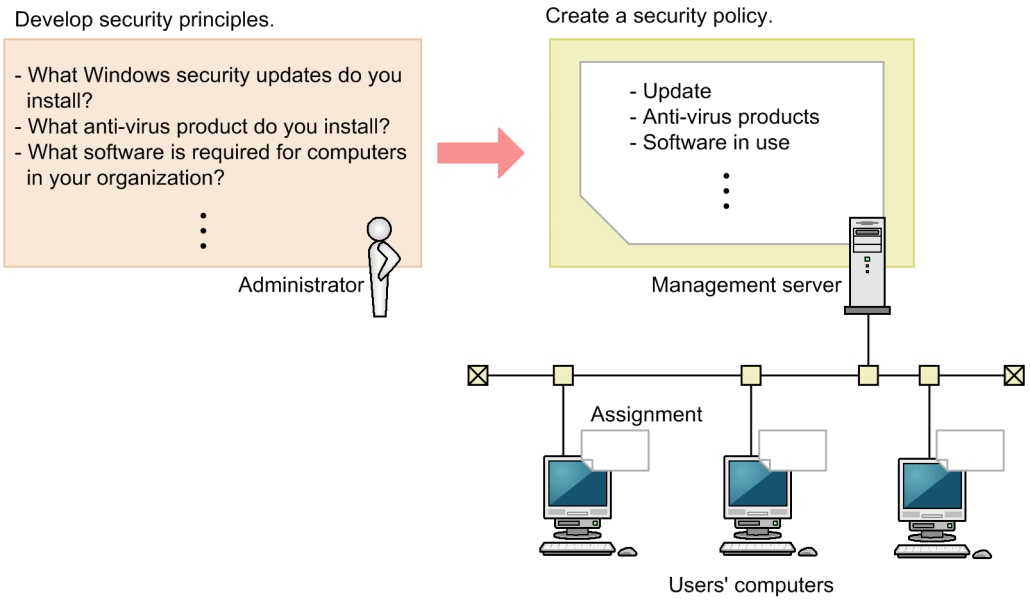
Tip

You can package and distribute Windows updates and a feature update to Windows 10 by using Remote Install Manager. For details, see the description of managing updates in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

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 2.

Based on the developed security principles, create a security policy by using JP1/IT Desktop Management 2. 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.



If you want to apply a security policy to offline-managed computers, develop the security principles for the offline-managed computers, different from those for online-managed computers.

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 2. Based on the developed security principles, create a security policy by using JP1/IT Desktop Management 2. 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 of addresses for monitoring targets if you want to monitor web access, email transmission, email reception, and file operations for 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.

You can generate a security policy that is applied to computers in an offline environment by selecting the **Create Tool for Applying Policy Offline** from Action in the **Security Policies** view. For details, see the description about the procedure for applying a security policy to offline-managed computers in the manual *JP1/IT Desktop Management 2 Administration Guide*.

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.

Important

Agents for UNIX are excluded from security policy-based management. An automatic countermeasure is also not performed. Network connection control is manually performed.

Agents for Mac can be managed by using security policies. However, any detected problems cannot be corrected automatically. The network access control can enable or disable the access depending on the results of security status evaluation.

Computers in the offline environment are included in security-policy-based management. However, the security policy must be applied to the computers via an external storage medium. For details, see the description about the procedure for applying a security policy to offline-managed computers in the manual *JP1/IT Desktop Management 2 Administration Guide*.

1.7.2 Taking measures against a security policy violation

In JP1/IT Desktop Management 2, 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 2 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.

Important

The following notes apply to agents for UNIX or Mac:

For agents for UNIX

- Because security status determination is not provided, (Unknown) is always displayed as the violation level.
- Neither automatic correction of security problems (automatic distribution of OS patches) nor email security notification is provided.
- Automatic control of enabling or disabling network access is not provided. You need to enable or disable network access on demand.

For agents for Mac OS

- Security status determination is provided for items listed below. For excluded items, **Out of Target** is displayed as the violation level.
  - Windows Update (Automatic Update)
  - Software use
  - OS Security (**Guest Account, Days Since Last Password Change, Auto Logon**, **Firewall**, and **Password (Screen Saver)**)
  - User-Defined Security Settings
- Neither automatic correction of security problems (automatic distribution of OS patches) nor email security notification is provided.
- To distribute or apply OS patches, you must use distribution with Remote Installation Manager.

(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.

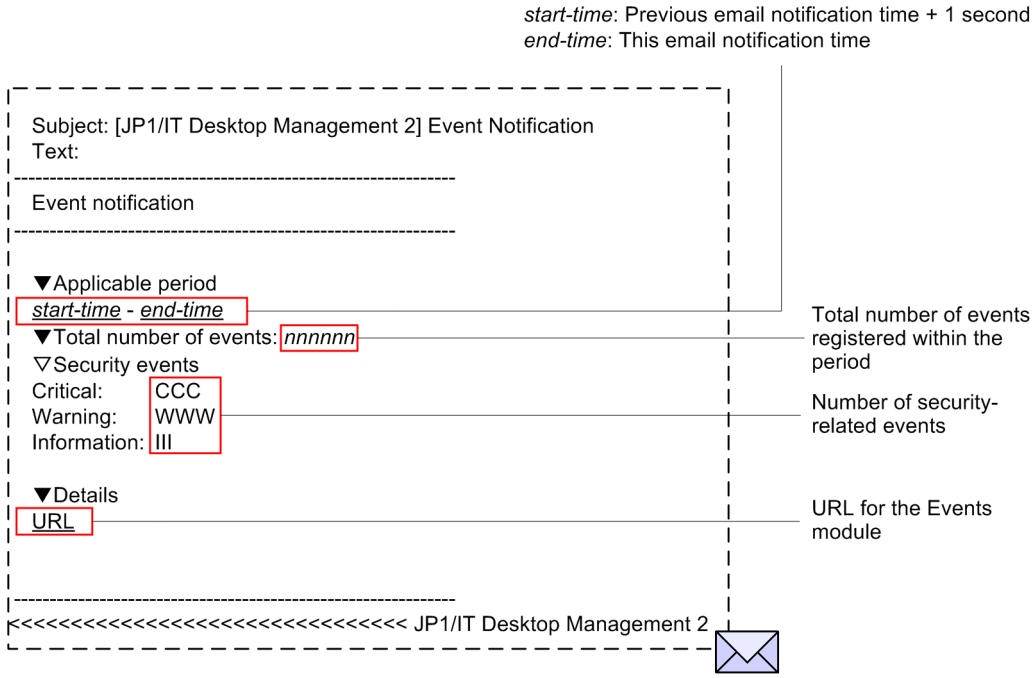
   The following table describes the correspondence between the severity of each event to be reported and the violation level of the security status:

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 2. If a critical event has occurred, start the operation view of JP1/IT Desktop Management 2 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 2, 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
- 15.7.1 Specifying settings for event notification
- 9.1 Checking the security status
- 15.8.1 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 2 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
- 6.26 Sending a notification to a user

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

The following automatic enforcement items do not work for computers managed offline:

- Auto Enforce for Install Updates
- Auto Enforce for prohibited software (uninstallation)
- Auto Enforce for mandatory software

For that reason, if you (administrator) check the security status and find that some security configuration item that automatic enforcement does not work for is in violation of the security policy, you 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 2 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

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

Important

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 other reason), you can distribute the updates as follows: By using a computer that can access the support service site, manually download updates and related information, and then upload the updates and information to the management server.

Related Topics:

- 15.8.3 Setting information for connecting to the support service
- 15.8.1 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 Windows Update (ITDM-compatible distribution)**.

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 2, 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 Windows Update (ITDM-compatible distribution)**.

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 (ITDM-compatible) 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 Windows Update (ITDM-compatible distribution)** 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 2 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 2 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 2, 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 2 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

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 (ITDM-compatible) 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 Windows Update (ITDM-compatible distribution)** 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 Managing cumulative updates and Security Monthly Quality Rollup for Windows

If the computers used in the company run Windows as the OS, you can keep track of whether cumulative updates and Security Monthly Quality Rollup (rollup updates) are applied by using JP1/IT Desktop Management 2.

Security judgment is possible even when Microsoft Japan releases rollup updates but the latest update information has not been posted on the support service site yet. Security judgment can also be performed taking into consideration the grace period given to apply updates.

Important

Even when Microsoft releases rollup updates, these updates cannot be automatically distributed to computers until the latest update information is posted on the support service site.

Tip

Until the latest rollup update information is posted on the support service site, you can distribute rollup updates by manually adding them to the Update List. In this case, you can distribute rollup updates in the same way as you distribute non-rollup updates. For details, see 1.7.4 Manually registering and distributing an update.

Related Topics:

- 15.3.5 Judgment for cumulative updates and Security Monthly Quality Rollup for Windows

1.7.6 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 2, 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 2, 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 2.

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 2, 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 Inventory 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.

1.7.7 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 2, 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 2, 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 2 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 Inventory 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 Inventory module and **Dashboard**. Click the link of the software name to navigate to the **Software Inventory** view of the Inventory 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 Inventory 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
- 10.2 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 Inventory 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:

- 6.24 Setting unauthorized software
- 9.3.1 Adding security policies

1.7.8 Restricting the use of USB devices

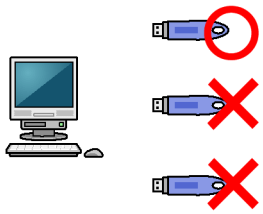
Various types of data such as customer data, sales data, and development data exist on computers in your organization. If any of these types of confidential information leaks out, there is huge damage and your organization's social reputation is also ruined. For that reason, you need to take security measures to protect confidential information by preventing data from being brought out or lost.

You can use JP1/IT Desktop Management 2 to deter the use of devices. 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.

Tip

When you permit only registered USB devices to be used, you can also apply the following conditions to limit assets that can use the USB devices.

- The registered USB device is permitted to be used only with assets that are registered with the same department as the USB device.
- The registered USB device is permitted to be used only with assets that are registered with the same location as the USB device.
- The registered USB device is permitted to be used only with hardware assets that are registered and associated with the USB device.

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 2 as authorized USB devices.

2. Deter the use of any USB devices other than the authorized USB devices.

   Using JP1/IT Desktop Management 2, 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 2, 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

- (7) 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 devices
- (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 2), 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 **Planned Hardware Asset Status** 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
- 15.4.1 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. In addition, you need to enable the operation log policy.

1. Display the operation log of the user.

   You can check operation logs in the **Operation Logs** view of the Security module. To check the history of a USB device, examine operation logs whose **Operation Type** is **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 on which the USB device was operated
   - Information about the user who operated the USB device
   - Information about the files copied to the USB device

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:

- 10.4 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 2 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
- 1.7.8 Restricting the use of USB devices
- (7) Handling the loss of a USB device

(6) Permitting users to bring out data for limited cases (depending on the department, installation location, or device)

You can restrict the use of USB devices to prevent information leakage caused by data brought out.

One way to restrict the use of USB devices is to permit users to bring out data depending on the department, installation location, or associated asset (device). For example, you can permit computers only in the sales department to use USB devices while prohibiting computers in any other departments from using USB devices.

This subsection describes how to permit USB devices to be used for limited cases (depending on the department, installation location, or device).

1. Set a security policy.

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

   In **Other Access Restrictions**, which is a security configuration item, enable USB devices, and select **Allow registered USB device usage**. You can also select **Limit the assets that can be used** to limit assets that can use the USB device by using the following conditions:

   - **Allow only the resources of the department that owns the USB device to be used**

     The registered USB device is permitted to be used only with assets that are registered with the same department as the USB device.
   - **Allow only the resources in the same location as the USB device to be used**

     The registered USB device is permitted to be used only with assets that are registered with the same installation location as the USB device.
   - **Allow only the resources associated with the USB device to be used**

     The registered USB device is permitted to be used only with hardware assets that are registered and associated with the USB device.

2. Register USB devices.

   Register USB devices as authorized USB devices. For details about how to register USB devices, see 9.7 Registering USB devices.

   When a USB device is registered, the department and installation location can also be added to the information of the user who registers the device.

3. Edit the hardware asset information.

   Edit the hardware asset information of the registered USB devices in the **Hardware Asset** view of the Assets module. In the hardware asset information of the registered USB devices, **Asset Status** is set to **Unconfirmed**. Set **Asset Status** to any value other than **Unconfirmed** or **Disposed** to register the USB devices as authorized USB devices.

   In the **Edit Hardware Asset** dialog box, you can set the information of the department, installation location, and associated hardware asset. The department, installation location, and other information you set here are used to limit authorized USB devices.

USB devices will be permitted to be used only with assets that are set in the security policy.

Related Topics:

- 9.3.1 Adding security policies
- 9.3.2 Editing security policies
- 11.1.2 Editing hardware asset information

(7) 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 Collect is selected in **Collect List of USB Device Files** under **Common settings for prohibited operations and operation logs**, you can see the information of the files stored in the 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.

> **Important**
>
> The file information might be incorrectly displayed when the USB device meets any of the following conditions:
>
> - File system is encrypted.
> - File system is password protected.
> - There is a floppy disk drive or optical disk drive.

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

1.7.9 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 2, 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 2, output the **Violation Level Status** report in **Security Detail Reports**.
2. Output event data related to security management.
   Using JP1/IT Desktop Management 2, output event data related to security management.
3. Output the status of the deterrence of prohibited operation.
   Using JP1/IT Desktop Management 2, output the **Other Access Restrictions Top N** report in **Security Detail Reports**.
4. Output a list of managed computers.
   Using JP1/IT Desktop Management 2, 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 2 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 suppression on the use of devices.

   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 Inventory 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:

- 6.21 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 2 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 2, 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 2, 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 2 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:

- 10.4 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.

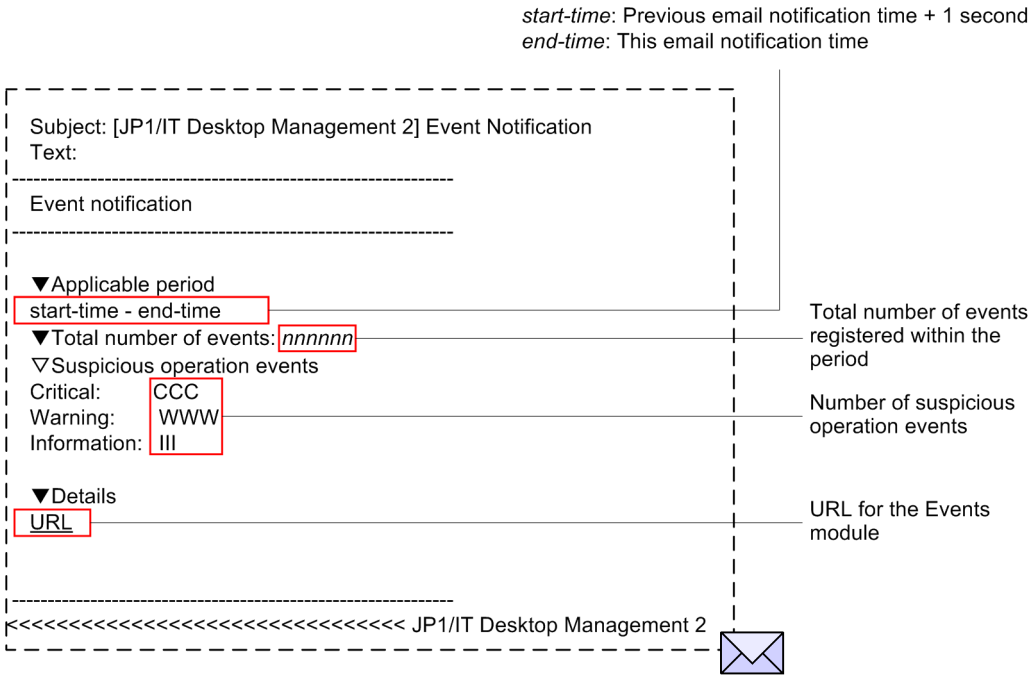
If a suspicious operation is detected, an event with **Suspicious Operation** set for **Type** is generated. Set the configuration in such a way that an email is sent to you when this event is generated.

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 2 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 **Operation Logs** view of the Security module, and then check the related operation logs.

2. Investigate operation logs by data tracing.

   In the **Operation Logs** view 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 2, 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**.

To check operation logs that do not exist in the database, import past operation logs into the management server. Because importing all operation logs requires a long time, you need to narrow down the target computers based on the brought out data, and then import operation logs.

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 **Device operation**.
- **Operation Type (Detail)** is **Logon**, **Copy file**, **Web Access (Upload)**, **FTP (Send File)**, or **Device category**.

Use a filter with conditions such as **Source**, **Department**, **Location**, and **User Name** to narrow down the computers from which data was brought out.

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.

Related Topics:

- 10.7.1 Importing old operation logs into a management server

- 10.7.2 Importing operation logs from selected computers

(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**.

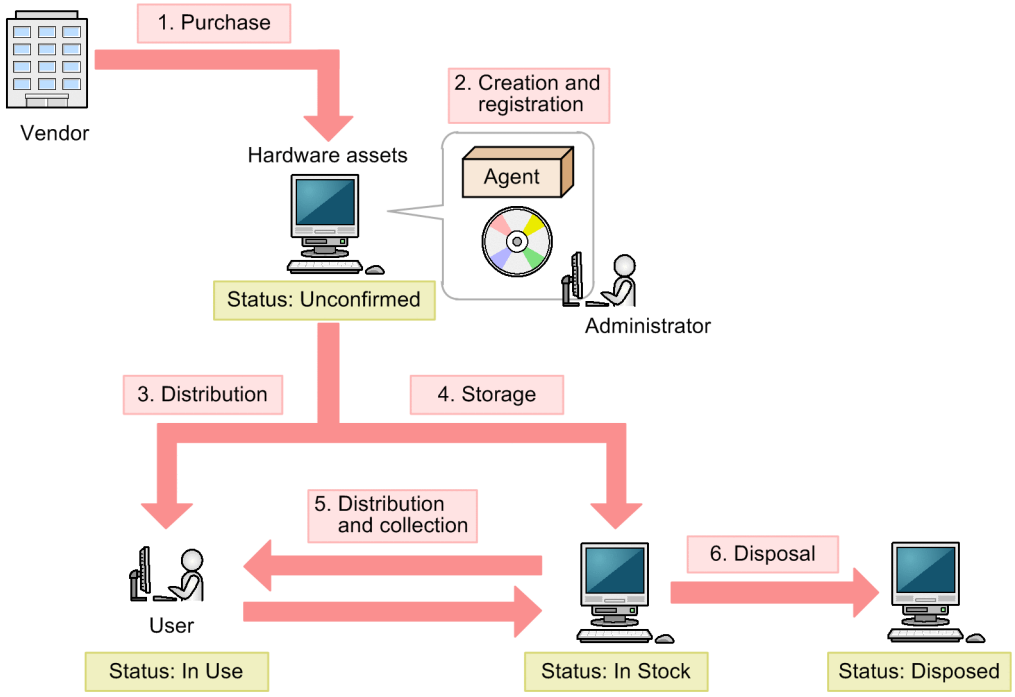
1.9 Managing hardware assets

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 2, 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: JP1/IT Desktop Management 2 - 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 2 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 2 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 2. By this association, you can import all information contained in the management ledger to the asset management items in JP1/IT Desktop Management 2.

   > **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 2 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 2 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**
>
> To specify an item as a mapping key, select an item for which a value exists both in JP1/IT Desktop Management 2 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**
>
> 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 or `setsecpolicy.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 2 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 2:

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 2.

   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 2, 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 2.

(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, or lease)
- 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

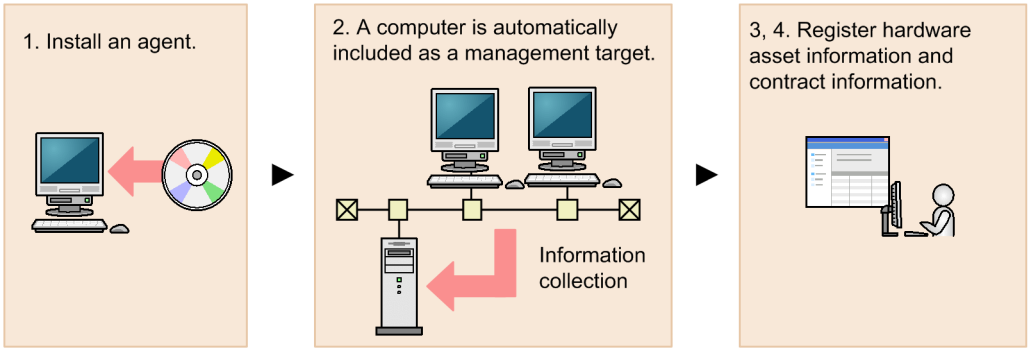
After purchasing computers, register the obtained user information in JP1/IT Desktop Management 2.

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 2. 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 2.

> **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 2.

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 Inventory 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
- 6.15 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 2, 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 2. 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 2, 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 2 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 2, 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 2, 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 2, 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 **Planned Hardware Asset Status** 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.

   Important

   If the network monitor is enabled on a device to be collected, you will need to disable the network monitor before collecting the device.

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:

- 15.6.2 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 2, 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 2 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 2 with the information of the devices found during the investigation.

Now the information in JP1/IT Desktop Management 2 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 2 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 2.

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 2 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 2 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 2 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 Inventory 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 Inventory 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 **Windows Agent Configurations and Create Agent Installers**.

Related Topics:

- 11.1.7 Changing the planned asset status
- 15.1.1 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 **Planned Hardware Asset Status** 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.

> **Important**
>
> If the network monitor is enabled on a device to be collected, you will need to disable the network monitor before collecting the device.

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:

- 15.6.2 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 Inventory 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.

   > **Important**
   >
   > If the network monitor is enabled on a device to be disposed of, you need to disable the network monitor before disposing of the device.

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 2:

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 2.

Then, the device repair operation is complete and the failure history is recorded in JP1/IT Desktop Management 2.

(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:

- 15.4.8 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 **Planned Hardware Asset Status** 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
- 15.6.2 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.

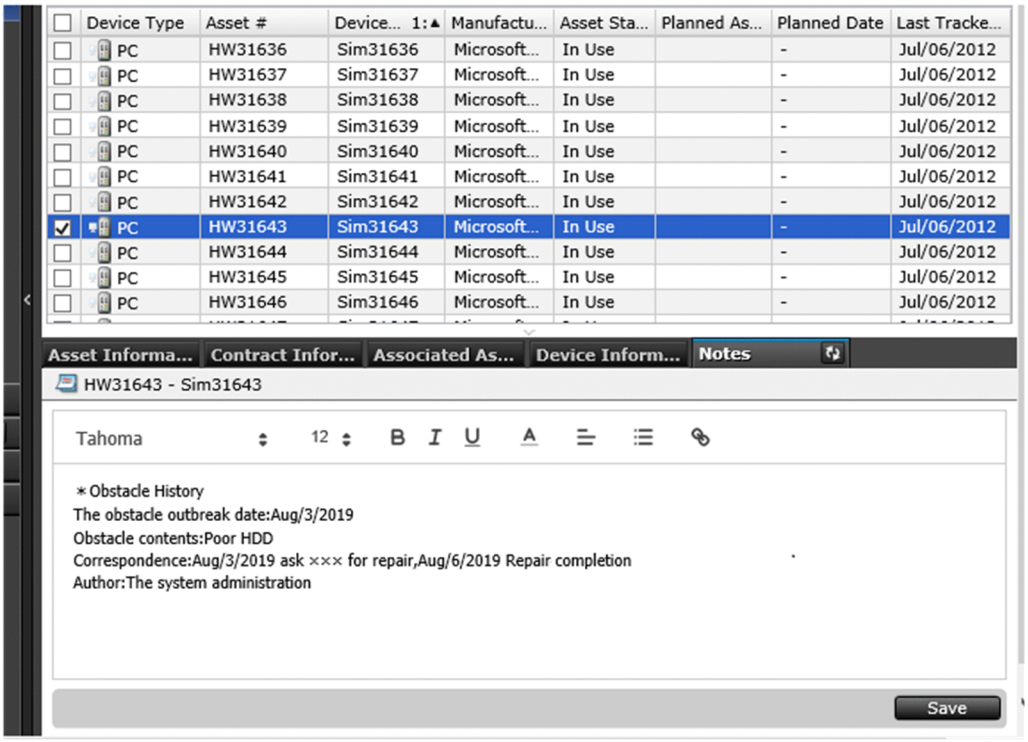
You can check the updated MAC address information in the **Device Inventory** view of the Inventory module and in the Network Filter Settings view. To display the **Network Filter Settings** view, in the Settings module, select **Network Access Control** and then **Network Filter Settings**.

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 2, and then investigate the unauthorized changes made to the device information.

1. In the operation view of JP1/IT Desktop Management 2, check the revision history of the device information.

   In the **Revision History** view of the Inventory 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 (ITDM-compatible) module of JP1/IT Desktop Management 2, 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.

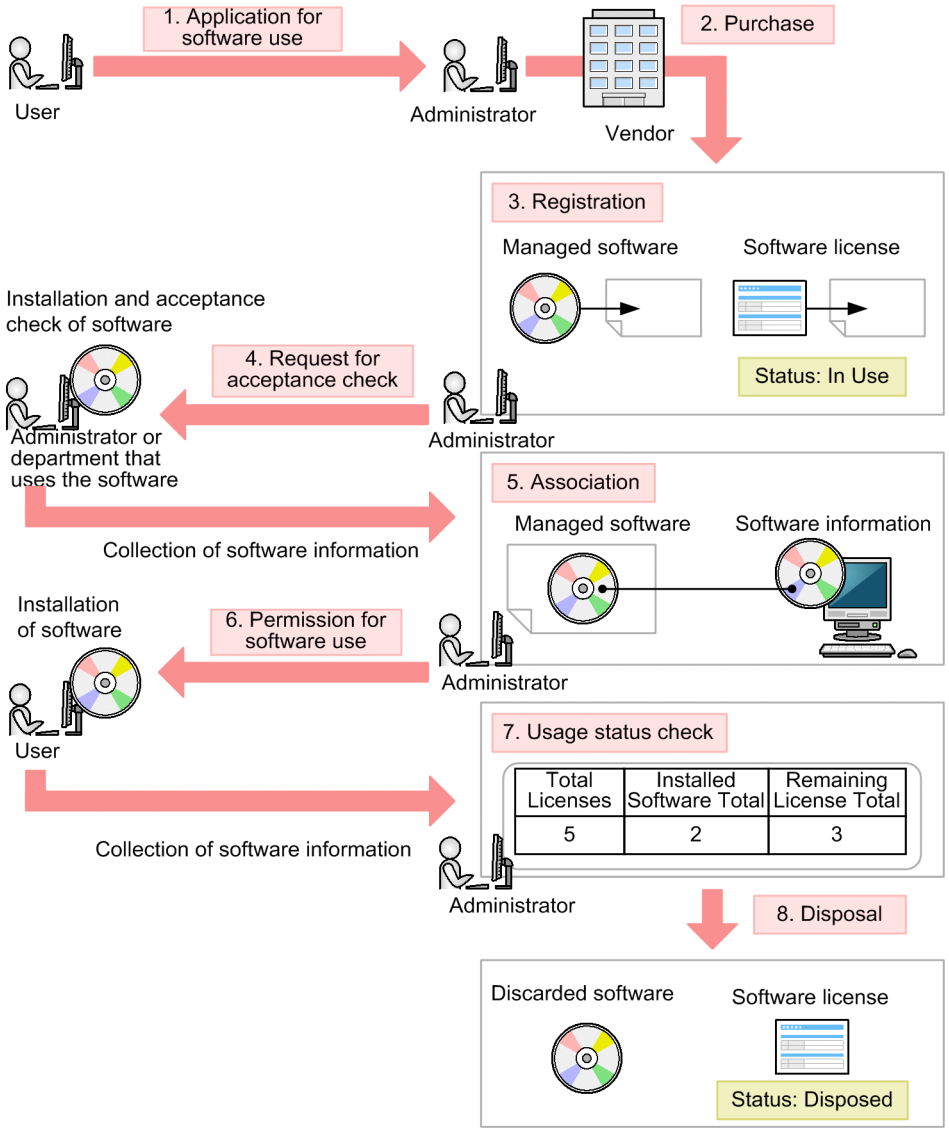
1.10 Managing software licenses

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 2, 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 2, 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 2. Also, register the managed-software information in JP1/IT Desktop Management 2 (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 2 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 2 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 2 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 2.

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 2 to check the usage status of the software licenses.

Now you can start the software license management tasks by using JP1/IT Desktop Management 2.

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 2 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 Inventory 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 2 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 2 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 2 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 2 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
- 15.6.2 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 2, 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 2 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 2 with the information of the software licenses found during the investigation.

Now the information in JP1/IT Desktop Management 2 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 2 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 2.

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 2 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 2 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 2 with the discarded software license.

Now the record of the discarded software license in JP1/IT Desktop Management 2 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 2.

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 2. 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 2 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 2, 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 2. 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 2, 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 2 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 2.

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 2 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 2 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 2 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:

- 15.6.2 Setting recipients of summary reports
- 15.8.1 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**
>
> 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 2, you can understand the cost involved in the operation of hardware assets and software licenses. JP1/IT Desktop Management 2 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**, **Software License Cost** , and **Other Cost** reports. You can also view the costs for the overall assets in the **All Assets Cost** report. 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

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

You can distribute software and files by using the distribution function to only the computers managed online.

Tip

If you distribute a file larger than 2 gigabytes, operate the distribution function as follows:

When Remote Install Manager is used

See *Distributing a file larger than 2 gigabytes* in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

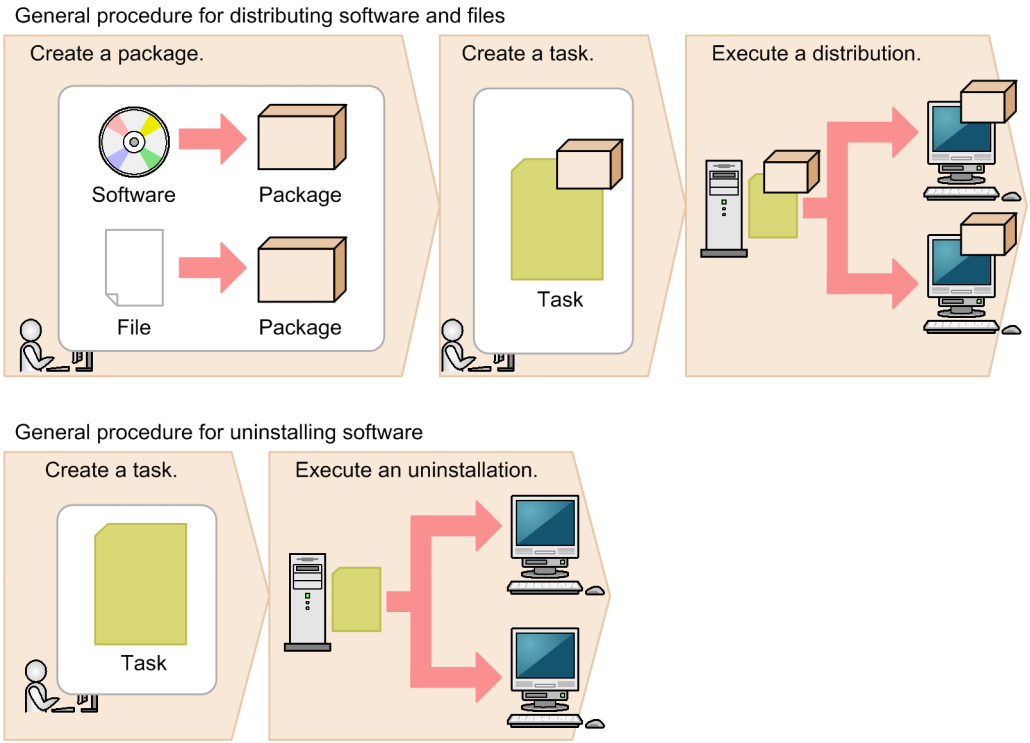
When the ITDM-compatible distribution is used

Split the file so that each piece of the file is less than or equal to 1 gigabyte, distribute the pieces, and then combine the split files after the distribution.

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 2 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.

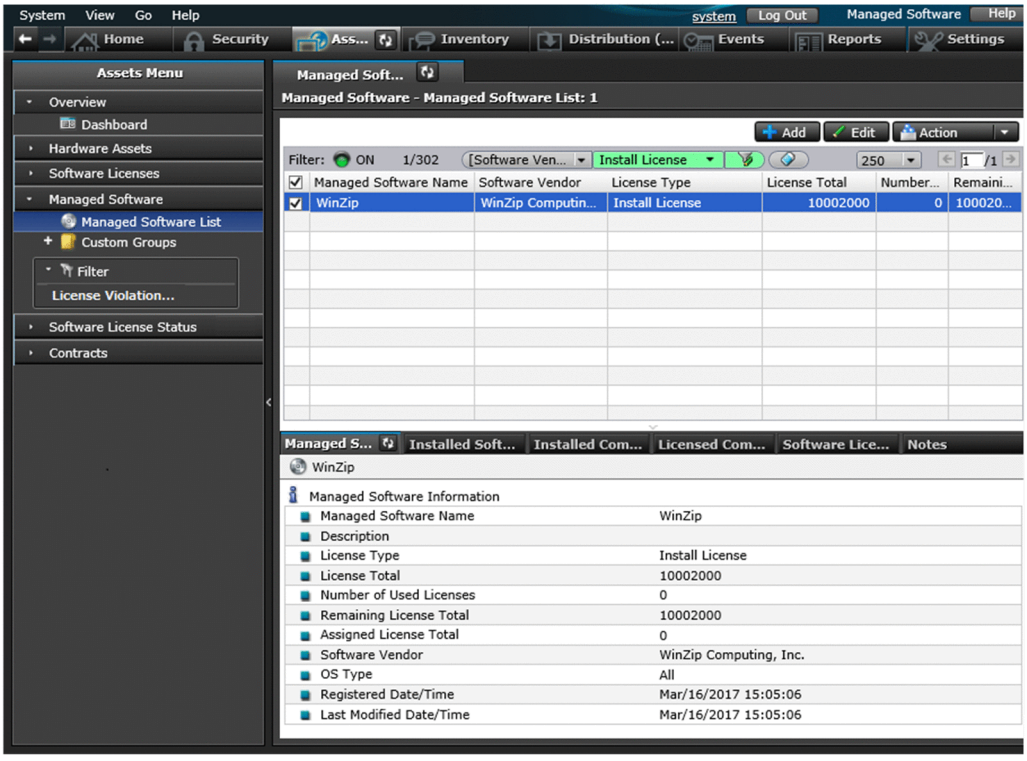
Related Topics:

- 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 2 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 (ITDM-compatible) 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 **Change Applicable 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 (ITDM-compatible) 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.

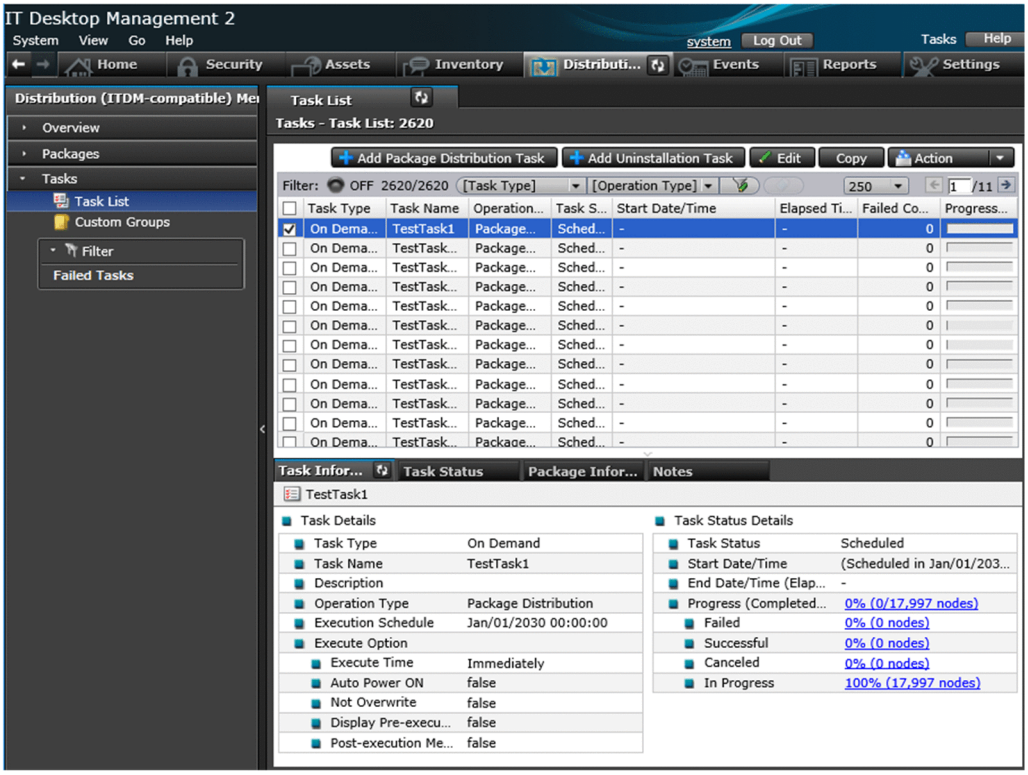
> **Important**
>
> You can register tasks to install Windows Store apps, but installation will not actually be performed. To install a Windows Store apps, you will need to perform installation on each target computer.

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 (ITDM-compatible) 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 2 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 (ITDM-compatible) 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.

   > **Tip**
   >
   > In the following cases, task information will be automatically deleted from the task list:

Tasks executed by the administrator:

- When 30 days have passed after the completion of distribution.
- When the number of devices subject to the task becomes 0.

Tasks executed by automatic countermeasure:

- When 7 days have passed after the completion of distribution.
- When the number of devices subject to the task becomes 0.
- Unset the Automatic Enforcement of Security Policy (Windows Update or Software Use).

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.

Tip

In **Distribution (ITDM-compatible)** - **Tasks** - **Task List**, the time displayed for Elapsed Time indicates the time that has elapsed since the starting time of the task, if the task status is In Progress. So it may be different from the actualtask completion time.

Related Topics:

- 15.7.1 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 (ITDM-compatible) 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 **Change Applicable 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 (ITDM-compatible) module.

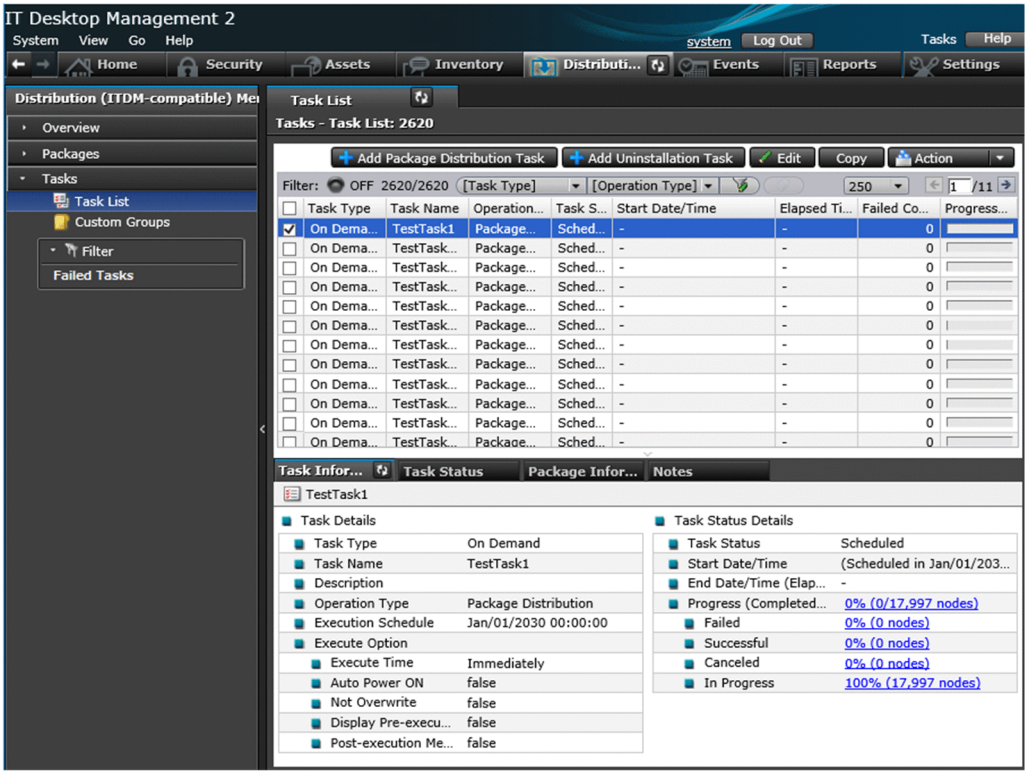
> **Tip**
>
> The users can change the schedule to execute the file distribution later if more urgent or important operation is in progress on their computers.

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 (ITDM-compatible) 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 2 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 (ITDM-compatible) 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.

   > **Tip**
   >
   > In the following cases, task information will be automatically deleted from the task list:
   >
   > Tasks executed by the administrator:
   >
   > - When 30 days have passed after the completion of distribution.
   > - When the number of devices subject to the task becomes 0.
   >
   > Tasks executed by automatic countermeasure:
   >
   > - When 7 days have passed after the completion of distribution.

- When the number of devices subject to the task becomes 0.
- Unset the Automatic Enforcement of Security Policy (Windows Update or Software Use).

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.

Tip

In **Distribution (ITDM-compatible)** - **Tasks** - **Task List**, the time displayed for Elapsed Time indicates the time that has elapsed since the starting time of the task, if the task status is In Progress. So it may be different from the actualtask completion time.

Related Topics:

- 15.7.1 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.

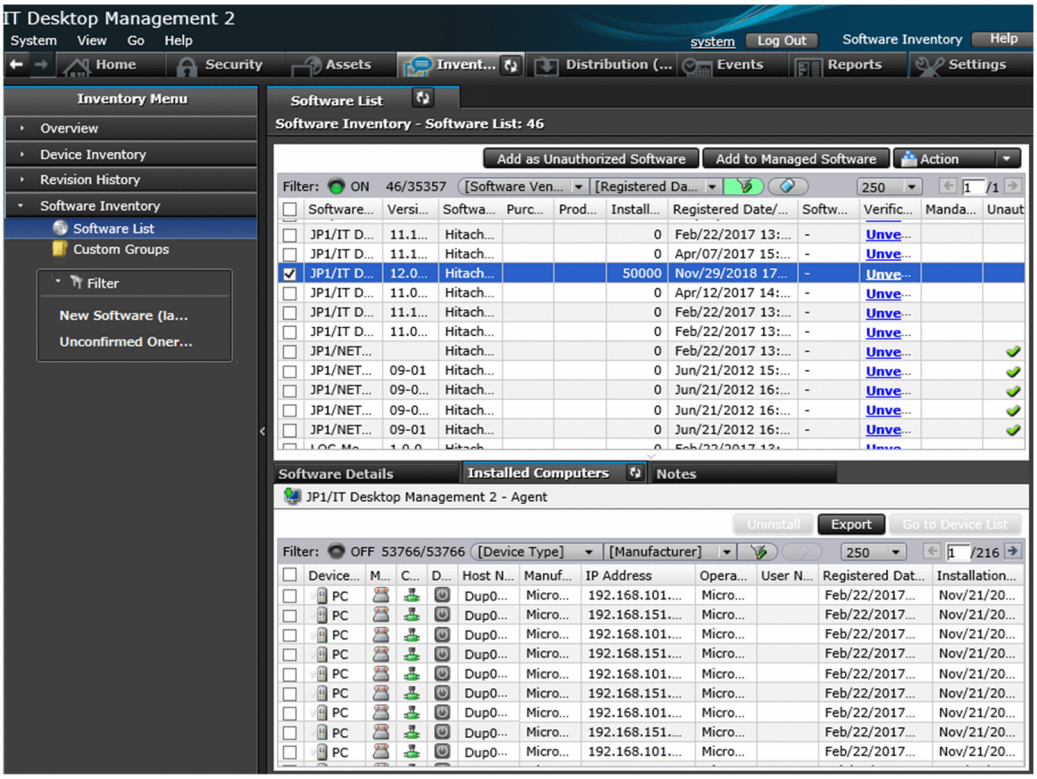
Related Topics:

- 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 Inventory 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 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 (ITDM-compatible) 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**.
   Only the software that completely matches the software name and version specified in the above view will be uninstalled.
6. In the **Select Target Computers** view, click the **Change** button.
7. In the **Change Applicable 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 (ITDM-compatible) 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.

Important

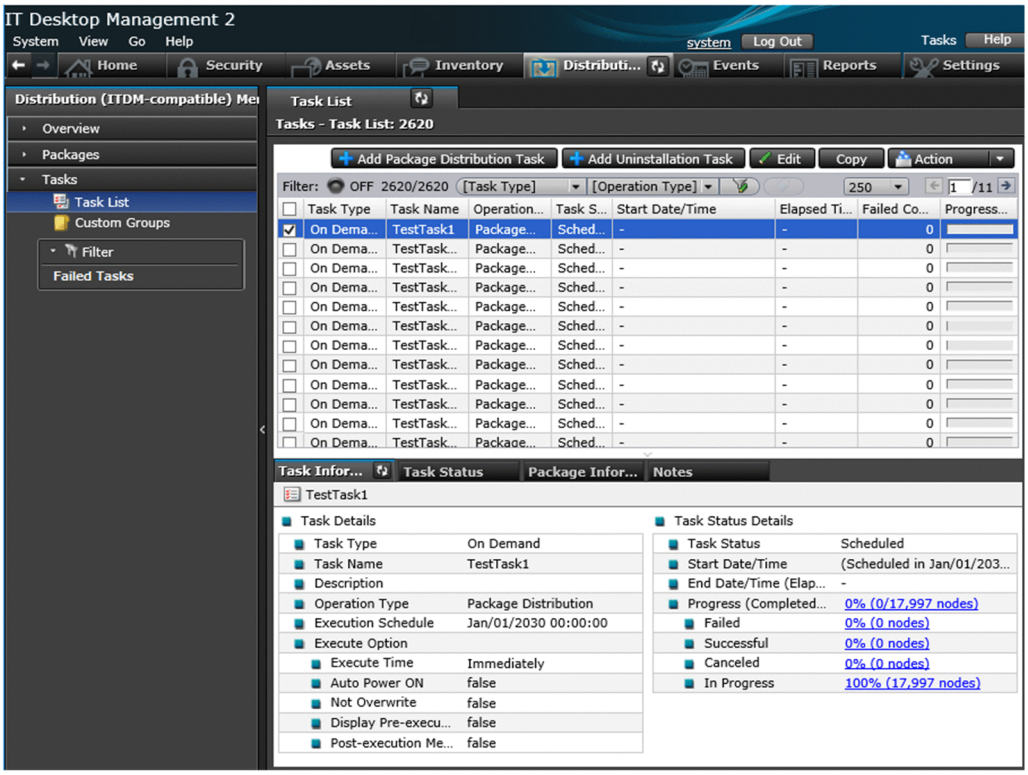
You can register tasks to uninstall Windows Store apps, but uninstallation will not actually be performed. To uninstall a Windows Store apps, you will need to perform uninstallation on each target computer.

Related Topics:

- 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 (ITDM-compatible) 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 2 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 (ITDM-compatible) 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.

   Tip

   In the following cases, task information will be automatically deleted from the task list:

   Tasks executed by the administrator:

   - When 30 days have passed after the completion of distribution.
   - When the number of devices subject to the task becomes 0.

   Tasks executed by automatic countermeasure:

   - When 7 days have passed after the completion of distribution.
   - When the number of devices subject to the task becomes 0.
   - Unset the Automatic Enforcement of Security Policy (Windows Update or Software Use).

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.

Tip

In **Distribution (ITDM-compatible)** - **Tasks** - **Task List**, the time displayed for Elapsed Time indicates the time that has elapsed since the starting time of the task, if the task status is In Progress. So it may be different from the actualtask completion time.

Related Topics:

- 15.7.1 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 2.

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 configurations 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 configurations 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 configurations 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

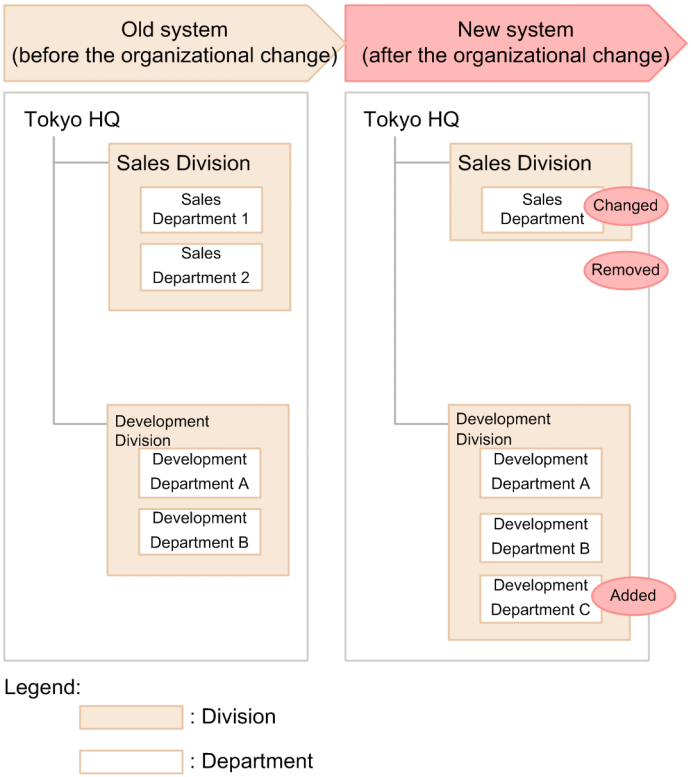
Related Topics:

- 1.7.1 Setting a security policy
- 15.1.1 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 configurations 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 2 from April 16.

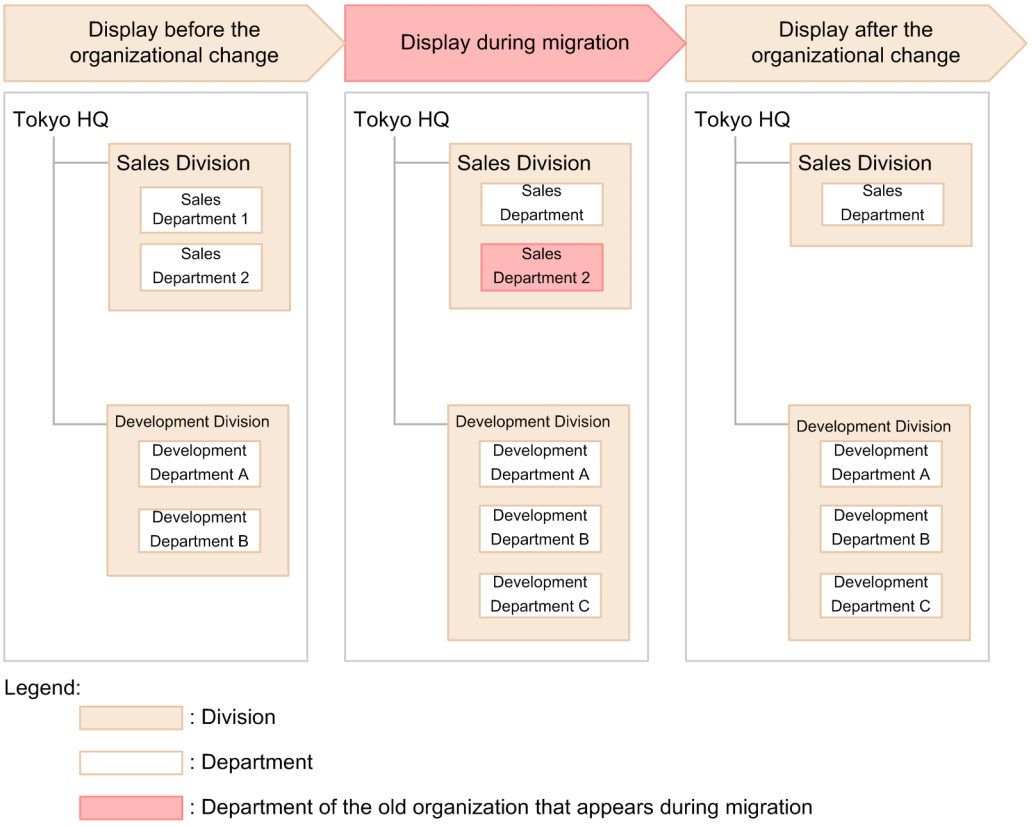
2. Inform the system administrators and departmental administrators of restrictions on the use of JP1/IT Desktop Management 2.

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 Inventory 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 **Assets** 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 2.

   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 configurations to the departments of the new organizational system.

   Assign security policies and agent configurations to the departments of the new organizational system in accordance with the assignment rules.

   After assignment is finished, you can create an agent configuration 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:

- 17.35 ioassetsfieldutil export (exporting the definitions of common management fields and additional management fields)
- A.6 Setting fields in the import file for the definitions of common management fields and additional management fields
- 16.2 Backing up databases
- 17.36 ioassetsfieldutil import (importing the definitions of common management fields and additional management fields)
- 16.3 Restoring databases
- 9.3.5 Assigning security policies
- 15.1.6 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 Inventory 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**
   >
   > 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
- 6.35 Removing only hierarchies that were used in the old organizational system

1.15 Configuring a VPN connection of a PC for use outside the company

You can use the distribution function of JP1/IT Desktop Management 2 to distribute a batch file for configuring a VPN connection environment on the PC for use outside the company. This operation enables you to easily configure the environment for that PC with JP1/IT Desktop Management 2.

> **Tip**
>
> JP1/IT Desktop Management 2 provides sample batch files that can configure the PC so that it can use the Windows-standard VPN client environment.

1.15.1 Adding the Windows-standard VPN profile and automatic VPN connection task to the PC for use outside the company

This subsection describes how to create the Windows-standard VPN profile in the PC for use outside the company and register the automatic VPN connection task in the Task Scheduler. This task is done on both the management server and the PC for use outside the company.

General procedure on the management server

1. Edit the sample batch file to create a VPN profile# and the sample batch file for VPN connections.

   For details about the sample batch files, see 1.15.3 Batch files used to configure the VPN connection.

   #: In Windows 7 or Windows Server 2008 R2, delete the section for executing the command to create the VPN profile in the sample batch file to create the Windows-standard VPN profile. For details, see (1) Sample batch file to create a VPN profile.

2. Distribute the batch files you edited in step 1 to the PC for use outside the company.

   See 12.1 Installing software on the computers to distribute the batch files to the PC for use outside the company.

   > **Tip**
   >
   > Specify the batch file to create the VPN profile you edited in step 1 in the command that is executed after the distribution.

General procedure on the PC for use outside the company

1. After the management server distributes the batch files, use an account with Administrator privileges to log on.

   A command prompt is displayed.

2. In the command prompt, specify the user name and password for signing in to the VPN server.

   The PC is now connected to the VPN server.

   > **Tip**
   >
   > Once the PC is successfully connected to the VPN server, this command prompt will not appear again later.

Important

- In the sample batch files, the user name and password for signing in to the VPN server are registered in the registry in plain text. If you want to register them in the registry in encrypted form, modify the sample batch files to suit your environment.
- If authentication fails at the time of the VPN connection, or if the PC fails to connect to the VPN server, a command prompt for signing in to the VPN server is displayed.

1.15.2 Removing the Windows-standard VPN profile and the automatic VPN connection task from the PC for use outside the company

This subsection describes how to remove the Windows-standard VPN profile and the task for automatic connection to the VPN that are created on the PC for use outside the company from the Task Scheduler. This task is done on the management server only.

General procedure on the management server

1. Edit the sample batch file to remove the VPN profile#.

   For details about the sample batch file, see 1.15.3 Batch files used to configure the VPN connection.

   #: In Windows 7 or Windows Server 2008 R2, delete the section for executing the command to remove the VPN profile in the sample batch file to remove the Windows-standard VPN profile. For details, see (3) Sample batch file to remove the VPN profile.

2. Distribute the batch file you edited in step 1 to the PC for use outside the company.

   See 12.1 Installing software on the computers to distribute the batch file to the PC for use outside the company.

   Tip

   Specify the batch file to remove the VPN profile you edited in step 1 in the Installation Command.

Important

If the batch file fails to remove the profile, redistribute the batch file to the target PC for use outside the company, or manually remove the VPN profile and the task on the PC for use outside the company.

1.15.3 Batch files used to configure the VPN connection

JP1/IT Desktop Management 2 provides sample batch files that configure a VPN connection environment for a PC for use outside the company. This subsection describes the sample batch files.

List of sample batch files provided by JP1/IT Desktop Management 2

Batch file	Storage location	Details
Sample batch file to create a VPN profile	*JP1/IT Desktop Management 2 - Manager-installation-folder*\mgr\sample\vpn\VpnProfileCreateSample.bat	Creates a Windows-standard VPN profile. It also registers the sample batch file for VPN connections in the Task Scheduler to automatically connect to the VPN.

Batch file	Storage location	Details
Sample batch file for VPN connections	*JP1/IT Desktop Management 2 - Manager-installation-folder*\mgr\sample\vpn\VpnConnectSample.bat	Automatically connects to the VPN if it is registered in the Task Scheduler when the VPN profile is created.
Sample batch file to remove the VPN profile	*JP1/IT Desktop Management 2 - Manager-installation-folder*\mgr\sample\vpn\VpnProfileRemoveSample.bat	Removes the Windows-standard VPN profile. It also removes the sample batch file for VPN connections from the Task Scheduler.

(1) Sample batch file to create a VPN profile

The sample batch file to create the VPN profile creates a Windows-standard VPN profile in a PC for use outside the company, and registers the sample batch file for VPN connections in the task scheduler.

Sections in the sample batch file to create the VPN profile

Parameter configuration

It is a set of parameters used in the batch file to create the VPN profile. If necessary, you edit them.

Execute the command to create the VPN profile

The command to create the VPN profile is executed. You edit this section to suit the target VPN server configurations (the type of VPN server and the authentication protocol).

Register the task schedule of the automatic VPN connection for logon

You edit this section if you change the execution timing of the batch file for VPN connections.

Register the task schedule of automatic VPN connection for system startup

You edit this section if the PC is connected to the VPN only when the user is logged on.

The following describes the details of each section:

Parameter configuration

Change the following parameters as needed:

- VPN connection name
- Address of the VPN server to connect to
- Path to Windows PowerShell (`powershell.exe`)
- Pre-shared key

Execute the command to create the VPN profile

A cmdlet to add the VPN profile (`Add-VpnConnection`) is executed as the Windows PowerShell command. The command used in the sample batch file is as follows:

```
Add-VpnConnection -Name VPN-connection-name-specified-in-the-parameter -Serv
erAddress address-of-the-connecting-VPN-server-specified-in-the-parameter -A
llUserConnection -RememberCredential -TunnelType L2TP -L2tpPsk pre-shared-ke
y -Force
```

For details about the `Add-VpnConnection` cmdlet, see the Windows PowerShell Help. The command should be changed to suit your environment.

Important

If the PC for use outside the company runs Windows 7 or Windows Server 2008 R2, remove this command line.

Register the task schedule of the automatic VPN connection for logon

The Windows `SCHTASKS` command is used to register the task in the task scheduler, so that the batch file for VPN connections can be executed automatically. In the sample batch file, the command is configured to be executed when any user logs on.

If you change the execution timing of the batch file for VPN connections, you modify the parameter of the `SCHTASKS` command in this command line. For details, see the Windows Help.

Register the task schedule of automatic VPN connection for system startup

The task is registered in the task scheduler so that the batch file for VPN connections can be executed automatically even when the user has not logged on. In the sample batch file, the task is configured to be executed when the system is started.

If you want the PC to automatically connect to the VPN only while the user logged on, remove this command line.

Important

If the security settings for VPN connections are modified, you need to create the VPN profile again or modify it with a PowerShell command.

(2) Sample batch file for VPN connections

The sample batch file for VPN connections is used to connect the PC for use outside the company to the VPN. Once the batch file is registered in the Task Scheduler, the PC can be connected to the VPN automatically.

Sections in the sample batch file for VPN connections

Parameter configuration

It is a set of parameters used in the batch file for VPN connections. If necessary, you edit them.

Determine the VPN connection conditions

You edit this section if the conditions for connecting the VPN must be determined or if an external program determines the conditions.

Obtain the VPN connection information from the registry

The VPN connection information is obtained from the registry. You edit this section if the VPN connection information is registered in encrypted form or if the information is stored anywhere other than the registry.

Enter the VPN connection information and register it in the registry

The VPN connection information is entered to register it in the registry. The information is registered in the registry in plain text. You edit this section if the information is registered in the registry in encrypted form or if the information is stored anywhere other than the registry.

Connect to the VPN

The PC is connected to the VPN. The `rasdial.exe` command in Windows is used for the VPN connection. You edit this section if another command is used to connect to the VPN. You also do so if a re-entry request is made when the connection fails and if the registry registration is modified.

The following describes the details of each section:

Parameter configuration

Change the following parameters as needed:

- VPN connection name
- Path to Windows PowerShell (`powershell.exe`)
- Address of the DHCP server for the internal network
- Path and item for the registry key that stores the VPN connection information

Determine the VPN connection conditions

The section determines the conditions for connecting to the VPN. The sample batch file determines that the connection comes from the outside of the company and connects the PC for use outside the company to the VPN, if the DHCP server used by the PC differs from the DHCP server for the internal network specified in the parameter.

You can also create an external program that suits your environment and determines whether the connection is from the outside, so that the PC can be connected to the VPN depending on the result of executing the program.

Obtain the VPN connection information from the registry

The VPN connection information is obtained from the registry. If the information is registered in the registry in encrypted form, you add an operation to decrypt it.

Enter the VPN connection information and register it in the registry

If the VPN connection information is not stored in the registry, a command prompt appears, asking the user to enter the user name and password for signing in to the VPN server. The entered information is registered in the registry.

In the sample batch file, the VPN connection information is registered in the registry in plain text. If you want to register encrypted text, add an operation to encrypt the information.

Connect to the VPN

The PC is connected to the VPN. In the sample batch file, the following Windows command is used to connect to the VPN:

```
rasdial.exe VPN-connection-name-specified-in-the-parameter user-ID-obtained
password-obtained
```

For details about the `rasdial.exe` command, see the Windows Help.

Tip

If the user name and password for signing in to the VPN server have been changed, the connection fails. If this happens, a command prompt appears, asking the user to specify the user ID and password again. The entered connection information is registered in the registry.

(3) Sample batch file to remove the VPN profile

The sample batch file to remove the VPN profile deletes the Windows-standard VPN profile from the PC for use outside the company, and removes the task that executes the sample batch file for VPN connections from the Task Scheduler.

Sections in the sample batch file to remove the VPN profile

Parameter configuration

It is a set of parameters used in the batch file to remove the VPN profile. If necessary, you edit them.

Disconnect from the VPN

The connection to the VPN is disconnected. You edit this section if you want to change the command to be used.

Execute the command to remove the VPN profile

The command to remove the VPN profile is executed. You edit this section to suit the target VPN server configurations (the type of VPN server and the authentication protocol).

Remove the VPN connection information from the registry

The VPN connection information is removed from the registry. You edit this section if the information is stored anywhere other than the registry.

Remove the task schedule of the automatic VPN connection for logon

You edit this section if the execution task of the batch file for VPN connections is not registered in the Task Scheduler.

Remove the task schedule of the automatic VPN connection for system startup

You edit this section if the profile is configured for the PC to connect to the VPN only while the user logged on in *(1) Sample batch file to create a VPN profile*.

Remove the file distributed upon creation (removal of the distribution-destination folder)

You edit this section if you want to remove the distribution-destination folder for the batch file specified in *1.15.1 Adding the Windows-standard VPN profile and automatic VPN connection task to the PC for use outside the company*.

The following describes the details of each section:

Parameter configuration

Change the following parameters as needed:

- VPN connection name
- Path to Windows PowerShell (`powershell.exe`)
- Path for the registry key that stores the VPN connection information

Disconnect from the VPN

The connection to the VPN is disconnected. In the sample batch file, the following Windows command is used to disconnect from the VPN:

```
rasdial.exe VPN-connection-name-specified-in-the-parameter /disconnect
```

For details about the `rasdial.exe` command, see the Windows Help.

Execute the command to remove the VPN profile

A cmdlet to remove the VPN profile (`Remove-VpnConnection`) is executed as the Windows PowerShell command. The command used in the sample batch file is as follows:

```
Remove-VpnConnection -Name VPN-connection-name-specified-in-the-parameter -A
llUserConnection -Force
```

For details about the `Remove-VpnConnection` cmdlet, see the Windows PowerShell Help. The command should be changed to suit your environment.

> **Important**
>
> If the PC for use outside the company runs Windows 7 or Windows Server 2008 R2, remove this command line.

Remove the VPN connection information from the registry

The VPN connection information is removed from the registry.

Remove the task schedule of the automatic VPN connection for logon

The task that is executed when the user logs on, registered in *(1) Sample batch file to create a VPN profile*, is removed.

Remove the task schedule of the automatic VPN connection for system startup

The task that is executed when the system is started, registered in *(1) Sample batch file to create a VPN profile*, is removed.

Remove the file distributed upon creation (removal of the distribution-destination folder)

The distribution-destination folder is removed to delete files, such as the file distributed when the VPN profile is created or the log file that is output when the sample batch file is executed.

1.15.4 Operational precautions when VPN connections are used

This subsection provides the operational precautions when VPN connections are used.

- If many VPN-connected PCs for use outside the company are managed simultaneously, the Windows-standard VPN server gets more access, which may cause disconnection of the VPN connections. Therefore, we recommend that you configure the PCs for use outside the company that are to be connected to the VPN so that they can access the VPN server less frequently. An example of this may include specifying a longer polling interval to a higher-level system.
- If the host name cannot be resolved between a PC for use outside the company and the management server, the server cannot communicate with the PC. Configure the settings so that the management server starts processing when the PC polls the server.

1.16 Managing devices used outside the company

There are two ways to manage computers used outside the company with JP1/IT Desktop Management 2: by connecting computers with the management server via VPN or by connecting computers with a higher system via the Internet gateway.

This section describes how to manage the connection of computers to a higher system via the Internet gateway. This section also describes how to manage the expiration date of the server certificate set on the Internet gateway server.

> **Tip**
>
> To connect computers to the management server via VPN, you have to specify VPN connection settings on the managed computers. For details, see 1.15 Configuring a VPN connection of a PC for use outside the company.

To connect computers with a higher system via the Internet gateway:

1. Install an agent on a managed computer. For details, see (2) Installing agents on computers.
2. In the Agent Configurations view of the Settings module, under **Basic settings**, select the **Perform HTTPS communication with the higher system via the Internet Gateway** check box.
3. Under **Perform HTTPS communication with the higher system via the Internet Gateway** in **Basic settings**, set the host name and port number of the Internet gateway server in **Internet Gateway**.
4. Change **Communication Settings - Communication Error Settings - Timing to Assume that a Communication Error Occurred - Assume that a communication error occurred if no response is received from communication software within the specified period** setting from 5 minutes to 30 minutes.
   When collecting files with large capacity exceeding 1 GB with the remote collection function, set the value to 120 minutes. If the setting value is increased, when there is no response from the server due to a temporary failure such as communication failure or server failure, it takes time until it is assumed as an error, so the time to the next polling will be longer.

> **Tip**
>
> To set Internet gateway connection authentication, in the Agent Configurations view of the Settings module, under **Basic settings**, in **Internet Gateway Communication Settings**, select the **Authenticate the User** check box. For **User ID** and **Password**, specify the user name and password for basic authentication that you have set for Default Web Site in Microsoft Internet Information Services on the Internet gateway server.

> **Tip**
>
> If a computer used outside the company needs to go through a proxy server in order to communicate with the Internet gateway, set information regarding the proxy server to be used by selecting the **Use Proxy Server** check box (which is displayed in the Agent Configurations view of the Settings module, under **Basic settings**, in **Internet Gateway Communication Settings**).
>
> Furthermore, during agent setup, you can select whether to use a value set with the management server or the one set with the client.

To manage the expiration date of the server certificate for the Internet gateway server:

The server certificate set for the Internet gateway server must be updated to ensure that it does not expire. Registering the server certificate as contract information in JP1/IT Desktop Management 2 allows you to manage the expiration date of the server certificate.

Registering contract information for the server certificate

In the Assets module, select **Contracts** and then **Contract List**. In the displayed view, enter contract information. For details about this procedure, see 11.3.1 Adding contract information. For example, enter the following contract information:

- Contract Name: Server certificate for the Internet gateway
- Contract Term: Expiry date of the server certificate
- Associated Information: Hardware assets of the Internet gateway

Add description and attachments as necessary.

Checking the contract of the server certificate that is about to expire

In the Home module or in the **Dashboard** view that is displayed by selecting **Overview** in another module, refer to the **Expired Contracts (next 3 months)** panel.

Tip

- If the **Expired Contracts (next 3 months)** panel is not displayed, display it by selecting the **View** menu and then setting **Panel Layout**. For details about this procedure, see 5.1 Setting the panels to be displayed and their layout.
- If you change the contract status of the server certificate to Expired, the server certificate in question does not show up in the **Expired Contracts (next 3 months)** panel.

To enable switching the connection destination of managed computers which brings to inside of the company:

Managed computers taken out of the company connect to the Internet gateway. You can change settings that these computers connect to the management server directly when they are brought to inside of the company.

To do so, open the Agent Configurations view of the Settings module, and then select **Basic settings**, and then **Perform HTTPS communication with the higher system via the Internet Gateway**. Select the **Communicate directly with the higher system if the Internet Gateway is unavailable** check box.

Tip

In an environment where a proxy server is used to access the Internet from the internal network, the computers cannot access the Internet gateway unless you set a proxy server for the internal network by opening the Agent Configurations view and then selecting **Basic settings**, **Internet Gateway Communication Settings**, and then **Use Proxy Server**. This means that by simply selecting **Basic settings**, **Perform HTTPS communication with the higher system via the Internet Gateway**, and then the **Communicate directly with the higher system if the Internet Gateway is unavailable** check box, computers connected to the internal network can directly access the management server without passing through the Internet gateway (in other words, there is no need to edit the proxy server setting).

Tip

In an environment where a proxy server is not used for access to the Internet from the internal network, set a firewall such that an attempt to access the Internet gateway from the internal network fails with an error.

1.17 Operation in a large-scale environment

In JP1/IT Desktop Management 2, if you enable the large-scale management option when installing JP1/IT Desktop Management 2 - Manager, you can manage a maximum of 300,000 devices.

The following describes the operation methods in a large-scale environment.

1.17.1 Operating the management server in a large-scale environment

In asset management using JP1/IT Desktop Management 2, device information is collected from agent devices and agentless devices into the management server. The asset management functionality, such as security judgment and report calculation, is then performed based on the collected device information.

The amount of data in the device information collected into the management server has to be decreased, so that the server can operate stably with its limited resources. Operations such as security judgment can make the management server busy. Performing such operations periodically, instead of doing them when triggered by collection of device information, can reduce the load on the server.

Configuring the collection of device information from a managed device

The default values for the following settings are the recommended values for when managing 300,000 devices. The same applies to agent configuration for agent devices connected to the management relay server.

Reducing these setting values causes the amount of data for device information collected by the management server to increase, which may place a burden on the management server.

Agent configuration

- **Timing of communication with the higher system** under **Basic settings**
  - **Monitoring Interval (Security)**
  - **Monitoring Interval (Others)**
  - **Polling interval**

Tuning the security judgment function

The security judgment function puts a high load on the server. As a result, it may take several hours for the function to finish as the number of managed devices increases. The parameters for security judgment can be tuned based on the specifications of the management server.

Tuning the start time of security judgment

Security judgment on a managed device starts at 18:00 by default. The result of the security judgment is used as input for report calculation that starts by default at 23:00. Adjust the start time of security judgment so that it can be completed by 1:00 (25:00), because security report calculation starts at 1:00 (25:00), which is two hours after the start of report calculation.

The start and end times of the judgment are logged in the publishing log file. You can specify the start time of security judgment by opening the Settings module from the management window and then selecting **Security Schedule**.

Tuning the number of processes handling security judgment

Increasing the value of the following property in the configuration file helps improve the performance when security judgment is performed. Do so if the CPU load is low.

Number of processes for handling security judgment (`Mgrsrv_jdnmssecurityctrl_L`)

While it does vary depending on the environment, it takes approximately one hour to perform security judgments for 50,000 devices with ten processes for handling security judgment.

Changing the timing for compilation of software license information

Software license information is normally compiled each time device information is updated.

The more managed devices there are, the slower installed software information is reflected for devices. Furthermore, as the number of software licenses in use is compiled after the device installed software information is updated, the number will be inaccurate for a time.

By setting the following property in the configuration file, you can change the timing for compilation of software license information to every three minutes.

```
Software_Licenses_Totalization_Method=SCH
```

> **Note**
>
> If you set this property, it may take up to three minutes after the device installed software is reflected on the window until the compilation result is reflected.

Backing up the database

The management server must be stopped to back up the database. Therefore, consider the conditions, such as the days of week and times when the management server is not used, before the backup.

Related Topics:

- 6.39 Tuning the settings for collecting device information
- 15.3.1 Changing the schedule for security judgment

1.17.2 Operation of the management window in a large-scale environment

As the number of managed devices increases, the management window tends to respond more slowly. Panels displayed in the Home module or the dashboard contain a large amount of data, and as a result it takes time to show them and the server bears a high load. If it takes time to show a module that is often displayed immediately after logins or when you move to a different module, operability will be deteriorated seriously. We recommend that you usually use the default panels, but show the ones you need as appropriate for your operation.

Note that some panels are not visible by default in the large-scale environment, but they have alternate windows. For details, see Differences when the large-scale management server is used for operation in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

1.17.3 Notes for operation in the large-scale environment

The following provides the notes for operation in the large-scale environment.

Security settings (automatic countermeasure)

In the large-scale environment, distribute software through Remote Install Manager to take measures. Disable the automatic countermeasure settings for the following software because the distribution function (ITDM-compatible) will be performed as an automatic countermeasure:

- Program updates
- Mandatory software
- Unauthorized software

Distribution of software and files

We recommend that you use Remote Install Manager for the large-scale environment to distribute software and files.

Network connection control

Make sure that your network connection control list contains 262,140 pieces or less of registered network information (MAC address or IP address). For example, if one device has two pieces of network information, 260 thousand pieces of network information for 130 thousand devices will be registered in network control list.

If the number of addresses in the network control list is likely to exceed 262,140, consider using the management relay server.

2 Registering a Product License

This chapter describes how to register a product license. And also, describing how to unregister a product license.

2.1 Registering a product license

By registering product licenses in JP1/IT Desktop Management 2, you can manage as many devices as the number of licenses you have registered.

Note that in a multi-server configuration, you can register product licenses only on primary management servers and on the management relay servers for which license registration is authorized.

To register a product license:

1. Display the Login window.
2. Click the **License** button in the Login window.
3. In the **License Details** dialog box that appears, click the **Register License** button.
4. In the **File Upload** dialog box that appears, select a license key file, and then click the **Open** button.
5. When license registration is complete, the **License Registration Completed** dialog box appears. Click the **OK** button.

License registration is complete.

Tip

Because the license key file is necessary when you replace the management server, be sure to store the file. For details on replacement, refer to the description of *Replacing a management server* in the manual *JP1/IT Desktop Management 2 Configuration Guide*.

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 2 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

2.4 Procedure for setting product license information for a management relay server

The product licenses within the share range of a management relay server can be managed by setting the information about the product licenses on that server. To set product license information on a management relay server, execute the `distributelicense` command from the primary management server. For details about the `distributelicense` command, see the related topics.

Tip

After executing the `distributelicense` command (to permit license registration to the management relay server), you need to register the product license.

Tip

You can use the Events module for the primary management server to check whether all management relay servers are completely configured. In addition, to check whether a specific management relay server is completely configured, you can use the Events module in the operation window for that management relay server. If setting fails, check the detailed information about the event, and then execute the `distributelicense` command again.

Related Topics:

- 2.1 Registering a product license
- 17.37 distributelicense (distributing licenses)

2.5 Procedure for checking the total number of devices discovered in the share range of a product license

You can identify how many more product licenses you need in a given share range by finding out the total number of devices discovered in that share range. You can do so by using the sharing-source server or a higher management server. From the operation window of the server, select **Discovery**, display the **Discovered Nodes** window, and filter the **Discovered Nodes** area.

The checking procedure depends on the pattern of the operation window used and applicable system configuration as follows:

Pattern 1

- Operation window used: Operation window of the sharing-source server
- System configuration: The management relay servers under the sharing-source server include those that are not sharing-destination servers.

Pattern 2

- Operation window used: Operation window of the sharing-source server
- System configuration: All the management relay servers under the sharing-source server are sharing-destination servers.

Pattern 3

- Operation window used: Operation window of a management server higher than the sharing-source server
- System configuration: Any

The procedure for each pattern is as follows:

To check the total number of devices discovered in a share range (pattern 1):

1. Select **Discovery**, and then display the **Discovered Nodes** window.
2. Select **Show only the devices that are directly under the device**.
   Only the devices discovered by the sharing-source server are displayed in **Discovered Nodes**. Check the number of displayed devices.
3. Clear the **Show only the devices that are directly under the device** check box.
4. Set filtering conditions to filter all discovered devices (**Discovered Nodes**).
   As filtering conditions, specify the routes from a sharing destination to the sharing source in **Route to the Managing Source**. Only the devices that satisfy the filtering conditions are displayed in **Discovered Nodes**. Check the number of displayed devices.
5. Perform step 4 for the routes from all sharing destinations to the sharing source.
6. Find the total number of the devices confirmed in step 2, step 4, and step 5.

The total found here is the total number of devices discovered in the share range.

To check the total number of devices discovered in a share range (pattern 2):

1. Select **Discovery**, and then display the **Discovered Nodes** window.
2. Clear the **Show only the devices that are directly under the device** check box.

The number of devices that the management server discovered in the share range is displayed in **Discovered Nodes**.

To check the total number of devices discovered in a share range (pattern 3):

1. Select **Discovery**, and then display the **Discovered Nodes** window.
2. Clear the **Show only the devices that are directly under the device** check box.
3. Set filtering conditions to filter all discovered devices (**Discovered Nodes**).

   As the filtering conditions, in **Route to the Managing Source**, specify the route to the local server from a management relay server in the share range you are checking. Only the devices that satisfy the filtering conditions are displayed in **Discovered Nodes**. Check the number of displayed devices.
4. Perform step 3 for the routes from all management relay servers in the share range you are checking to the local server.
5. Total the number of devices you confirmed in steps 3 and 4.

The total found here is the total number of devices discovered in the share range.

2.6 Deleting product licenses

This section describes how to delete product licenses.

> **Important**
>
> Before deleting product licenses, back up databases and operation logs just in case of hardware failure or other unexpected events.

> **Important**
>
> After deleting product licenses, re-register product licenses in the management server.

To delete product licenses:

1. Stop services of the management server.

   In the case of a non-cluster configuration, execute the `stopservice` command on the management server.

   In the case of a cluster configuration, stop services in the following order by using the cluster manager on the active management server:

   - JP1_ITDM2_Web Server
   - JP1_ITDM2_Web Container
   - JP1_ITDM2_Service
   - JP1_ITDM2_Agent Control
   - JP1_ITDM2_DB Cluster Service
   - JP1_ITDM2_DB Service

2. Delete product licenses by executing the `deletelicense` command on the management server.

   For details about the `deletelicense` command, see 17.42 deletelicense (delete licenses).

3. Start services on the management server.

   In the case of a non-cluster configuration, execute the `startservice` command on the management server. Executing the `startservice` command causes an error message (KDEX4065-E) to be output to the command prompt. This error message appears when some of the services are started without the licenses being registered. This error message is therefore irrelevant to the license deletion procedure.

   In the case of a cluster configuration, start services in the following order by using the cluster manager on the active management server:

   - JP1_ITDM2_DB Service
   - JP1_ITDM2_DB Cluster Service
   - JP1_ITDM2_Web Container
   - JP1_ITDM2_Web Server

3 Logging in to the Operation Window

This chapter describes how to log in to the operation window of JP1/IT Desktop Management 2.

3.1 Logging in

Perform user authentication in the Login window. If successfully authenticated, you can then log in to JP1/IT Desktop Management 2.

You need to register a license for JP1/IT Desktop Management 2 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/jp1itdm.jsp

   #: 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.

In case of ITDM2 authentication, the default user ID is `system` and 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.

If you are logging in by using JP1 authentication, log in by using a JP1 user ID that registered on the JP1/Base authentication server in advance.

> **Tip**
>
> In case of ITDM2 authentication, passwords are valid for the number of days specified as the password expiration period in the **Other Settings** view during setup. 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 the password expiration period has passed, the **Change Password** dialog box is displayed when you log in.

> **Important**
>
> In case of ITDM2 authentication, if the number of consecutive login failures before the account is locked has been specified in the **Other Settings** view during setup, a user account is locked if login fails consecutively the specified number of times. 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 2, 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 2 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 the number of days specified as the password expiration period in the **Other Settings** view during setup. 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 the password expiration period has passed, 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 2, 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.

> **Important**
>
> The user account that is added by selecting **User Management** in the Settings module and then **Account Management** cannot be used as a login account for JP1 authentication. However, such an account can be used to receive notifications of events or digest reports. To add a login account to perform JP1 authentication, add a JP1 user on the JP1/Base authentication server.

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 **Add User Account** dialog box that appears, enter the user account information, and then click **OK**.
   The password specified here is the initial password. When user account registration is complete, users will be prompted to change their password when they first log in. Notify users of new accounts that they will need to change their passwords when prompted.
   For details about specifying permissions and task allocation, see 1.3.1 General procedure for determining the settings to be specified for each user account.

The user account is added and listed in **User Account List**.

> **Important**
>
> Even if an account is not actually added, an event indicating that the account is deleted or added is output. This symptom occurs when all of the following conditions are met:
>
> - The upgraded database is used.
> - Security details were obtained before the upgrade.
> - Security details are updated for the first time after the upgrade.

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.

> **Important**
>
> A JP1 user cannot edit their own user account. To change the information of a JP1 user, you must edit the information on the JP1/Base authentication server.

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 there is an administrator whose account has been locked, the **Status** item will appear in the **Edit User Profile** dialog box. Select **Enabled** to unlock the account.

Related Topics:

- 4.1 Adding a user account
- 4.3 Removing a user account
- 4.9 Unlocking 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.

> **Important**
>
> Even if an account is not actually deleted, an event indicating that the account is deleted or added is output. This symptom occurs when all of the following conditions are met:
>
> - The upgraded database is used.
> - Security details were obtained before the upgrade.
> - Security details are updated for the first time after the upgrade.

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 the number of days specified as the password expiration period in the **Other Settings** view during setup. 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 the password expiration period has passed, the **Change Password** dialog box is displayed 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.

> **Important**
>
> A JP1 user cannot change their own password. To change the information of a JP1 user, you must edit the information on the JP1/Base authentication server.

> **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 the number of days specified as the password expiration period in the **Other Settings** view during setup. 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 the password expiration period has passed, the **Change Password** dialog box is displayed 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 2 using the reset password.

The administrator logs in JP1/IT Desktop Management 2 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

If the number of consecutive login failures before the account is locked has been specified, a user account is locked if login fails consecutively the specified number of 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**.

> **Tip**
>
> The **Status** item and the ability to select **Enabled** are only available for locked user accounts.

The user account is unlocked.

> **Tip**
>
> If no other administrator has user account management authority, restart the management server. The user account is unlocked.

4.10 Adding email notification destinations

To add email notification destinations, in the Settings module, select **User Management** and then **Account Management**.

If you add email notification destinations in advance, you can use the email notification function even if no user accounts are registered in the **Account Management** window (which can be accessed by selecting **User Management** in the Settings module). For example, if JP1 authentication is used to log in to JP1/IT Desktop Management 2, you can use the email notification function by adding the email address of a JP1 user as a recipient of notification emails.

Note that, to add email notification destinations, you must have the user account management authority.

To add email notification destinations:

1. Go to the Settings module.
2. In the menu area, select **User Management** and then **Account Management**.
3. At the bottom of the information area, in the email notification destinations area, click the **Add** button.
4. In the dialog box that appears, enter information about the email notification destination, and then click **OK**.

The email notification destination is added and displayed in the list of email notification destinations.

Related Topics:

- 4.11 Editing email notification destinations
- 4.12 Removing email notification destinations

4.11 Editing email notification destinations

To edit email notification destinations, in the Settings module, select **Account Management** and then **User Management**.

Note that, to edit email notification destinations, you must have the user account management authority.

To edit email notification destinations:

1. Go to the Settings module.
2. In the menu area, select **User Management** and then **Account Management**.
3. At the bottom of the information area, in the email notification destinations area, click the **Edit** button for the email notification destination whose information you want to edit.
4. In the dialog box that appears, edit the information about the email notification destination, and then click **OK**.

Information about the selected email notification destination is updated.

Related Topics:

- 4.10 Adding email notification destinations
- 4.12 Removing email notification destinations

4.12 Removing email notification destinations

To remove email notification destinations, in the Settings module, select **Account Management** and then **User Management**.

Note that, to remove email notification destinations, you must have the user account management authority.

To remove email notification destinations:

1. Go to the Settings module.
2. In the menu area, select **User Management** and then **Account Management**.
3. At the bottom of the information area, in the email notification destinations area, select the email notification destination that you want to remove, and then click the **Remove** button.
   You can select and remove multiple email notification destinations at once.
4. In the dialog box that appears, click **OK**.

The selected email notification destinations are removed.

Related Topics:

- 4.10 Adding email notification destinations
- 4.11 Editing email notification destinations

5 Window Operations

This chapter describes common operations that you can perform in operation windows in JP1/IT Desktop Management 2.

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.

   To display the Home module in a multi-server configuration, select the **Status of management servers under the local server** tab.

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**.

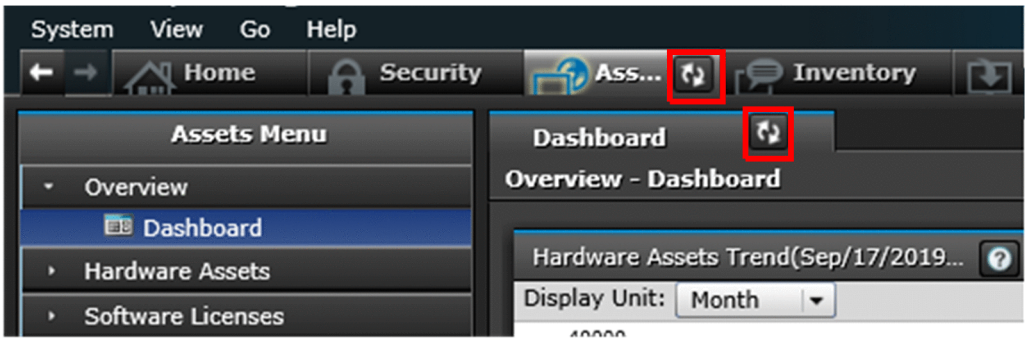
The panels that are displayed in the view and their layout change according to your settings.

> **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.

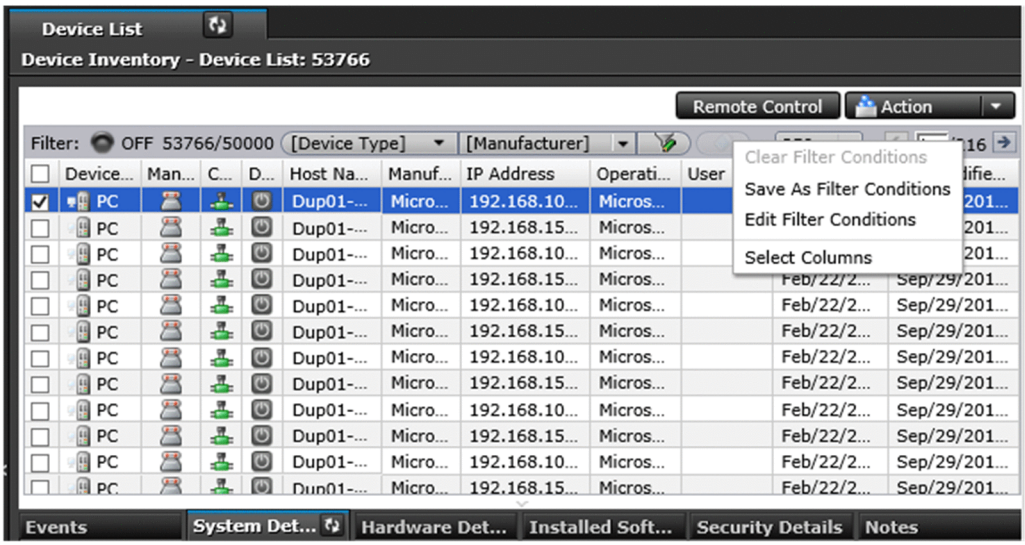
5.3 Changing items displayed in a list

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 **Assets**, select **Asset Field Definitions**, and then add the management item in the **Asset Field Definitions** view that appears.

Related Topics:

- 15.4.1 Adding asset management items

5.4 Common view operations

This section describes operations that are common to all views in JP1/IT Desktop Management 2.

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
- 5.6.1 Adding a custom group

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.

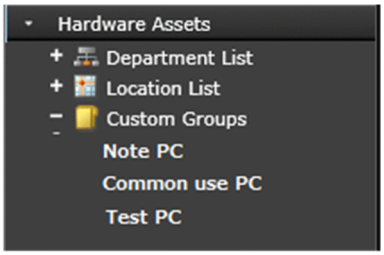
Related Topics:

- 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 Inventory 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

There are two types of filters: *simple filters* and *detailed filters*. This section describes how to save and delete filter conditions defined for detailed filters. For details about simple and detailed filters, see the description of Using filters in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

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 **OK**.
   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:

- 17.21 ioutils exportfilter (exporting filter settings)
- 17.22 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 Procedure for checking the status of the management relay servers under the local server

For a multi-server configuration, you can use the **Hierarchical Configuration Under the Local Server and Operation Status** panel to check whether the management relay servers under the local server are operating normally. If any problem is detected with one or more management relay servers, you need to check the status in the **Details of Management Relay Server** dialog box, and then take necessary action.

To check the status of management relay servers under the local server:

1. Display the Home module.
2. Select the **Status of management servers under the local server** tab.
3. From the **Hierarchical Configuration Under the Local Server and Operation Status** panel, right-click the icon of the management relay server whose details you want to check, and select **Display Details of the Management Relay Server**.

The **Details of Management Relay Server** dialog box is displayed. Check the summary of the management relay servers and system details, and then take necessary action.

5.9 Procedure for logging in to the operation window of a management relay server under the local server

For a multi-server configuration, you can log in from the operation window of the local server directly to the operation window of a management relay server under the local server. There are two types of log-in procedures. One is to log in after selecting a screen that you want to display, and the other is to log in to the same window as the one that is being displayed.

> **Tip**
>
> To log in from the operation window of the local server directly to a management relay server under the local server, you need to set in advance the same user account in both the local server and that management relay server. In addition, the administrator's computer that displays the operation window must be able to resolve the host names of the management relay servers under the local server.

To log in after selecting a window you want to display:

1. Display the Home module of the local server.
2. Click the **Status of management servers under the local server** tab.
3. Click the icon of the management relay server you want to log in to, and select the window you want to display from the menu.

A new window opens to allow you to log in to the operation window of the management relay server under the local server.

To log in to the same window as the one that is being displayed:

1. From **Operation-target server** on the top of the window, select the host name of the management relay server you want to log in to.

A new window opens to allow you to log in to the operation window of the management relay server under the local server.

5.10 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 2.
- 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.

  For Chrome

  1. From the Chrome menu, select **More tools**, and then **Advanced**.
  2. Click **Privacy and security**, **Site Settings**, and then **Cookies and site data**.
  3. In the **Allow** section, click **Add**.
  4. In the **Add a site** dialog box, within the **Site** box, enter the address of the management server, and then click **Add**.
  5. 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. Note that the timeout value cannot be changed.
- 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 2 is installed. The procedure for deleting the temporary Internet files in each web browser is explained below:

For Internet Explorer

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**.

For Chrome

1. From the Chrome menu, select **Settings**, and then **Clear browsing data**.
2. In the **Clear browsing data** view, select **Cached images and files**, and then click **Clear data**.

- 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**.

- In the **Send User Notification**, **Deny Network Access**, and **Edit Other Language Message** windows that users can enter text, the font information is converted to the number of characters, and is added to the actual number of characters that a user enters. The estimated number of characters of font information to be added is as follows:

  - 189 characters per line
  - 7 characters per part where bold, italic, or underline is used.
  - 92 characters per part where a font is changed in the middle of the line.
  - 38 characters and the number of characters of URL per part where a hyperlink is used.

- A horizontal scroll bar may appear in the legend for charts in the management window. So the contents of the legend may not be seen. To avoid this problem, change the width of the management window and then refresh the display.
- When the display of JP1/IT Desktop Management 2 dialog and message boxes is enabled, in an environment where tablet mode is enabled, dialog and message boxes are sometimes displayed on the desktop, which does not appear in tablet mode. As a result, the user might not notice when a dialog or message box is displayed. In particular, if the user selects **Turn off** from the operation menu, the user might shut down the system without noticing the dialog or message box. To prevent this, in the settings window, click **Agent settings** and then **User notification settings**. Then, in **Settings of computer shutdown and reboot**, enable **Follow the user response in a dialog box indicating shutdown or reboot**. Alternatively, when the display of JP1/IT Desktop Management 2 dialog and message boxes is enabled, consider disabling the tablet mode.

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 2.

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 2.

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 2.

How to manage devices managed by an external system through the API:

By linking an external system with JP1/IT Desktop Management 2 through the API, you can include devices managed by the external system as the management targets of JP1/IT Desktop Management 2.

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 create an agent installation set, in the Home module, click the **Getting Started** button. The **Getting Started** wizard starts when the button is clicked. You can use this wizard to create an agent installation set. To search for a device, use the **Discovery** view of the Settings module. In the **Discovery** view, you can set search conditions and perform a search.

Important

The creation of agent installation sets or the distribution of agents cannot be performed on computers whose operating systems are UNIX or Mac.

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 wizard, click the **Next** button.
3. Create the installation set you want to apply to each computer by following the instructions in the wizard.

   Configure the following items. Click the **Next** button when you set the item:

   Selecting agent settings

   From **Agent Configuration Name**, select the agent configuration you want to apply to the computer.

   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 **Windows Agent Configurations and Create Agent Installers**.

   When you select an agent configuration, you can change the folder in which the agent is installed.

   To change the installation folder, enter the new installation folder for an agent in **Installation Folder**.

   In addition, when you install agents on shared VDI-based virtual computers, you have to specify **Settings when generating the host ID**.

   Account settings

   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 when you install agents on computers running 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 specify an account that has Administrator privileges, users who do not have Administrator privileges can use the specified account to install agents. 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.

   Settings for the components to be installed

   Specify the type of components to be installed (select whether to install them as agents or relay systems), and whether to install remote control agents, which are subcomponents.

   Settings for the registration-destination ID

   Specify the ID (ID group used for receiving jobs from the managing server) to which the agent is to be registered.

   Settings for the file to be deployed

   Specify the file that is deployed when the agent is installed and the folder in which the file is to be deployed.

   Settings for the file to be automatically executed

   Specify the files that are automatically executed after the agent is installed, and the files and arguments necessary for the automatic execution.

> **Tip**
>
> To automatically install Hibun (Hibun DC or Hibun DE) or some other related product on an agent, first prepare (create) installation media containing the related product in a folder in `C:\DATA` on the administrator's computer. Compress the entire folder or all of the files in the folder to a ZIP file. Then, to automatically install the related product on an agent, specify this ZIP file as a file to be automatically executed after agent installation. For details about how to create installation media for Hibun, see the *JP1/HIBUN Installation and Setup (for Administrators)*.

Settings for an overwrite installation

Specify whether to perform an overwrite installation if the agent has already been installed.

4. Check the settings, and then click the **Create** button.
   The **Create Agent Installer** dialog box appears.
5. In the **Create Agent Installer** dialog box, click the **Save** button.
   The default file name of the saved installation set is `ITDM2Agt.exe`.
6. The **Completed** screen is displayed, click the **Close** button and exit the wizard.

The installation set is created, and then downloading of the installation set begins.

> **Tip**
>
> You can also create an installation set in the **Windows Agent Configurations and Create Agent Installers** view. To display this view, in the Settings module, select **Agent** and then **Windows Agent Configurations and Create Agent Installers**. 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 **Create** button. The installation set is created, and then downloading of the installation set begins.

> **Tip**
>
> You can create the file for connection destinations (`itdmhost.conf`) or the information file for higher connection destinations (`dmhost.txt`) and store it in the JP1/IT Desktop Management 2 - Manager data folder. When you create the installation data set, the file you created is incorporated into the installation data set. For details about the file for connection destinations (`itdmhost.conf`), see the description about automatically setting the connection destinations of agents in the *JP1/IT Desktop Management 2 Configuration Guide*. For details about the information file for higher connection destinations, see the description of automatic change of connection destinations for agents in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

> **Important**
>
> You cannot use an installation set to install an agent on UNIX computers or Mac OS computers.

Related Topics:

- 15.1.2 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. You can search for devices registered in Active Directory.

In the Settings module, select **General**, and then **Active Directory**. In the **Active Directory** view that appears, specify the domain information for the Active Directory you want to search. Then, in the Settings module, select **Discovery**, **Configuration**, and then **Active Directory**. In the **Active Directory** view that appears, specify the search condition and other necessary information. When you click the **Start Discovery** button, the search begins according to the specified schedule.

To search for devices registered in Active Directory:

1. In the Settings module, select **General**, and then **Active Directory** to display the **Active Directory** view.
2. Set the domain information of the Active Directory you want to access.
   To make sure that you can access the set Active Directory, click the **Test** button.

   Important

   In a multi-server configuration, do not specify the same Active Directory domain information for different management servers. If you do so, you might not be able to manage device information normally because the server that manages the information about a device might be changed unintentionally each time the device is detected.
3. In the Settings module, select **Discovery**, **Configuration**, and then **Active Directory** to display the **Active Directory** view.
4. In **Auto Discovery Schedule**, specify the search schedule.
5. In **Edit Discovery Option**, specify whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them.
6. To send a notification email to yourself (administrator) after completion of the search, specify the notification destination in **Notification of Discovery Completion**.
7. Click the **Start Discovery** button in the upper right corner of the window.

The display changes to the **Active Directory** view (which is displayed by selecting **Discovery**, **Discovery Log**, and then **Active Directory** in the Settings module), and then the search is performed according to the specified search schedule.

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. You can search for devices connected to the network.

In the Settings module, select **Discovery**, **Configuration**, and then **IP Address Range**. In the **IP Address Range** view that appears, set the range of IP addresses to be searched and the authentication information to be used during the search. When you click the **Start Discovery** button, the search begins according to the specified schedule.

To search for devices connected to the network:

1. In the Settings module, select **Discovery**, **Configuration**, and then **IP Address Range** to display the **IP Address Range** view.

2. In **Search Node Locations**, set the range of IP addresses to be searched.
   By default, **Management Server** is set as the IP address range. **Management Server** is a network segment that contains a management server.

   Important

   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.

   If you discover more than 50,000 IP addresses, disable the **Intensive Discovery** option.

   Important

   In a multi-server configuration, do not specify the same search range for different management servers. If you do so, you might not be able to manage device information normally because the server that manages the information about a device might be changed unintentionally each time the device is detected.

3. In **Credentials Used**, set the authentication information to be used during the search.

4. In **Search Node Locations**, set the authentication information to be used for each IP address range.

   Important

   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 might cause some users to be unexpectedly locked out of their accounts.

   Important

   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.

5. In **Auto Discovery Schedule**, specify the search schedule.

6. In **Edit Discovery Option**, specify whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them.

7. To send a notification email to yourself (administrator) after completion of the search, specify the notification destination in **Notification of Discovery Completion**.

8. Click the **Start Discovery** button in the upper right corner of the window.

9. In the dialog box that opens, confirm the search settings, and then click the **OK** button.

   If you select the **Intensive Discovery** check box, a network search is repeated without a break in the specified period of time. Therefore, we recommend that you select this check box if you want to discover as many devices as possible at the initial stage of operation. For example, if you repeat a search, devices that were turned off and could not be discovered during the first search are more likely to be discovered during the second and subsequent searches.

   Important

   With the **Intensive Discovery** check box selected, a search that is continuously repeated imposes a heavy load on the network during the specified period of time. Select this check box after due consideration of the load on the network.

The display changes to the **IP Address Range** view (that is displayed by selecting, **Discovery**, **Discovery Log**, and then **IP Address Range** in the Settings module), and then the search is performed according to the specified search schedule.

Tip

When performing Discovery from IP Address Range to network devices that are in a redundant configuration, a device may be registered as two devices. If you do not want to manage one of devices, set either device to Ignored Node.

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 Inventory 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**
>
> 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 Inventory 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

You cannot exclude a computer for which the 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):

> **Important**
>
> When a user computer is switched from offline management to online management, the security policy for online-managed computers or groups is automatically applied to the user computer.

1. In the **Basic settings** view for the agent configuration, select the **Communicate with the higher system** check box, 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 2 - Agent**, **Administrator Tool**, and then **Setup**.

   > **Tip**
   >
   > When setup starts, a dialog box might appear asking you to enter a password. This occurs when a password has been set to protect the agent configuration assigned to the agent. You can continue by entering the password set in the agent configuration.

3. In the **Setup (Agent)** dialog box, select the **Communicate with the higher system** check box, and then click **OK**.
4. In the displayed confirmation dialog box, click **Yes**.

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**
>
> 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**
>
> 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 list of agent configurations in **Windows Agent Configurations and Create Agent Installers** under **Agent** in the Settings module, click the **Edit** button for the agent configuration whose settings you want to change.
2. In the **Basic settings** area of the **Edit Agent Configuration** dialog box, clear the **Communicate with the higher system** check box, and then click **OK**.
3. In the **Confirming the Settings for Communications with Higher Systems** dialog box that appears, 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.

Tip

In a multi-server configuration, if device information is deleted from a server, the device information is also deleted from the higher management servers.

However, if deletion of device information from a higher management server fails for any reason, you need to delete the device information manually from that server to retain consistency. For details about the deletion procedure in such a case, see 6.20 Procedure for deleting (from the local server) a device managed by a management relay server under the local server.

Tip

You can use device maintenance to automatically detect and delete duplicate or idle devices and to discard the hardware asset information associated with devices to be deleted. For details, see 6.38 Procedure for configuring device maintenance settings and checking detection results and 11.1.16 Automatically changing the asset status of hardware assets associated with deleted devices.

Tip

When devices are deleted, the system configuration information corresponding to the deleted devices is also deleted automatically. Deletion of the system configuration information corresponding to the device deletion is applied to the agents managed by the local server. The relay systems are not deleted automatically.

For details, see the description about the relationship between device maintenance and system configuration information maintenance in the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

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

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 Inventory 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

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

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.

Important

The edited device information value is only applied to the higher management server. If you want to apply the change to the management relay servers under the server, you need to edit values in the management relay server under the server.

Important

If an invalid value is specified for the device information in the Edit Device Details dialog box, you may not be able to operate the device. For example, if a device's IP address is deleted, you cannot start Remote Control to the device, or cannot control network access for the device. To solve this problem, correct the device information by performing the Update Device Details menu from the Action menu.

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 **User notification settings**, you specified display of the End User Form view.

To acquire the latest device information:

1. Display the Inventory 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**.
   For agents for UNIX or Mac, the *Get system information from computer (UNIX)* and *Get software information from computer (UNIX)* jobs are executed. You can check the execution status of these jobs in the **Collect_Device_Inventory** folder of the **Job Status** window of the Remote Install Manager. These jobs are automatically deleted after the elapse of 14 days. In addition, by default, notifications of system information and software information are sent every 24 hours (once a day) from agents for Mac to the management server.
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**
>
> For details about the Wake on LAN function, see the description of the notes about how to set up Wake on LAN in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.
>
> In the following cases, the device might be automatically turned off after the device information is collected:
>
> - 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
>
> If the communication from Manager to the target computer fails, there is a case that the computer might not be automatically turned off after the device information is obtained. In this case, select **Power OFF** from the Action menu to turn off the computer.
>
> Note that agents for UNIX or Mac do not provide automatic power control (on and off).

Related Topics:

- 15.5.7 Setting AMT credentials
- 6.27 Controlling the computer power

6.12 Changing the association between device information and assets

In JP1/IT Desktop Management 2, devices and assets are associated by using BIOS serial numbers. As a result, when multiple devices have the same BIOS serial number, multiple devices are associated with the same asset. In such a case, you can register multiple devices as different assets by changing the condition for associating devices with assets from the BIOS serial number to the host name, UUID, or host ID of the computer.

To change the association between device information and assets:

1. Create a settings file.
   The following table shows the details of the settings file:

Item	Description
File name	jdnSetProductNumberPath
Storage location	*installation-folder-of-JP1/IT Desktop Management 2 - Manager*\mgr\temp (Default: C:\Program Files(x86)\Hitachi\jp1itdmm\mgr\temp)
Timing when the file is read	When the JP1/IT Desktop Management 2 service starts

   How to specify the settings file (to associate devices with assets by using host names)
   /SystemInventory/HostName

   How to specify the settings file (to associate devices with assets by using UUIDs)
   /SystemInventory/ComputerSystemProduct/UUID

   How to specify the settings file (to associate devices with assets by using host ID)
   NodeID

2. Restart the management server.

How to confirm:

For a registered device, execute **Update Device Details** to make sure that **Last Modified Date/Time** has been updated. Next, make sure that **Serial #** has been changed to the host name, UUID, or host ID in **Asset Information** in **Hardware Details** of the asset.

To reset the association between device information and assets:

1. Delete the settings file.
2. Restart the management server.

Important

- To associate devices with assets by using host names, the host names must be unique. If a host name is not unique, multiple devices might be associated with the same asset.
- When settings are changed, the association with a registered device is not automatically changed to another asset. Manually change the device associated with the asset in the management window, or delete the device and then register the device as a device to be managed again.
- The settings file is case sensitive. In addition, do not enter a linefeed character on the file. If an error exists in the settings file, device information cannot be associated.
- By changing the condition for associating devices with assets to host ID, if the host ID is changed due to cases such as re-installing the OS, the device will be registered as another asset.

6.13 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 Inventory 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 `ITDM2Offline.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:

- 6.14 Notification of the device information collected by using the information collection tool

6.14 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. In a multi-server configuration, an online-managed computer that is managed by the same server that manages the offline-managed computer notifies the device information of the offline-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

When out-of-date device information is notified, the current device information registered with JP1/IT Desktop Management 2 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

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 2 - 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 to protect information from external storage media** displayed by clicking **Password settings** 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.

   Important

   If you notify the management server of the device information that was collected by executing the Information Collection Tool from the 64-bit OS agent by executing **Notification of Collected Information**, do not place the storage folder (`\Data` folder) for the device information to be notified

in the path (example: `C:\Windows\system32`) where the file system redirector is run by OS. The storage folder cannot be specified in the **Specify storage location** dialog box.

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 tools fail.

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
```

Important

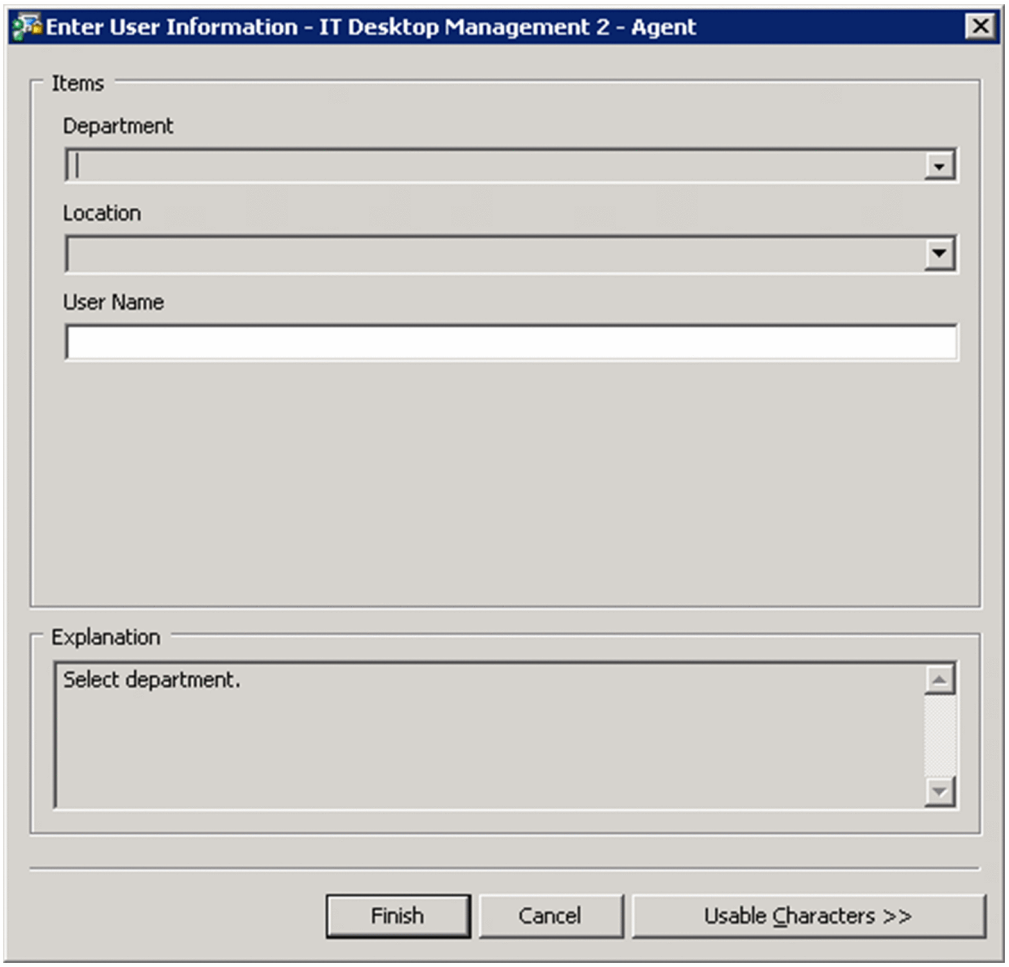
Do not notify the management server of the device information of a computer that is connected to the management server, by using the **Notification of Collected Information** menu. If you notify it, the device information may become inconsistent with the existing data. In this case, perform the **Update Device Details** menu in the Device List window to update the device information.

Related Topics:

- 6.13 Creating the information collection tool

6.15 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. With the Citrix XenApp and Microsoft RDS server, you cannot display a window for entering user information. Whether the End User Form view is displayed depends on the settings of **User notification 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 **Assets** 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 **Assets** 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:

- 15.4.1 Adding asset management items

6.16 Procedure for changing the display order of user information

You can change the order of items displayed in the **Enter User Information** window.

To change the display order of user information:

1. Display the Settings module.
2. In the menu area, select **Assets**, and then **Asset Field Definitions**.
3. In the information area, click the **Change** button for **Field order of Custom Fields on the user input window**.
4. In the **Change End User Form Order** dialog box, change the order of the items displayed in the **Enter User Information** window, and click OK.

The order of the items displayed in the **Enter User Information** window changes.

Tip

- You can open the **Change End User Form Order** dialog box also from the **Add Custom Fields** dialog box or the **Edit Custom Fields** dialog box.
- The default display order of items on **Change End User Form Order** dialog is based on order of item name in language set as default language on **Edit Other Language Settings** sorted with character code "UTF-8".

6.17 Setting the display interval for the End User Form view in the Inventory 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 Inventory module.
2. In the menu area, select a group from **Device Inventory**.
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:

- 6.15 Obtaining user information

6.18 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 **Assets** 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, in the **Asset Field Definitions** window, 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**.

   In the **Add Custom Fields** or **Edit Custom Fields** dialog box that appears, click **Data Source** and specify **Active Directory**.

   > **Important**
   >
   > You cannot specify **Active Directory** if the item you are adding or editing does not support Active Directory as a data source.
5. Specify the Active Directory management item from which information is obtained.

   Set the item name, description, data type, template, entity, and attribute to acquire from Active Directory, and then click **OK** button.

The information managed in Active Directory can now be obtained as an additional management item of each device.

6.19 Procedure for reporting device information to the higher management server

In a multi-server configuration, if a new higher management server is deployed or the connected management server is changed, you must manually report the device information managed by the local server to the higher management server. Through the reporting of device information, you can resynchronize the device information of the local server and the higher management server.

> **Important**
>
> To maintain the integrity of the device information being reported, do not update the device information until the reporting is complete. Device information is not collected until the reporting is complete. You can check whether the reporting is complete in the Events module.

To report device information to the higher management server:

1. Display the Inventory module.
2. In the menu area, select a group from **Device Inventory**.
3. In **Action**, select **Report all Device Details to the Higher Management Server**.
4. In the displayed dialog box. select the **Continue Operation** check box, and then click **OK**.

Reporting of device information to the higher management server starts.

> **Tip**
>
> After you click the **OK** button, about one or two hours is required for preparation before the actual report starts. During preparation, you can cancel the report for all device details. To cancel the reporting, in **Action**, select **Report all Device Details to the Higher Management Server**. In the displayed **Report all of the Device Details to the Higher Management Server** dialog box, select **Continue Operation**, and then click **OK**. In the displayed **Cancel the Reporting of Device Details to the Higher Management Server** dialog box, click **OK** again.
>
> Note that you cannot cancel the reporting after data transmission starts.

6.20 Procedure for deleting (from the local server) a device managed by a management relay server under the local server

In a multi-server configuration, if device information is deleted from a management relay server under the local server, the device information is also deleted from the local server. However, if automatic deletion of device information fails for any reason, you need to delete the device information manually from the local server to retain consistency.

To delete (from the local server) a device managed by a management relay server under the local server:

1. Display the Inventory module.
2. From **Device Inventory** in the menu area, select a group.
3. Select the device you want to delete.
4. From **Action**, select **Remove**.
5. In the displayed dialog box, click **OK**.

The device is deleted from the local server.

> **Tip**
>
> This procedure deletes the device from the local server only. To delete the device from the entire system, delete the device on the management relay server (under the local server) that manages the device.

Related Topics:

- 6.9 Removing a device

6.21 Exporting device information

Select **Device Inventory** in the Inventory module, then you can export (in a batch) the information displayed in the information area of the **Device Inventory** 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 Inventory module.
2. Select a group from **Device Inventory**, and display the device whose information you want to export in the information area.
3. From **Action**, select **Export Device List** or **Export Device Details**.
4. 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.
5. 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**.

Important

The exporting process may take a long time or fail to complete. This may occur when any of the following conditions are met:

- More than 1,000 devices are displayed on the window.
- The items other than the default items are selected for the export.
- The security assessment process or distribution process is being processed in the background.

If the export process is not completed, work around this problem by any of the following methods.

- Reduce the number of devices displayed on the screen to 1,000 or less by using a filter or a custom group.
- Narrow down the export items and select only necessary items.
- Perform the **Export Device Details** from the Action menu while the ITDM-compatible distribution as such is not being processed in the background.

6.22 Exporting software inventory

Select **Software Inventory** in the Inventory 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 Inventory module.
2. Select **Software Inventory** and then **Software List**, and display the software whose inventory whose information you want to export in the information area.
3. From **Action**, select **Export Software List**.
4. 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.
5. 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.

6.23 Removing software inventory

Select **Software Inventory** in the Inventory 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 Inventory 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.

6.24 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 Inventory 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

6.25 Uninstalling software from the computers in the Inventory module

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 Inventory 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 (ITDM-compatible) module.

> **Tip**
>
> You can also create and execute an uninstallation task from the Distribution (ITDM-compatible) 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

6.26 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 (agents for Windows).

In addition, this function is not supported on the Citrix XenApp and Microsoft RDS server.

Note

- If the setting of message language which is consistent with browser language exists, default language will be set to browser language.
- For message notification, the message will be displayed as follows depending on the language which is set to the message and the display language of OS:

  In case that the language corresponding to the display language of OS of the agent exists in the language which is set to the message

  Message will be displayed in corresponding language.

  In case that the language corresponding to the display language of OS of the agent does not exist in the language which is set to the message

  Message will be displayed in default language.

To send a notification to a user:

1. Display the Inventory module.
2. From **Device Inventory** 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.

6.27 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.

You cannot control power supply (ON, OFF, or restart) of agents for UNIX or Mac.

To control the computer power:

1. Display the Inventory module.
2. From **Device Inventory** 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.

6.28 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 2 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 2.

6.29 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 Inventory module.
2. From **Device Inventory** 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**
>
> 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 2. Therefore, locking of the smart device is complete at the time the MDM system receives the execution request from JP1/IT Desktop Management 2.

6.30 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 Inventory module.
2. From **Device Inventory** 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 2. 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 2.

6.31 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 Inventory module.
2. From **Device Inventory** 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.

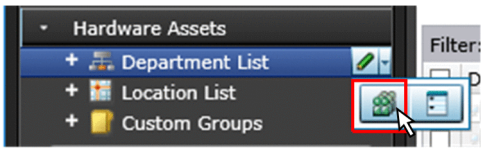
> **Tip**
>
> A smart device is reset by the MDM system according to a request issued by JP1/IT Desktop Management 2. Therefore, the reset of the smart device is complete at the time the MDM system receives the execution request from JP1/IT Desktop Management 2.

6.32 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 Inventory 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 **Assets** and then **Asset Field Definitions**. In the window that appears, click either **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

> **Important**
>
> If there is a large number of departments and locations, it might take time to edit them in the **Asset Field Definitions** window. Use the `ioassetsfieldutil import` command to set departments and locations.

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 Inventory module.

Related Topics:

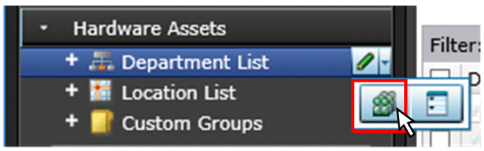
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location

6.33 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 Inventory 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 **Assets** and then **Asset Field Definitions**. In the window that appears, either click **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

> **Important**
>
> If there is a large number of departments and locations, it might take time to edit them in the **Asset Field Definitions** window. Use the `ioassetsfieldutil import` command to set departments and locations.

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 Inventory 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 Inventory 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 6.35 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:

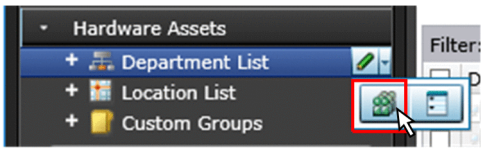
- 6.32 Adding the definition for a department or location
- 6.34 Removing the definition for a department or location

6.34 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 Inventory 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 Inventory 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 6.35 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location

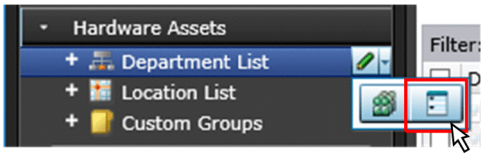
6.35 Removing only hierarchies that were used in the old organizational system

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 Inventory 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 Inventory 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 Inventory module is now consistent with the definitions.

6.36 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location
- 6.37 Deleting a department or location

6.37 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location
- 6.36 Changing the name of a department or location

6.38 Procedure for configuring device maintenance settings and checking detection results

You can configure device maintenance settings to define duplicate or idle devices as devices suggested for deletion. Devices that are detected as devices suggested for deletion can then be deleted automatically or manually.

To add definitions of devices suggested for deletion:

1. Display the Settings module.
2. In the menu area, select **Inventory** and then **Device Maintenance Settings and Detection Results**.
3. In the information area, click the **Add Detection Conditions for Duplicate Devices** button or the **Add Detection Conditions for Idle Devices** button.
4. In the dialog box that appears, specify the conditions for determining duplicate devices and idle devices.
5. Click the **OK** button.

The definitions of duplicate devices and idle devices are added and displayed in the **Detection Conditions for Device Maintenance** area of the **Device Maintenance Settings and Detection Results** view.

Tip

Based on the specified conditions for detecting duplicate or idle devices, detection is performed once a day. If devices that match the conditions exist, **List of Devices Suggested for Deletion** appears in the lower part of the **Device Maintenance Settings and Detection Results** view. Scheduled detection is performed according to the value specified for the `DeviceAutoMaintenanceTime` property in the configuration file (`jdn_manager_config.conf`). For details about the `DeviceAutoMaintenanceTime` property, see the description of how to use configuration files to change processing settings in the *JP1/IT Desktop Management 2 Configuration Guide*.

Devices not subject to device maintenance can be specified in advance. Alternatively, you can select devices in **List of Devices Suggested for Deletion** and change their settings so that they are no longer subject to device maintenance.

Tip

When a device is deleted, the system configuration information is deleted along with the device information. At this time, the device is also deleted from the host group and ID group.

In addition, you can specify settings so that the asset status of the hardware assets associated with deleted devices is automatically changed to the **Disposed** status or to another status. However, if you want the asset status of the hardware asset information associated with deleted devices to be automatically changed to the **Disposed** status or to another status, you will need to configure the appropriate settings. For details, see 11.1.16 Automatically changing the asset status of hardware assets associated with deleted devices.

Notes on using device maintenance to delete device information for the first time

Perform the following procedure:

1. Disable the automatic deletion of duplicate devices and idle devices to prevent device information from being automatically deleted by mistake.

   You can disable this feature by clearing the Automatic deletion setting check box in the following dialog boxes.

   - **Add Detection Conditions for Duplicate Devices**
   - **Edit Detection Conditions for Duplicate Devices**
   - **Add Detection Conditions for Idle Devices**
   - **Edit Detection Conditions for Idle Devices**

2. In the **Device Maintenance Settings and Detection Results** view that opens from **Inventory** of the Settings module, click the **Start Detection** button to manually start the detection of devices suggested for deletion. Then, decide whether to delete each device or exclude it from the maintenance targets.

> **Note**
>
> To allocate a software license to a device that was added when a device was replaced or an OS was re-installed, you can transfer a software license.

To specify or change the settings for suppressing device maintenance:

You can explicitly specify to exclude, from the targets of device management, devices that do not access a management server for a long time (for example, because the user of the device is on a long-term business trip or the device is in a cluster environment).

1. Go to the Settings module.
2. In the menu area, select **Inventory** and then **Device Maintenance Settings and Detection Results**.
3. In **Settings for Suppressing Device Maintenance** in the information area, click the **Change** button.
4. In the dialog box that appears, select a device, and then click the **Make Related** button or the **Exclude** button to specify whether to include the device in the targets for which device maintenance is suppressed.

If you include a device in the targets for which device maintenance is suppressed, the device will not be detected as a device suggested for deletion even if the device meets the defined detection conditions for duplicate devices or the defined detection conditions for idle devices. In addition, the device will not be deleted during the automatic deletion of devices suggested for deletion. If you exclude a device from the targets for which device maintenance is suppressed, the device will be detected as a device suggested for deletion if the device meets the defined detection conditions for duplicate devices or the defined detection conditions for idle devices.

To edit the definitions of devices suggested for deletion:

If you want to change the defined detection conditions for duplicate devices or the defined detection conditions for idle devices, edit the conditions. Note that you can edit the detection conditions for duplicate devices and the detection conditions for idle devices only on the local server. In a multi-server configuration, if you want to change the detection conditions for duplicate devices or the detection conditions for idle devices of a management relay server under the local server, edit the conditions by using the operation window on the applicable management relay server.

1. Go to the Settings module.
2. In the menu area, select **Inventory** and then **Device Maintenance Settings and Detection Results**.
3. In the information area, click the **Edit** button for the detection conditions you want to edit (detection conditions for duplicate devices or detection conditions for idle devices).

4. In the displayed dialog box, edit the detection conditions for duplicate devices or the detection conditions for idle devices, and then click the **OK** button.

The selected detection conditions (either the detection conditions for duplicate devices or the detection conditions for idle devices) are updated.

To remove definitions of devices suggested for deletion:

You can remove unused detection conditions for duplicate devices and unused detection conditions for idle devices. Note that you can remove the detection conditions for duplicate devices and the detection conditions for idle devices only on the local server. In a multi-server configuration, in you want to remove the detection conditions for duplicate devices or the detection conditions for idle devices of a management relay server under the local server, use the operation window on the applicable management relay server.

1. Go to the Settings module.
2. In the menu area, select **Inventory** and then **Device Maintenance Settings and Detection Results**.
3. In the information area, select the detection conditions that you want to remove (detection conditions for duplicate devices or detection conditions for idle devices), and then click the **Remove** button.

   You can select multiple detection conditions to remove detection conditions for duplicate devices and detection conditions for idle devices in a batch.
4. In the dialog box that appears, click the **OK** button.

The selected detection conditions (detection conditions for duplicate devices or detection conditions for idle devices) are removed.

Related Topics:

- 11.1.16 Automatically changing the asset status of hardware assets associated with deleted devices
- 11.2.13 Transferring software licenses

6.39 Tuning the settings for collecting device information

Device information is collected regularly from the devices listed below and stored in turn in the management server. You can adjust the amount of data to be collected to suit your operational practices and the specifications of the management server.

- Agent-controlled device
- Agentless managed device
- AD-controlled device
- MDM-linked managed device
- API-controlled device

You can see the performance logs from device information registration in *JP1/IT-Desktop-Management-2-Manager-installation-folder*`\log\JDNAGCQn.LOG`.

The value for `RegDelayQueue` indicates the number of collected pieces of data that have not been processed yet. Carry out operation for several days and check that the number of unprocessed items does not increase. If there is an increasing trend, consider increasing the following settings.

No.	Settings
1	Following settings in agent configuration • Monitoring Interval (Security) • Monitoring Interval (Others)
2	Following setting in agentless management configuration • Scheduled update interval
3	Following setting in MDM-linkage configuration • Unit and method for repetition in the collection schedule
4	Following setting in the security policy • Interval for notifications to higher systems for restrictions and operation logs

Related Topics:

- 15.1.2 Adding agent configurations
- 15.1.8 Regularly updating agentless device information
- 15.8.4 Specifying settings to link with an MDM system

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 2. 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 Inventory 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

If you are using Firefox or Chrome 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

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.
- 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.

Note that the remote control agent is not installed on an agent for UNIX or Mac.

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 2 - 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. Start the controller.
2. On the toolbar of the **Remote Control** window, click the **Options** button.
3. 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 that are used for agent setup.

For details about how to set up the agent, see 15.1.1 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 2. 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 2 - 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 and then select **Connect** from the pull-down menu.
3. In the **Agent Specification** dialog box that appears, select the computer to which you want to connect, and then click the **Connect** button.

   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.

Important

If you are unable to connect to the target computer, check for the following issues:

- The remote controller is not installed on the target computer.
- The credentials given for the target computer are wrong.
- The target computer is not running.

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 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 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. In the toolbar in the **Remote Controller** window, select the computer to which you want to connect from the list of past connection targets in the **Agent Specification** pull-down 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 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. From the **File** menu in the **Remote Controller** window, select **Search for connectible computers** and search for computers to which to connect.
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 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 2.

To connect to a computer:

1. Display the Inventory module.

2. In the **Device Inventory** view, select the computer you want to connect to.

> **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 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.

> **Tip**
>
> If the computer selected in the **Device Inventory** view is an agent for UNIX, clicking **Remote Control** will result in an error and remote control will not start. Note that the remote control function can be used on a computer running a Mac operating system only if the computer is connected by using RFB.

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.

> **Important**
>
> You cannot control power supply (ON and OFF) of agents for UNIX or Mac.

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 that an RFB-connected computer cannot be turned off from the controller. Use the Inventory module to turn off such a computer. For details, see 6.27 Controlling the computer power.

> **Important**
>
> You cannot control power supply (ON and OFF) of agents for UNIX or Mac.

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 that an RFB-connected computer cannot be rebooted from the controller. Use the Inventory module to reboot such a computer. For details, see 6.27 Controlling the computer power.

> **Important**
>
> You cannot restart agents for UNIX or Mac.

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 at the bottom of the **Remote Control** window.
2. On the keyboard input bar, click the button associated with the special key you want to send to the target computer.

Any special keys registered to the button you clicked are sent to the connected computer.

> **Tip**
>
> If the special key you want to send is not on the keyboard input bar, you can register the special key. For details, see 7.5.15 Registering a special key with the controller.

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.

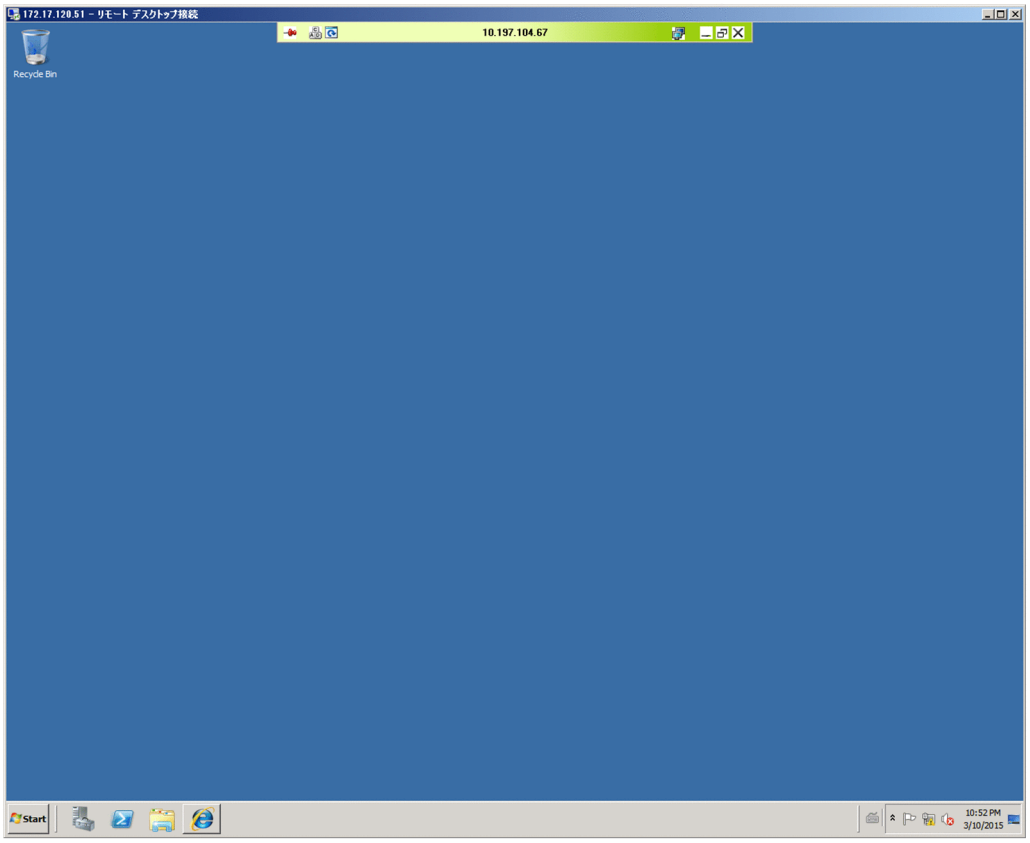
To remotely control a computer by using the fullscreen display:

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.

In a multi-server configuration, you can use the remote CD-ROM function only for the devices immediately under the local server and for the devices that can be connected via a network.

> **Important**
>
> 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:

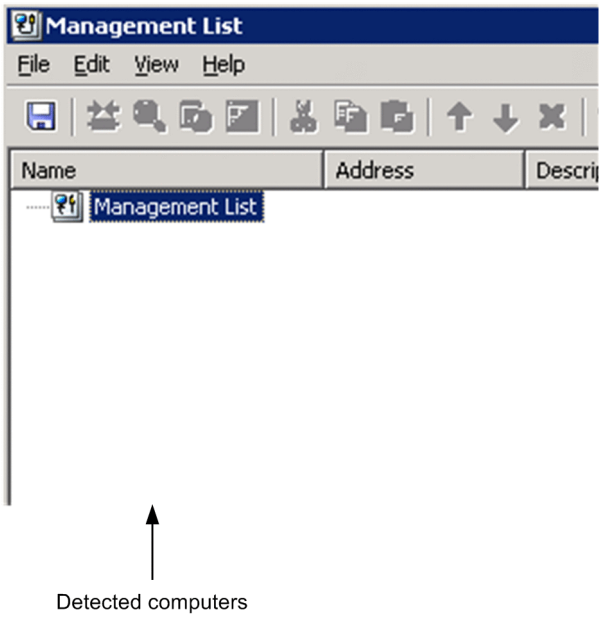
1. From the menu of the **Remote Controller** window, select **Connection List** and then **Change List**.
2. From the displayed connection list, select the location to create a **Network** icon.

> **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**
>
> When remote control is disconnected, the file transfer connection is automatically terminated.

> **Important**
>
> 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. Display the list of agent configurations in **Windows Agent Configurations and Create Agent Installers** in the **Settings** module, and then click the **Edit** button for the agent configuration whose file access permissions you want to set.
2. In the **Edit Agent Configuration** dialog box that appears, set **Access Permission to File** under **File Transfer** in the remote control settings.

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.

- To copy files or folders, drag and drop the files or folders.
- To move files or folders, drag and drop the files or folders while holding down the **Shift** key.
- If you drag the files or folders with the right mouse button, a menu appears when you drop them. 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. Display the **Connection List** dialog box by selecting **Connection list** and then **Edit Connection list**.
2. Select the computer for which you want to set up a connection environment.
3. On the toolbar, click the **Properties** button () of the **Connection List** dialog box.
4. On the **Settings** tab of the **Properties** dialog box, select **Set up the connection options**.
5. 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

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

You can record the on-screen activity of a computer you are remotely controlling, and save it as a video file. You can also play back these video files in the controller. For details, see the description of Recording and playback of remote control sessions in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

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.

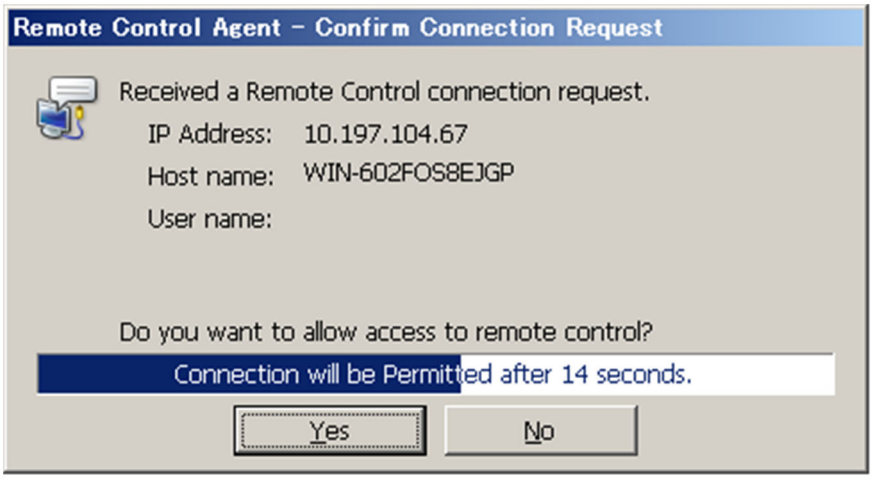
The remote control agent is stopped.

> **Important**
>
> 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 the **Display user-response dialog boxes on user computers** check box in the **Remote control settings** view 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 the controller is in control mode, the keyboard and mouse on a connected computer cannot be used. If you need to use the keyboard or mouse on the computer, you can forcibly release control mode, and change it to standard mode.

To forcibly release control mode:

1. On the connected computer, simultaneously press the **Ctrl**, **Alt**, and **Delete** keys.

The computer is now in standard mode, and you can operate it.

Note that when the connection mode of the connected 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

The Requester wizard can only be used on online-managed computers.

Important

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 2 - 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

If you want to establish contact with a user while engaged in a remote control session, you can use the chat feature to communicate with users who cannot be reached by telephone. Because the chat feature uses text data, it is also a useful way to provide IP addresses, URLs, and other text-based information in real time. For details, see the description of Using the chat feature in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

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 2 - 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 2 - 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 2 - 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 2 - 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 2 - 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 2 - 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 Inventory 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 for the group in the menu area.

Important

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

A component (a network monitor agent) must be registered on the management server to enable the network monitor.

Important

You cannot enable the network monitor if the computer is an agent for UNIX or Mac.

Important

In a multi-server configuration, you can enable the network monitor only for the computers immediately under the local server.

Important

If you enable or disable Network Monitor for the same device repeatedly within a short period of time, enabling Network Monitor might fail. If this happens, wait for a while and try to enable Network Monitor again.

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 2 - 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 Inventory 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

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

A component (a network monitor agent) must be registered on the management server to disable the network monitor.

Important

In a multi-server configuration, you can disable the network monitor only for the computers immediately under the local server.

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 2 - 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. In a multi-server configuration, you can allow network connections only for the computers immediately under the local server.

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 Inventory 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.

Important

When you change the network connection setting to Permit against a device that was disconnected by the Network Monitor function, it may take around ten minutes until the device can be connected to the network.

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

If there are two or more networks whose IP address ranges have an inclusion relation in **Device List (Network)**, a network to which devices belong cannot be identified. Accordingly, the devices may not access the server as specified in Server Configuration Settings. In this case, please check the subnet mask of the devices. When two or more networks whose IP address ranges have an inclusion relation are unintentionally created in **Device List (Network)**, remove either network which is unnecessary from **Device List (Network)** and then re-apply the server settings in the Server Configuration Settings panel.

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. In a multi-server configuration, you can block network connections only for the computers immediately under the local server.

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 Inventory 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. Note that you cannot send messages to agents for UNIX or Mac.

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

If a network connection is manually blocked, the network connection is automatically disallowed.

Important

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 network connection period, the icon  is displayed to indicate that devices are 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.

Tip

Events that are issued when the block target devices access the network trigger a network search to locate the devices accessing the network. You can enable the issuance of events by selecting the **Only detect nodes and do not block network access.** check box in the dialog box displayed in step 4.

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 Access Control** and then **Network Access Control Settings**.
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 Access Control** and then **Network Access Control Settings**.
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.

> **Important**
>
> You cannot enable network monitors on agents for UNIX or Mac.

> **Important**
>
> In a multi-server configuration, you can assign network monitor settings only to the computers immediately under the local server.

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, select the device that you want to edit and then click the **Edit** button for the device that you want to edit.

   You can select multiple devices to be edited.
4. In the **Edit Network Connection Permission or Denial** dialog box that appears, edit the necessary information, and then click **OK**.

   The information you can set includes the form of judgment and whether to permit connection to the network. You cannot edit MAC addresses.

   If you selected multiple devices, you can edit items by selecting the associated check box in the **Edit Network Connection Permission or Denial** dialog box. In this case, you cannot edit host names, MAC addresses, or IP addresses.

The network control settings of the selected device are updated.

For details about the network control, see the description of controlling network access of devices in the manual *JP1/IT Desktop Management 2 Administration Guide*.

8.7.3 Removing devices from the network control list

You can remove devices that were added manually from the network control list, in the **Network Filter Settings** window of the Settings module.

> **Important**
>
> What you can remove from the **Network Filter Settings** window are only the devices that were added to the network control list by any of the following procedure.
>
> - Devices manually added to the network control list
> - Manually added hardware asset information including MAC address or IP address
> - Imported hardware asset information including MAC address or IP address
>
> To remove devices that have been automatically added to the network control list as a result of a detection by a network monitor or a network search, delete the relevant device information in the Inventory module. In a multi-server configuration, you can also remove automatically added devices from the **Network Filter Settings** window under a specific condition. The condition is that only the devices immediately under the local server are specified as the target for automatic update of the network control list, and the devices are managed by management relay servers under the local server.
>
> To determine whether a device was added automatically, check whether information is displayed in **Host name** of the network control list.

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.

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 Procedure for importing network connection information

You can update network connection information collectively by importing a CSV file that was exported from another management server or was edited with spreadsheet software or a text editor.

Use the **Import the Network Connection Information** wizard to import network connection information.

To import network connection information:

1. Display the Settings module.
2. In the menu area, select **Network Access Control**, and then **Network Filter Settings**.
3. In **Action**, select **Import Network Connection Information** to start the wizard.
4. Check the flow of import on the **What is this Wizard?** window, and then click **Next**.
5. In the **Upload CSV file** window, specify the CSV file to be imported, specify **Import Starting Line** for the CSV file, and then click **Next**.
6. In the **Confirm Settings** window, check the result of importing the CSV file.
   If part of the data was not read, **Check Result Details** is displayed. We recommend that you check the information displayed in **Check Result Details**, correct the CSV file, and then re-import the file by clicking **Upload and Pre-Check CSV File**. Note that you can output the display content by clicking **Export**.
7. Click **Import**.

Control moves to the **Import Completed** window and the system starts to import network connection information.

8.7.5 Procedure for exporting network connection information

You can export network connection information, which can then be imported to another management server or edited.

To export network connection information:

1. Display the Settings module.
2. In the menu area, select **Network Access Control**, and then **Network Filter Settings**.
3. In **Action**, select **Export Network Connection Information**.
4. In the displayed dialog box, click **OK**.
5. In the displayed window, specify the file name, and then click **Save**.

The CSV file is saved with the specified file name.

8.7.6 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**.

   If you use the primary management server to manage the network connections in the entire multi-server configuration, perform steps 6 to 8 on only the primary management server.

6. In the information area, click the **Edit** button for **Range of targets subject to automatic updates of the Network Filter List**.

7. In the displayed dialog box, specify the range of targets subject to automatic updates.

8. Click **OK**.

The automatic update of the network filter list are changed.

8.7.7 Using a command to update the network control list

A network control list on a management server can be updated by executing the network control command.

To update a network control list by using the network control command:

1. Edit the network control command configuration file.

2. Execute the network control command (jdnrnetctrl command).

The network control list on the management server that is specified in the network control command configuration file is updated.

Related Topics:

- 1.6.5 Controlling network access of devices by using a command
- 17.40 jdnrnetctrl (controlling network access)

8.7.8 Notes on using the network control list

- The number of items (rows) in the network control list is up to 262,140. If the items are likely to exceed the limit, delete unnecessary rows.
- In **Settings** - **Network Access Control** - **Network Filter Settings**, items in the Simple Filter may be displayed or may not be displayed. In this case, widen the width of the management window or information area.
- If the device information has not been obtained from a computer, no values are displayed for the computer's asset information, such as department and location, in the network control list.

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 Access Control** and then **Network Access Control Settings**.
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 Access Control** and then **Network Access Control Settings**.
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 Access Control** and then **Network Access Control Settings**.
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 2 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.

8.10 Enabling the NX NetMonitor/Manager linkage settings

When you link with NX NetMonitor/Manager, replace "JP1/NETM/NM - Manager" described in this manual with "NX NetMonitor/Manager".

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 2 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.

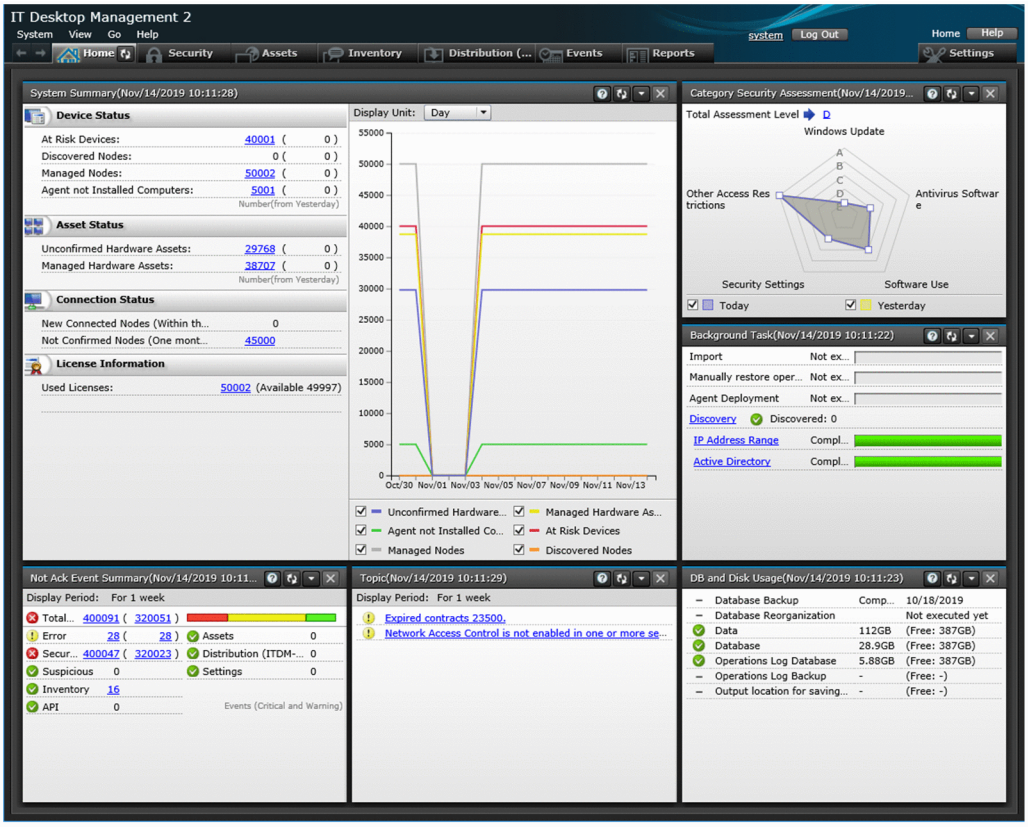
> **Important**
>
> In the case of agents for UNIX, security statuses are not determined based on security policies. Therefore, perform security management independently according to the security policy of your organization.

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.

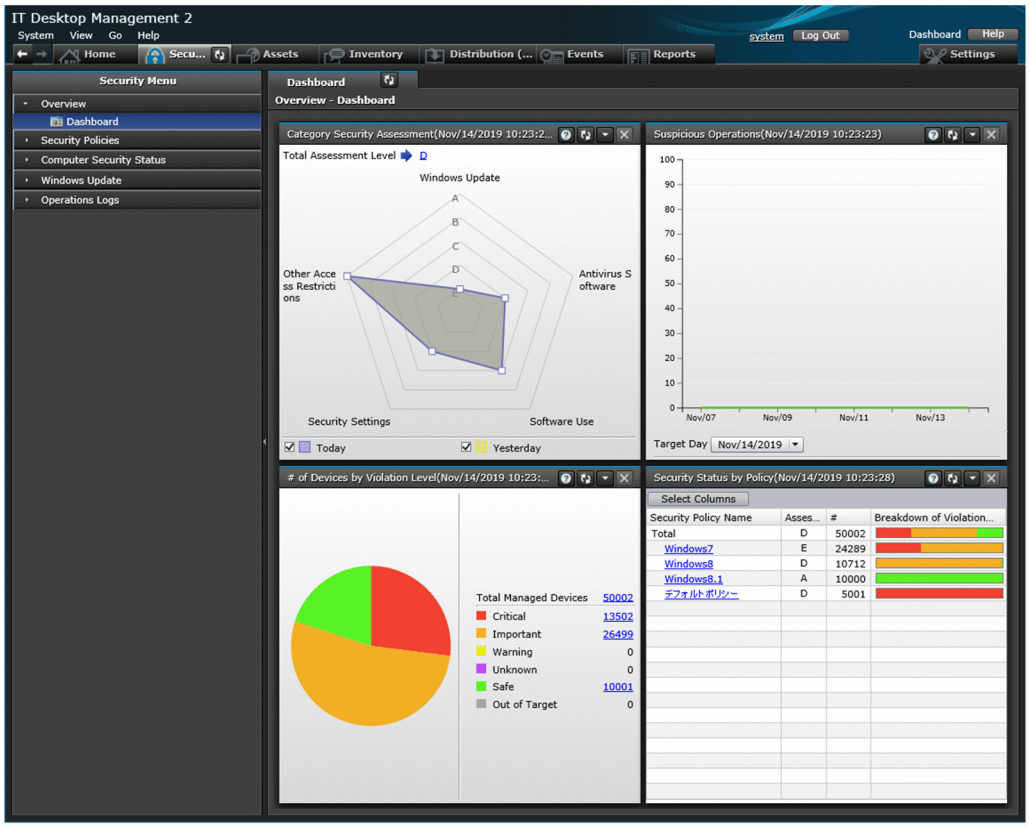


Checking the security status in the Security module

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.

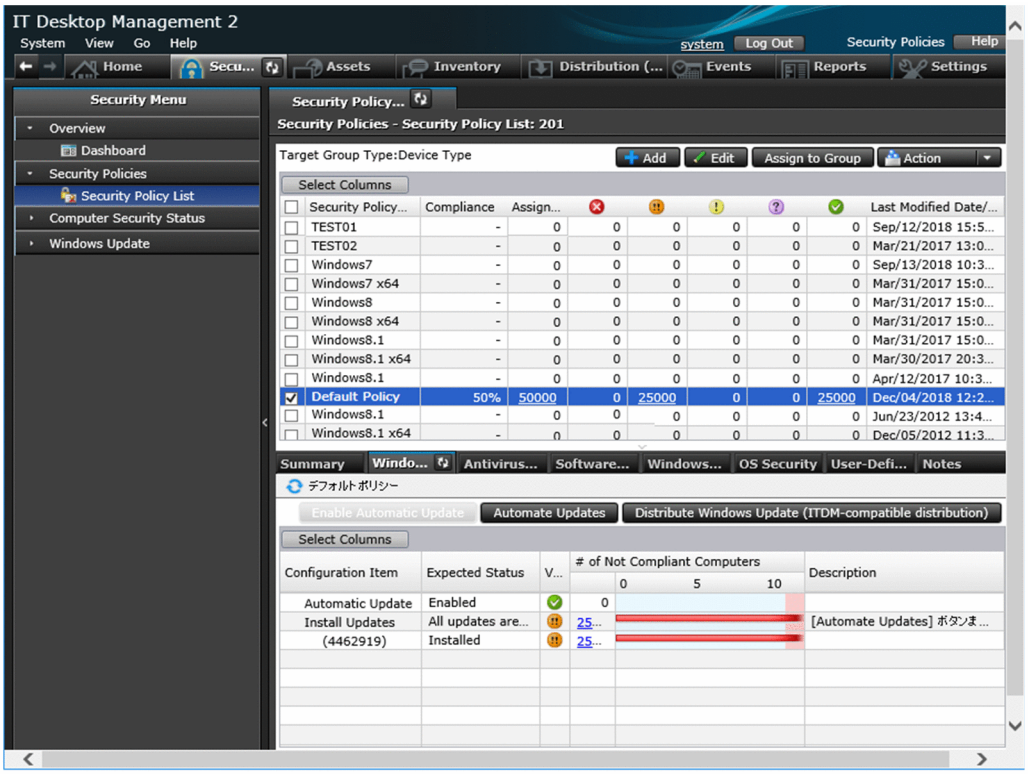
The security policies might not be adhered to if 0 is not displayed for (danger), (warning), and (caution).

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**

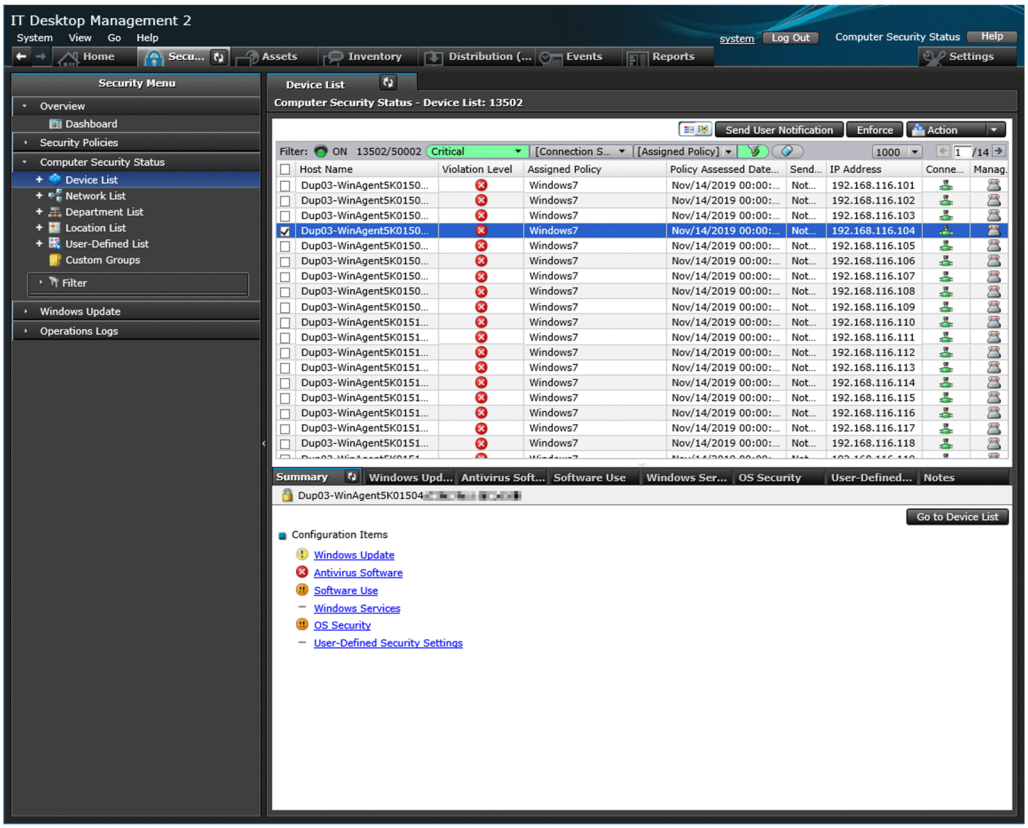


Checking status in the **Computer Security Status** view

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.

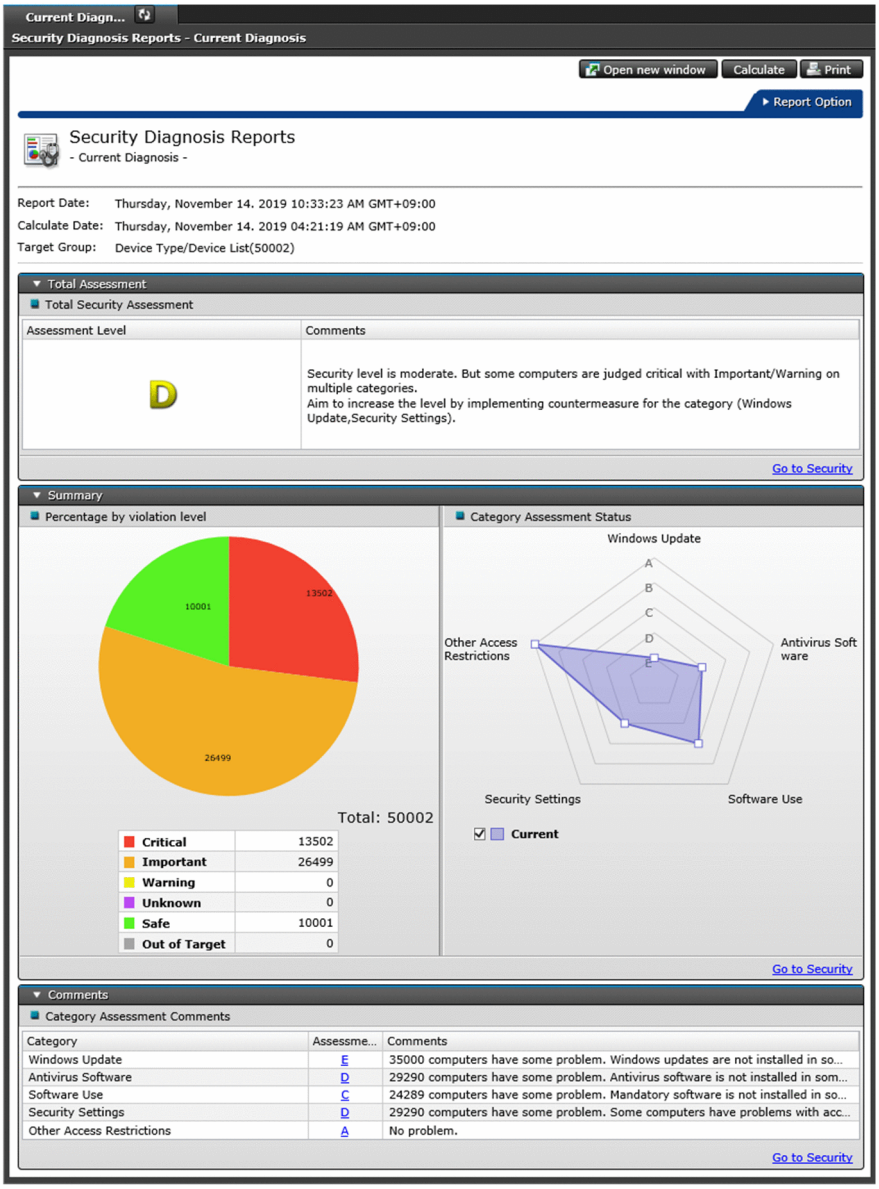
The security policies might not be adhered to if the violation level is displayed as (danger), (warning), or (caution). Review the security status for each security item, and then address any security issues.



Checking the status in a report

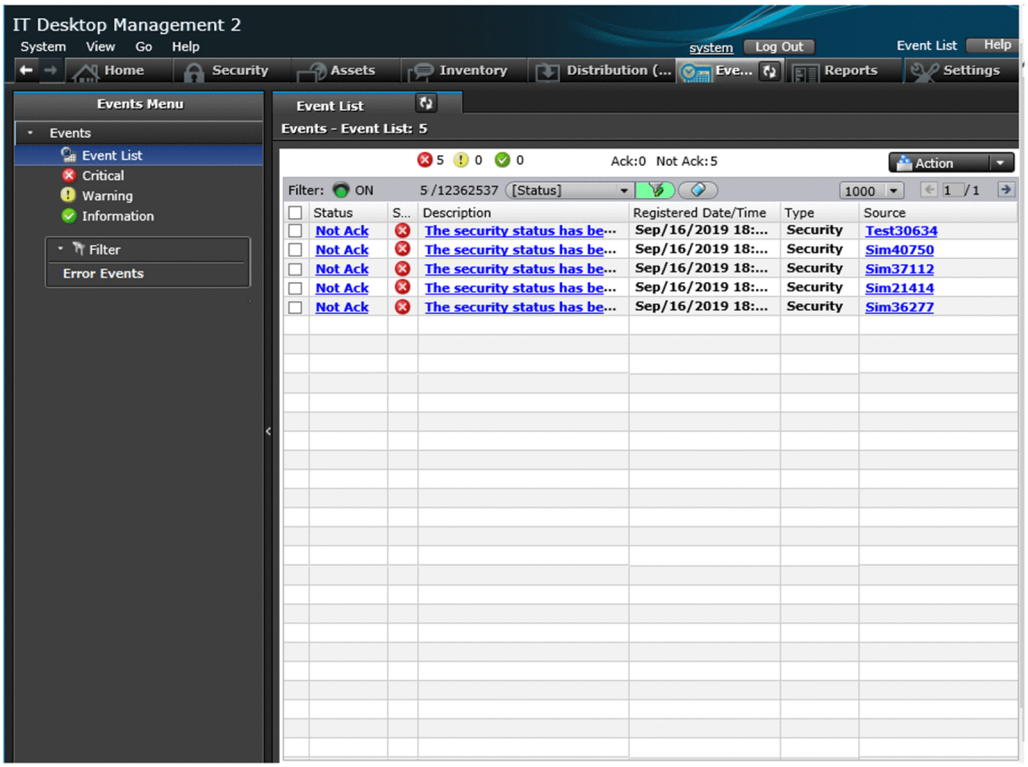
You can check the security status in **Summary Reports**, **Security Diagnosis Reports**, and **Security Detail Reports**.

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.


IT Desktop Management 2
System View Go Help
system Log Out
Event List Help
Home Security Assets Inventory Distribution (... Eve... Reports Settings
Events Menu
Events
Event List
Critical
Warning
Information
Filter
Error Events
Event List
Events - Event List: 5
5 0 0
Ack:0 Not Ack:5
Action
Filter: ON
5 /12362537 [Status]
1000
1 /1
Status S... Description Registered Date/Time Type Source
Not Ack The security status has be... Sep/16/2019 18:... Security Test30634
Not Ack The security status has be... Sep/16/2019 18:... Security Sim40750
Not Ack The security status has be... Sep/16/2019 18:... Security Sim37112
Not Ack The security status has be... Sep/16/2019 18:... Security Sim21414
Not Ack The security status has be... Sep/16/2019 18:... Security Sim36277

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.
   JP1/IT Desktop Management 2-installation-fodler\mgr\conf

The security status of the user accounts specified in the setting file will not be evaluated as a target.

Related Topics:

- A.3 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 Inventory 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.

9.3.9 Applying a security policy to an offline-managed computer

You can apply a security policy to an offline-managed computer. In the **Security Policies** view of the Security module, create and manage a security policy for offline-managed computers.

> **Important**
>
> It is possible to create multiple security policies for offline-managed computers, but it is recommended to have one for a system to prevent accidental application of the security policy.

(1) Preparing for the application of a security policy

To prepare for applying a security policy to an offline-managed computer:

1. Create a security policy.
2. Assign the security policy to a group.
3. Create a tool for applying policy offline.
4. Add agent configurations for offline computers.
5. Create an installation set.

The following describes the detailed procedure of the preparation for applying the security policy.

Creating a security policy:

Create a security policy for the offline-managed computer. For details about how to add a security policy, see *9.3.1 Adding security policies*.

> **Important**
>
> - In **Other Access Restrictions** of Security Configuration Items, enable USB devices.
>
> Note that for **Limit the assets that can be used**, accept the default (and do not select it). If it is selected, all USB devices are prohibited to use.
> - In **Operations Logs** and **Common settings for prohibited operations and operation logs** of Security Configuration Items, accept the defaults and do not change them.

Assigning the security policy to a group:

When you create a group for offline-managed computers, assign the security policy to the group. For details about how to assign the security policy to the group, see *9.3.5 Assigning security policies*.

> **Note**
>
> If you do not create a group for offline-managed computers, you can skip this step.

Tip

If you create a group for offline-managed computers and assign a security policy to the group, perform the following in advance:

1. Add an item to "obtain any registry information" to the hardware asset information.
   For details about how to add an asset field, see *15.4.1 Adding asset management items*. The following table shows an example of configuring the item name and the data source of information:

Field Name		Offline identifier information
Data Source		**Registry**
Type		**Text**
Registry Path	**Root Key**	HKEY_LOCAL_MACHINE
	Path	SOFTWARE\Hitachi\JP1/IT Desktop Management - Agent
	Registry Name	OfflineInfo

2. Create a user-defined group.
   For details about how to add a user-defined group, see *5.5.1 Adding a user-defined group*. The following table shows an example of configuring the user-defined group and user-defined group conditions:

User-defined group name		OfflinePC group
User-Defined Group Conditions	**Target Item**	Offline identifier information
	Judgment Condition	**Equals the judgment value**
	Judgment Value	OfflinePC

Creating a tool for applying policy offline:

To create the tool:

1. Open the Security module.
2. In the menu area, select **Security Policies** and then **Security Policy List**.
3. Select the security policy you created in *Creating a security policy*, and from **Action**, select **Create Tool for Applying Policy Offline**.
4. Check the displayed dialog box, and then click the **Save** button to save the tool for applying policy offline in any location.

Adding agent configurations for offline computers:

For details about how to add an agent configuration, see *15.1.2 Adding agent configurations*.

Important

In the **Basic Settings** view for the agent configuration, under **Timing of communication with the higher system**, clear the **Communicate with the higher system** check box.

Creating an installation set:

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

In Files to Be Automatically Executed Settings in the **Create Agent Installer** view, register the tool for applying policy offline (ZIP file) you saved in *Creating a tool for applying policy offline*. In the **Add Information about the File Required for Automatic Execution** dialog box, configure the following settings and click the **OK** button:

- **Expansion Category**: **Expand this Archived File, and Execute it Automatically after Installing the Agent**
- **Type of File to Be Executed**: **non-HIBUN Installer**
- **Path of File to Be Executed**: Click **Select File to Be Executed Automatically in the Expanded Folder** and select `setsecpolicy.vbs`.
- **Parameter**: Specify the options for `setsecpolicy.vbs` (security policy application command).

  For details about the security policy application command, see *17.41 setsecpolicy.vbs (applying a security policy to the offline-managed computer and collecting device information)*.
- Select the **Specify the expansion folder for the files** check box.
- **Expand Folder**: Specify the path to the folder that stores collected inventory files.

> **Tip**
>
> When you create a group for offline-managed computers and assign a security policy to it, you need to create a registry before executing a tool for applying policy offline. When you create a registry by using a batch file, perform the following:
>
> 1. Create a batch file to make a registry entry. An example of the command is as follows:
>
>    ```
>    reg add "HKLM\SOFTWARE\Hitachi\JP1/IT Desktop Management -
>    Agent" /v OfflineInfo /t REG_SZ /d OfflinePC
>    ```
> 2. In the **Set Files to Be Automatically Executed** view, click the **Add** button to show the **Add Information about the File Required for Automatic Execution** dialog box. Click the **Browse** button , select the batch file you created in step 1, and select the **Execute this file after installing the agent** check box.

After the file described above is registered, click the **Create** button to save the installation set. Store the saved installation set in an external storage medium.

(2) Applying a security policy to an offline-managed computer

To apply a security policy to an offline-managed computer:

1. Execute the installation set.

   On the offline-managed computer, execute the installation set (ZIP file). When you click the **OK** button in the execution confirmation window, the security policy is applied and inventories are collected.

   > **Tip**
   >
   > If you specify `/silent` in the Arguments when creating the installation set, the execution confirmation window is not displayed.

2. Send the inventory information to the administrator.

The `Data` folder has been created in the folder where `setsecpolicy.vbs` is stored. Store the `Data` folder in an external storage medium and send the medium to the administrator.

(3) Checking the inventory information collected from an offline-managed computer

To check the inventory information collected from an offline-managed computer:

1. Report the collected inventory information to the management server.
2. Check the offline-managed computer in the management console.
3. Change the name of the assigned policy.

The following describes the detailed procedure for checking the inventory information collected from the offline-managed computer.

Reporting the collected inventory information to the management server:

For details about how to report the collected inventory information, see *6.14 Notification of the device information collected by using the information collection tool*.

Checking the offline-managed computer in the management console:

Go to **Device Inventory (Device List)** in the Inventory module and check that offline PCs are registered.

> **Important**
>
> You can check that the security policy has been applied by viewing the registration in **Device Inventory (Device List)** because a command is used to apply the security policy and collect the inventory information at one time.

Changing the name of the assigned policy:

If a security policy is applied to a computer without creating a group, follow the procedure described below to manually change the name of the assigned policy:

1. Under **Computer Security Status** of the menu area in the **Security module**, select all offline-managed computers in **Device Inventory (Device List)**.
2. From **Action**, select **Assign Policy**, and in the displayed dialog box, from **Select Policy**, select the security policy for offline-managed computers and then click the **OK** button. **Assigned Policy** is changed.

> **Important**
>
> If you change the name of the policy assigned to an offline-managed computer, make sure that you apply a filter with the conditions described below to show the list of offline-managed computers only before changing the name.
>
> Filter conditions
>
> **- Assigned Policy - is - Default Policy**
>
> **- Management Status - contains any of - Offline management**

(4) Reapplying a security policy to an offline-managed computer

If a security principle is modified, you need to reapply the security policy. To reapply the security policy:

1. Re-create the tool for applying the security policy.

   If you modify the security policy, or if you register an additional USB device for use on the offline PC, re-create the tool for applying the security policy. For details about the procedure, see *Creating a tool for applying policy offline:* in *(1) Preparing for the application of a security policy*.

2. Unzip the re-created tool for applying policy offline (ZIP file) and then store it in an external storage medium.

3. Connect the external storage medium to the offline-managed computer, and apply the security policy.

   When you execute the stored `setsecpolicy.vbs` (security policy application command) and click the **OK** button in the execution confirmation window, the security policy is applied and inventories are collected.

   For details about the security policy application command, see *17.41 setsecpolicy.vbs (applying a security policy to the offline-managed computer and collecting device information)*.

4. Send the inventory information to the administrator.

   The `Data` folder has been created in the folder where `setsecpolicy.vbs` is stored. Store the `Data` folder in an external storage medium and send the medium to the administrator.

> **Tip**
>
> If a setting of the offline-managed computer is modified, you need to re-create and re-execute the installation set or the tool for applying the security policy depending on the modified setting. For details about which setting requires re-execution if modified, see *A.11 Conditions where the tools must be re-executed on an offline-managed computer*.

9.3.10 Notes on using a security poricy

- If you define two or more judgment conditions with the same user defined item names when specifying a user defined security settings for a security policy, the number of computers whose security settings are inappropriate (which is displayed in the **Security** - **Security Policy list** window - **User Defined Security Settings** tab) might not match the actual number of computers whose security settings are inappropriate. We recommend that you specify judgment conditions with a unique user defined item name in a user-defined security settings.
- If you specify two or more judgment conditions with the same software name and version to configure Target Software in the Mandatory Software settings of a security policy, the number of **# of Not Compliant Computers** (which is displayed in **Security Policies** - **Security Policy List** - the **Software Use** tab) might not match the actual number of computers that are not compliant with the security policy. We recommend that you do not specify judgment conditions with the same software name and version in the Mandatory Software settings.
- If you specify two or more judgment conditions with the same software name and version to configure Target Software in the Unauthorized Software settings of a security policy, the number of **# of Not Compliant Computers** (which is displayed in **Security Policies** - **Security Policy List** - the **Software Use** tab) might not match the actual number of computers that are not compliant with the security policy. We recommend that you do not specify judgment conditions with the same software name and version in the Unauthorized Software settings.
- The compliance rate and the number of assigned computers displayed in the Security Policy List are calculated from the number of devices for which security judgment was executed. Therefore, the compliance rate shows the ratio of devices which do not violate a security policy among devices for which a security judgment was executed with the security policy. In addition, the number of assigned computers shows the number of devices for which a security

judgment was executed with the security policy. Even if the security policy is assigned to devices, the devices in which a security judgment was not executed are not targeted for calculation of the compliance rate and the number of assigned computers. Also, devices are not targeted for calculation in the following cases because a security judgment is not executed:

  - A security policy in which only **Other Access Restrictions** and/or **Operation Logs** are enabled is assigned to devices.
  - All judgment items become "Out of target".

- When you specify software which is not shown in Windows **Add or Remove Programs** or **Unauthorized Software** in a security policy, the uninstallation task for the software can be created, however the task cannot be executed. If you wish to uninstall software which is not shown in Windows **Add or Remove Programs**, create an uninstallation task in the **Distribution (ITDM-compatible)** view and execute the task.

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 Inventory module. For details, see 6.26 Sending a notification to a user.

> **Note**
>
> - If the setting of message language which is consistent with browser language exists, default language will be set to browser language.
> - For message notification, the message will be displayed as follows depending on the language which is set to the message and the display language of OS:
>
>   In case that the language corresponding to the display language of OS of the agent exists in the language which is set to the message
>
>   Message will be displayed in corresponding language.
>
>   In case that the language corresponding to the display language of OS of the agent does not exist in the language which is set to the message
>
>   Message will be displayed in default language.

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 devices

You can specify policies regarding prohibited operations to suppress writing to or reading from devices.

To suppress the use of devices:

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.
   If the view is disabled, the suppression of device usage is disabled. To enable it, click the **Enabled** button in the top-left corner.
5. In **Suppression of Device Usage**, specify the devices which you want to suppress the use of.
6. If necessary, select devices to be displayed as suppressed on users' computers in **List of devices to be displayed in the suppression message**.
   The message can be displayed only for devices whose usage is suppressed.
7. To suppress only writing to some devices, specify those devices in **List of devices for which the write operation is suppressed**.
   The devices must be permitted for use before you can suppress writing to them. Devices to which you can suppress only writing depends on the OS of the computer. For details about the devices that can be suppressed for each OS, see the *JP1/IT Desktop Management 2 Overview and System Design Guide*.
8. Click **OK**.

The use of devices is suppressed according to the specified policy regarding prohibited operations.

If you select **Permits the use of registered USB devices** when setting the suppression of USB devices, the USB devices for which hardware asset information is registered will not be suppressed. In addition,You can also select **Limit the assets that can be used** to limit assets that can use the USB device, depending on the condition of the department, location, or associated asset.

Tip

If you assign a security policy with writing suppressed in **List of devices for which the write operation is suppressed**, a message that prompts a user to restart their computer appears. The security policy settings take effect when the user's computer is restarted in response to the message.

Tip

If you suppress the use of an internal CD or DVD drive or internal floppy disk drive, an event occurs on a computer that contains such devices. Therefore, security assessment of a prohibited operation might be temporarily degraded irrespective of user operation.

Tip

After blocking connection of a USB device with the function for prohibiting operation, allow the USB device to be connected, the OS might not recognize the USB device. In this case, enable the USB device with the following procedure:

1. Open the Windows device manager on the PC where the phenomenon that a USB device is not recognized occurs.
2. Expand **Disk drives** of the device manager.
3. Connect the USB device to the PC.
4. Confirm that the disk drive added under **Disk drives** of the device manager is disabled, when it is disabled, right-click the disk drive and then select **Enable** from the menu.

Related Topics:

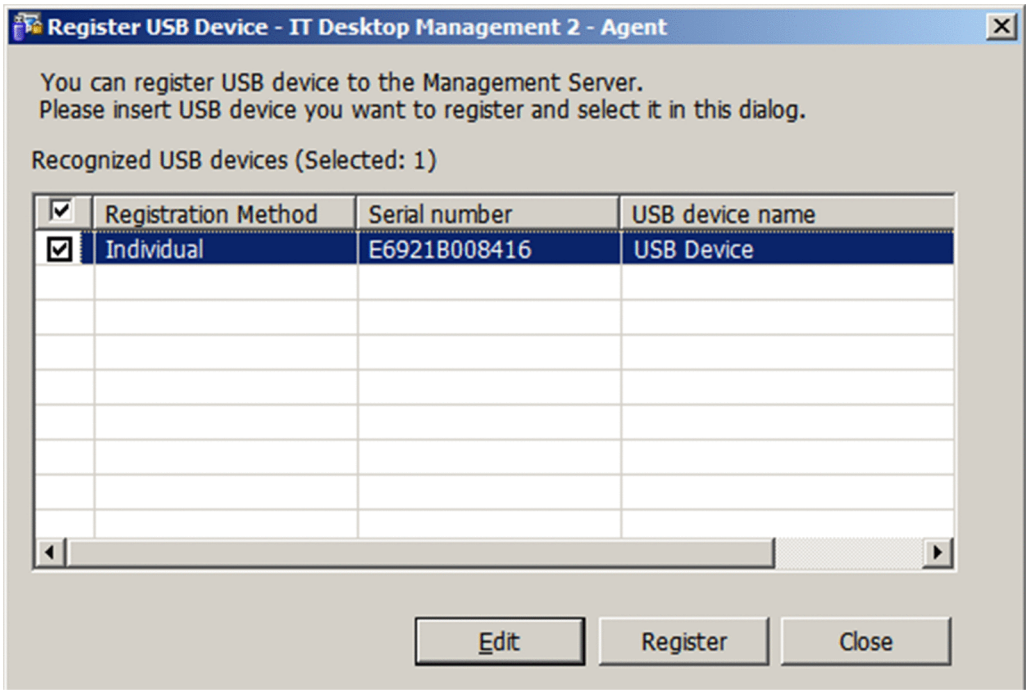
- 1.7.8 Restricting the use of USB devices
- 9.7 Registering USB devices

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 2 - 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 2 password `manager` is set.

3. Connect the USB device to the computer.

> **Important**
>
> 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 2.

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

While **Register USB Device** is displayed on a computer, suppression of USB devices is temporarily disabled on that computer even if the use of USB devices is suppressed.

Tip

- UBS devices whose device instance IDs begin with the specified value will be registered.
- 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.

Tip

You can also register USB devices from the management server by setting device instance IDs. For details on how to register a USB device from the management server, see 11.1.1 Adding hardware asset information.

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 Windows Update (ITDM-compatible distribution)**, 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 2.

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:

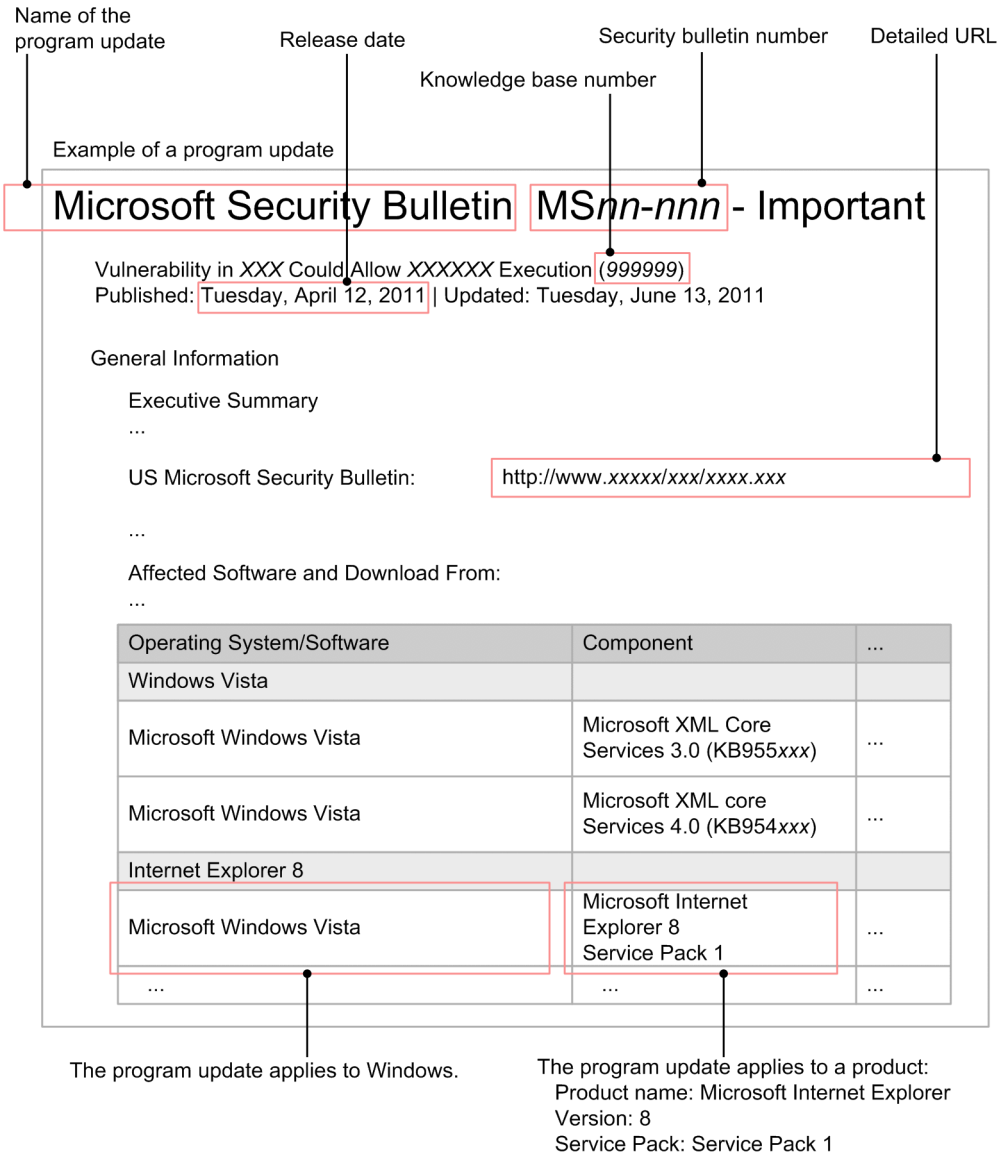
1. Open the security page.
   From the Microsoft Japan website, open the security page (security home page).
2. From the security page, check the detailed information about the program updates.
   From the security page, click the link to the program updates and display the information page for the program 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 2.
   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.
   If service packs for Windows or other products have been applied, be sure to specify information about those service packs.

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 (ITDM-compatible) 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 (ITDM-compatible) 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

9.8.11 Registering the same updated programs with multiple management servers

You can export the information of updated programs from a management server in a representative location and then import the information to management servers in different locations.

To export the information of updated programs from a management server and import the information to a different management server:

1. On a representative management server, execute the `ioutils exportupdatelist` command to export the updated program list (also called patch information CSV file).
2. On management servers in different locations, execute the `ioutils importupdatelist` command to import the updated program list (patch information CSV file).
   By using the `-import` option of the `ioutils importupdatelist` command, specify the patch information CSV file that you exported in step 1.

Now, the same updated programs as those on a representative management server are registered with multiple management servers in different locations.

Related Topics:

- 17.18 ioutils exportupdatelist (exporting the updated program list)
- 17.19 ioutils importupdatelist (importing the updated program list)

9.9 Setting intervals for reporting prohibited-operation suppression events and operation logs to the higher-level system

You can set the interval (minutes or days) for reporting prohibited-operation suppression events and operation logs from a user's computer to the higher-level system.

To set the interval for reporting prohibited-operation suppression events and operation logs to the higher-level system:

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 you want to edit, and then click the **Edit** button.
   To add a new security policy, click the **Add** button.
4. Select **Common settings for prohibited operations and operation logs**, which is a security configuration item.
5. In **Intervals reporting prohibited operations and operation logs to the higher-level system**, select the interval for reporting prohibited-operation suppression events and operation logs from the user's computer to the higher-level system.
6. Click the **OK** button.

The interval for reporting prohibited-operation suppression events and operation logs to the higher-level system is set as specified in the common settings for prohibited operations and operation logs.

9.10 Setting the period for holding prohibited-operation suppression events and operation logs

You can set the maximum number of days for which prohibited-operation suppression events and operation logs can be retained on a user's computer before those events and operation logs are reported to the higher-level system.

To set the period for holding prohibited-operation suppression events and operation logs:

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 you want to edit, and then click the **Edit** button.
   To add a new security policy, click the **Add** button.
4. Select **Common settings for prohibited operations and operation logs**, which is a security configuration item.
5. In **Period for which prohibited operations and operation logs are kept on the user's computer**, specify the period for holding prohibited-operation suppression events and operation logs.
6. Click the **OK** button.

The period for holding prohibited-operation suppression events and operation logs is set as specified in the common settings for prohibited operations and operation logs.

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**
>
> To collect operation logs, the agent must be installed in advance on a computer from which operation logs are to be collected. Note that operation logs are not collected from offline-managed agents, and agents for UNIX or Mac.

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.
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
- 10.2 Viewing operation logs

10.2 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.

At the top of the view, a time chart is displayed, and the dates of operation logs are displayed on the view in a blue frame. If you click the button for a date, operation logs for that date are displayed at the top. Note that you cannot click the dates for which **No operation logs** 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.

If you narrow down information by using a filter, the target dates are displayed in a green frame.

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**
>
> If you specify the operation log backup folder during setup, operation logs are backed up. Operation logs are deleted from the database if they exceed the period specified in **Period for storing automatically restored operation logs:** (displayed by selecting **Operation Log Settings**, and then **Automatic restoration of operation logs** in the Setting module). Therefore, if you want to view past operation logs, import the backed up operation logs.

> **Tip**
>
> If it takes a long time to display operation logs, use **Operation Date/Time (Browser)** to narrow down the search range. Then specify search conditions such as **Department**, **Location**, **Source**, and **User Name** to narrow down the target devices.

Important

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 Inventory module.

To view the operation logs of the device, in the Inventory module, select **Device Inventory**, 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.

Tip

If the number of operation logs narrowed down by the filter exceeds 10,000, "10000+" is displayed.

Related Topics:

- 10.4 Viewing suspicious operation logs
- 10.6 Tracing operation logs
- 10.7.1 Importing old operation logs into a management server
- 17.20 ioutils exportoplog (exporting operation logs)

10.3 Specifying settings for detecting suspicious operations

To detect suspicious operations, specify settings for **Suspicious Operations To Be Reported** 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 Reported**.
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:

- 10.4 Viewing suspicious operation logs
- 10.5 Viewing events for suspicious operations

10.4 Viewing suspicious operation logs

If you select one or more of the following items for **Suspicious Operations To Be Reported** 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**.
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:

- 10.5 Viewing events for suspicious operations
- 10.2 Viewing operation logs
- 10.7.1 Importing old operation logs into a management server
- 10.6 Tracing operation logs

10.5 Viewing events for suspicious operations

If you specify settings for **Suspicious Operations To Be Reported** 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:

- 10.4 Viewing suspicious operation logs
- 15.7.1 Specifying settings for event notification

10.6 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**.
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 10.7.1 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.

> **Tip**
>
> You cannot trace imported HIBUN logs even when you click the **Trace** button. You can instead trace them by using the Operation Date and File Operation filters in the Operation Log List view.

Related Topics:

- 10.2 Viewing operation logs
- 10.4 Viewing suspicious operation logs
- 17.20 ioutils exportoplog (exporting operation logs)

10.7 Importing old operation logs

10.7.1 Importing old operation logs into a management server

If operation logs no longer exist in the operation log database, you can import old operation logs from an operation log backup.

> **Important**
>
> You cannot import operation logs (for the relevant range) that have been deleted from the operation log backup folder.

> **Tip**
>
> To import old operation logs, in the **Operation Log Settings** 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. To import operation logs for a longer range, increase the value in **Maximum number of days for which the operation logs are to be stored in the database**. Alternatively, in the Settings module, in the **Operation Log Settings** view, reduce the value in **Period for storing automatically restored 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 **Manually acquire the stored operation logs**.

   > **Important**
   >
   > If there is no operation log backup file, you cannot perform this operation.

4. In the dialog box that appears, specify the range of operation logs to be imported, and then click the **OK** button.
   Operation logs are imported and the import status is displayed.
5. Click the **Close** button.

The operation logs for the specified range are imported.

In the **Manually acquire the stored operation logs** dialog box, you can specify the computers from which you want to import operation logs. Import of a long range of operation logs or from many computers might require a long time due to the large amounts of data. We recommend that you specify target computers to narrow down operation logs to be imported. For details about how to specify computers from which to import operation logs, see 10.7.2 Importing operation logs from selected computers.

Tip

If you cannot specify a sufficient range of operation logs to be imported because too much data was previously imported, from **Action**, select **Delete the manually-acquired operation logs**, and then delete operation logs for the unnecessary range. Note that the deleted operation log is actually deleted at the same timing as that of Delete operation log database execution (1:00 every day by default).

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:

- 10.2 Viewing operation logs
- 10.6 Tracing operation logs
- 10.4 Viewing suspicious operation logs
- 15.3.2 Automatically restoring operation logs
- 17.20 ioutils exportoplog (exporting operation logs)

10.7.2 Importing operation logs from selected computers

To import operation logs for a long range or from many computers, you can select the computers from which to import operation logs. You can also import JP1/IT Desktop Management 2 operation logs.

Important

You cannot import operation logs (for the relevant range) that have been deleted from the operation log backup folder.

Tip

To import old operation logs, in the **Operation Log Settings** 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. To import operation logs for a longer range, increase the value in **Maximum number of days for which the operation logs are to be stored in the database**. Alternatively, in the Settings module, in the **Operation Log Settings** view, reduce the value in **Period for storing automatically restored operation logs:**.

To import operation logs from selected computers:

1. Display the Security module.
2. In the menu area, select **Operation Logs**, and then **Operation Log List**.
3. From **Action**, select **Manually acquire the stored operation logs**.

> **Important**
>
> If there is no operation log backup file, you cannot perform this operation.

4. In **Range of manual acquisition** of the dialog box, specify the range of operation logs to be imported.
5. In **Computers from which to manually acquire operation logs**, select **Acquire operation logs from selected computers.**, and then click the **Change** button.
6. In the dialog box that appears, select the computers from which you want to import operation logs, and then click the **Make Related** button.

   If you select the **Show only related items** check box, only the computers selected for import are displayed in the list. To exclude a selected computer from the import target, select the computer, and then click the **Exclude** button.
7. Click the **OK** button.

   The **Manual Acquisition of Stored Operation Logs** dialog box is redisplayed.
8. Click the **OK** button.
9. Import of operation logs begins, and the import status is displayed.
10. Click the **Close** button.

The operation logs for the specified range are imported from the target computers.

> **Important**
>
> Depending on the environment, import of operation logs for three months from 200 computers might require 2 hours or more. To reduce the import time, specify a shorter range for manual acquisition.

> **Tip**
>
> If you cannot specify a sufficient range of operation logs to be imported because too much data was previously imported, from **Action**, select **Delete the manually-acquired operation logs**, and then delete operation logs for the unnecessary range. Note that the deleted operation log is actually deleted at the same timing as that of Delete operation log database execution (1:00 every day by default).

> **Tip**
>
> You can also export operation logs by using the `ioutils exportoplog` command. We recommend that you export operation logs if you want to use them for other reference.

Related Topics:

- 10.2 Viewing operation logs
- 10.6 Tracing operation logs
- 10.4 Viewing suspicious operation logs
- 10.7.1 Importing old operation logs into a management server
- 17.20 ioutils exportoplog (exporting operation logs)

10.8 Managing operation log backup files

10.8.1 Deleting backup files from the operation log backup folder

You can delete backup files for unnecessary operation logs from the operation log backup folder to provide an area for storing operation logs.

> **Important**
>
> To delete operation log backup files from the backup folder, you must stop the services on the management server. Therefore, delete operation log backup files on a day of the week and a time of day when the manager server is not running.

To delete backup files from the operation log backup folder:

1. Open the operation log backup folder.
2. Delete unnecessary backup files.
   Operation log backup files are stored on a daily basis. Delete the folders of unnecessary dates.

The operation log backup files are deleted, and you can allocate an area for storing operation logs.

10.8.2 Backing up operation logs

Because the amount of operation log data is likely to become large, we recommend that you periodically back up operation logs on another disk. You can back up operation logs while services on the management server are running.

To back up operation logs.

1. Open the operation log backup folder.
2. Copy the operation log backup files to a backup disk.
   Operation log backup files are stored on a daily basis.

The operation log backup files are saved in the backup disk.

> **Important**
>
> Do not copy files with extension `.copying`. Such files are being copied, or have failed to be copied.

> **Tip**
>
> To restore operation logs, move the backup files to the backup folder. After restoring operation logs, you need to restart the management server.

10.8.3 Temporarily changing the operation log backup folder

You can temporarily change the operation log backup folder to handle errors or for maintenance.

> **Tip**
>
> Prepare a disk (temporary disk) where operation logs are temporarily saved.

To change the operation log backup folder:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, and then **Setup**.
2. Click the **Next** button until the **Operation Log Settings** view appears. In the **Operation Log Settings** view, specify a temporary disk in **Operation log backup folder**.
3. Click the **Next** button until the **Confirm Setup Settings** view appears. In the window indicating completion of setup, click the **OK** button.
4. After an operation such as error handling or maintenance is completed, perform steps 1 to 3 again to resume the original settings of the operation log backup folder.
5. Move the operation log backup files from the temporary disk to the original backup folder.
6. Restart the services on the management server.

The operation log backup files are stored in the original backup folder.

> **Important**
>
> Do not copy files with extension `.copying`. Such files are being copied, or have failed to be copied.

10.8.4 Changing the disk where operation logs are to be stored

If the amount of free space is insufficient on the disk where operation logs are stored, change the disk.

> **Tip**
>
> Prepare a disk where new operation logs are to be stored.

> **Important**
>
> To delete operation log backup files from the backup folder, you must stop the services on the management server. Therefore, delete operation log backup files on a day of the week and a time of day when the manager server is not running.

To change the disk where operation logs are stored:

1. Copy the operation log data to the new storage disk.

2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, and then **Setup**.

3. Click the **Next** button. In the **Operation Log Settings** view, specify the new storage disk in **Operation log backup folder**.

4. Click the **Next** button. In the window indicating completion of setup, click the **OK** button.

Operation logs are saved in the new storage location.

10.8.5 Changing the free disk space thresholds for operation logs

If available disk space for operation logs is insufficient, an event is displayed in the Events module. You can specify free-space thresholds that trigger this event to be reported.

To change the free disk space thresholds for operation logs:

1. Add the settings to the configuration file.
   The configuration file (`jdn_manager_config.conf`) is stored in:
   JP1/IT Desktop Management 2-installation-folder\mgr\conf

2. Restart the services for JP1/IT Desktop Management 2.

Events will be reported according to the settings specified in the configuration file.

The following table shows the definitions you can specify in the configuration file:

Property	Description	Set value calculation formula
Capacity_OplogDBPathWarningThreshold	Free-space warning threshold for the operation log database folder	**Required capacity**-*of-the-operation-log-database* x 0.1
Capacity_OplogDBPathErrorThreshold	Free-space error threshold for the operation log database folder	**Required capacity**-*of-the-operation-log-database* x 0.03
Capacity_OplogBKPathWarningThreshold	Free-space warning threshold for the operation log backup folder (periodical export is disabled)	70 KB x *number-of-managed-devices* x 7
Capacity_OplogBKPathErrorThreshold	Free-space error threshold for the operation log backup folder (periodical export is disabled)	70 KB x *number-of-managed-devices* x 3
Capacity_OplogBKPathWarningThreshold_ExportEnabled	Free-space warning threshold for the operation log backup folder (periodical export is enabled)	730 KB x *number-of-managed-devices* x 7
Capacity_OplogBKPathErrorThreshold_ExportEnabled	Free-space error threshold for the operation log backup folder (periodical export is enabled)	730 KB x *number-of-managed-devices* x 3
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportDisabled	Free-space warning threshold for the data folder (operation log is enabled and periodical export is disabled)	15.3 MB x *number-of-managed-devices* x 0.5 + 3 GB
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportDisabled	Free-space error threshold for the data folder (operation log is enabled and periodical export is disabled)	15.3 MB x *number-of-managed-devices* x 0.3 + 500 MB
Capacity_DataPathWarningThreshold_OpLogEnabled_ExportEnabled	Free-space warning threshold for the data folder (operation log is enabled and periodical export is enabled)	21.4 MB x *number-of-managed-devices* x 0.5 + 3 GB

Property	Description	Set value calculation formula
Capacity_DataPathErrorThreshold_OpLogEnabled_ExportEnabled	Free-space error threshold for the data folder (both operation log and periodical export are enabled)	21.4 MB x *number-of-managed-devices* x 0.3 + 500 MB

The following is an example of configuration file settings:

```
#
# Configuration file
#
# Free-space warning threshold for the operation log database folder
Capacity_OplogDBPathWarningThreshold=10000
```

10.9 Importing HIBUN logs

You can import the HIBUN log files that were output from the HIBUN server into the operation log database for JP1/IT Desktop Management 2.

Important

The formats of the HIBUN log file that JP1/IT Desktop Management 2 can import are shown below. Any other file format is not supported.

- Comma (,) separated CSV format
- UTF-8 (with BOM)

To import the HIBUN log:

1. On the HIBUN log relay server, export a HIBUN log file in CSV format.
   Execute the following HIBUN command:

```
sflogcmd /m:in:administrator-name:password
sflogcmd /c:dc:"full-path-to-the-storage-folder-of-the-HIBUN-log-file":"full-path-to-the-output-folder-of-the-HIBUN-operation-log-file-in-CSV-format":UTF-8:c:b
sflogcmd /m:ot
```

   For details about the HIBUN commands, see the manual *JP1/HIBUN Command Reference (for Administrators)*.

   Important

   Do not change the file name of the CSV file exported by the HIBUN command, nor edit the file contents.

2. Use the external log import command (`ioutils importexlog`) to import the HIBUN log file in CSV format.
   The HIBUN logs are imported into the operation log database.

Related Topics:

- 17.23 ioutils importexlog (importing external logs)

10.9.1 Operating daily import of HIBUN logs

You can examine daily HIBUN logs reported from client PCs by importing them into the JP1/IT Desktop Management 2 operation log. The following procedure shows an example of operating these logs.

To operate the logs:

1. Create a shared folder on the JP1/IT Desktop Management 2 management server, so that the HIBUN log relay server can access the folder.

2. On the HIBUN log relay server, use the Windows Task Scheduler to execute HIBUN commands on a regular basis to output HIBUN logs in CSV format.
   The logs should be output to the folder for the HIBUN log relay server, with the path containing the command execution date in its name. Specify the different output destinations between HIBUN logs on the previous day and

late-reported HIBUN logs (HIBUN logs older than or equal to two days ago). In this procedure, the output destination of the late-reported HIBUN logs is "*the-command-execution-date*_old".

3. Copy the CSV file that was output in step 2 to the JP1/IT Desktop Management 2 management server.

   The file should be copied to the folder for the JP1/IT Desktop Management 2 management server, with the path containing the command execution date and *the-command-execution-date*_old in its name.

4. Considering the time when the operations in steps 2 and 3 finish, execute the external log import command with the folders "the command execution date" and "*the-command-execution-date*_old" copied in step 3 as input.

   The HIBUN logs are now imported into JP1/IT Desktop Management 2.

   To acquire HIBUN logs on the previous day prior to the late-reported HIBUN logs, acquire logs in the order of "the command execution date" and "*the-command-execution-date*_old". Periodically delete the folder "the command execution date" and "*the-command-execution-date*_old".

HIBUN commands

The following example shows HIBUN commands you execute in step 2 of the *To operate the logs* section.

```
sflogcmd /m:in:administrator-name:password
sflogcmd /c:dc:"input-folder":"output-folder":UTF-8:c:b
sflogcmd /m:ot
```

The input-folder and output-folder should be specified as follows:

input-folder

HIBUN-log-relay-server-data-folder\User_Log*type-of-log**YYYY_MM**DD*

The type-of-log should be specified as one of the following:

Access log: `Access`, Event log: `Event`, HIBUN extended operation log: `OML`

output-folder

*any-folder**type-of-log_command-execution-date*

For the type-of-log, the type of log designated in the input-folder should be specified.

Example of the batch file to execute HIBUN commands

The following example shows a batch file that outputs HIBUN access logs for three days stored in the *data-folder-in-the-HIBUN-log-relay-server*\User_Log\Access folder to the `C:\work\HibunLog\Access\`*command-execution-date(in-YYYYMMDD-format)* folder in CSV format when the date display format in the OS is set to yyyy/MM/dd. To output logs on the preveous day, describe "`set IMPORTDAYS=2`" on the second line and "`set i=1`" on the third line. To output logs for four days from two days ago, describe "`set IMPORTDAYS=6`" on the second line and "`set i=2`" on the third line.

```
@echo off
set IMPORTDAYS=3
set i=0
sflogcmd /m:in:administrator-name:password
:days_loop
set PERIOD=%i%
call :getpastdate
call :getcurrentdate
sflogcmd /c:dc:"HIBUN-log-relay-server-data-folder\User_Log\Access\%PASTDATE
%":"C:\work\HibunLog\Access\%yy%%mm%%dd%":UTF-8:c:b
set /a i+=1
if %i% lss %IMPORTDAYS% goto days_loop
```

```
sflogcmd /m:ot
exit /b

rem Subroutine to return a date in the past (N days ago)
rem Set the number of days for the PERIOD variable and call the subroutine
rem Set the result (YYYY_MM\DD) for the PASTDATE variable
rem Set the current date for the yy, mm, and dd variables
:getpastdate

rem == Get the current date ==
call :getcurrentdate
set PASTDATE=%yy%_%mm%\%dd%
if %PERIOD% equ 0 exit /b

rem Calculate the date before the specified date
set n=0
:getpastdate_loop

set /a n=n+1
set /a dd=1%dd%-101
set dd=00%dd%
set dd=%dd:~-2%
set /a ymod=%yy% %% 4

rem == Operation for a new month or year ==
if %dd%==00 (
if %mm%==01 (set mm=12& set dd=31& set /a yy=%yy%-1)
if %mm%==02 (set mm=01& set dd=31)
if %mm%==03 (set mm=02& set dd=28& if %ymod%==0 (set dd=29))
if %mm%==04 (set mm=03& set dd=31)
if %mm%==05 (set mm=04& set dd=30)
if %mm%==06 (set mm=05& set dd=31)
if %mm%==07 (set mm=06& set dd=30)
if %mm%==08 (set mm=07& set dd=31)
if %mm%==09 (set mm=08& set dd=31)
if %mm%==10 (set mm=09& set dd=30)
if %mm%==11 (set mm=10& set dd=31)
if %mm%==12 (set mm=11& set dd=30)
)
if not %n% == %PERIOD% goto getpastdate_loop
set PASTDATE=%yy%_%mm%\%dd%
exit /b

rem Subroutine to get the current date
rem Set the result for the yy, mm, and dd variables
:getcurrentdate

rem == Get the current date ==
set dt=%date%
rem == For the yyyy/MM/dd format ==
set yy=%dt:~0,4%
set mm=%dt:~5,2%
set dd=%dt:~8,2%
exit /b
```

External log import command

The following example shows the external log import command you execute in step 4 of the *To operate the logs* section. The execution result of the command is redirected to the execution result output file for output.

```
ioutils importexlog -import input-folder -log type-of-HIBUN-log >> execution
-result-output-file 2>>&1
```

The input-folder and the type-of-HIBUN-log should be specified in the following format:

input-folder

*any-folder**type-of-log*_*command-execution-date*

For the type-of-log, the type of log designated in the output-folder for the HIBUN command to be executed should be specified.

type-of-HIBUN-log

One of the following can be specified:

HA: HIBUN access log, HE: HIBUN event log, HO: HIBUN extended operation log

Example of the batch file to execute the external log import command

The following example shows a batch file that imports HIBUN access logs stored in the `C:\work\HibunLog\Access\`*command-execution-date(in-YYYYMMDD-format)* folder and outputs the execution result to the `C:\log\HA_`*command-execution-date(in-YYYYMMDD-format)*`.log` when the date display format in the OS is set to yyyy/MM/dd.

```
@echo off
setlocal
call :getcurrentdate
ioutils importexlog -import C:\work\HibunLog\Access\%yy%%mm%%dd% -log HA >>
C:\log\HA_%yy%%mm%%dd%.log 2>>&1
exit /b

rem Subroutine to get the current date
rem Set the result for the yy, mm, and dd variables
:getcurrentdate

rem == Get the current date ==
set dt=%date%
rem == For the yyyy/MM/dd format ==
set yy=%dt:~0,4%
set mm=%dt:~5,2%
set dd=%dt:~8,2%
exit /b
```

When HIBUN logs are imported from multiple HIBUN log relay servers

If you import HIBUN logs from multiple HIBUN log relay servers, create a folder for each log relay server that stores the CSV file, on the JP1/IT Desktop Management 2 management server.

Time to import HIBUN logs

When you execute the step 2 and 3 at 00:30 and execute the step 4 at 03:00 of the above "To operate the logs:", in the list view of operation logs, you can see the operation logs notified on the previous day.

Importing late-reported logs

A management target PC is sometimes brought to the outside of the company, and its logs cannot be reported to the HIBUN log relay server.

For example, if you want to import HIBUN logs that are reported one month later into JP1/IT Desktop Management 2, you need to output the HIBUN logs for one month as a CSV file and then use the external log import command to import the file.

Depending on the environment of the management server and the number of days for which HIBUN logs are to be acquired, it might take more than one day for HIBUN logs to be acquired. In this case, consider an operation to reduce the number of days for which HIBUN logs are to be acquired.

Operation in a multi-server configuration

When JP1/IT Desktop Management 2 is configured in the multi-server configuration, operate the system as follows:

1. Copy the CSV file containing HIBUN logs to the management server that stores the operation logs.
2. On the management server in step 1, execute the external log import command to import the HIBUN logs into JP1/IT Desktop Management 2.

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**
>
> 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

When the hardware asset information and device information are associated with each other, the **Inventory 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 Planned Asset Status** 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. With the Citrix XenApp and Microsoft RDS server, you cannot display a window for entering user information.

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 **Assets** in the Settings module and then **Asset Field Definitions**.

Related Topics:

- 15.4.1 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
- 11.1.16 Automatically changing the asset status of hardware assets associated with deleted devices

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 Planned Asset Status** 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 Planned Asset Status** 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 2 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 2, 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

If an error occurs when updating the stocktaking date, an asset which is not managed by JP1/IT Desktop Management 2 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 2 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. With the Citrix XenApp and Microsoft RDS server, you cannot display a window for entering user information. 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 2.

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**
   >
   > If an error occurs when updating the stocktaking date, an asset which is not managed by JP1/IT Desktop Management 2 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

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.

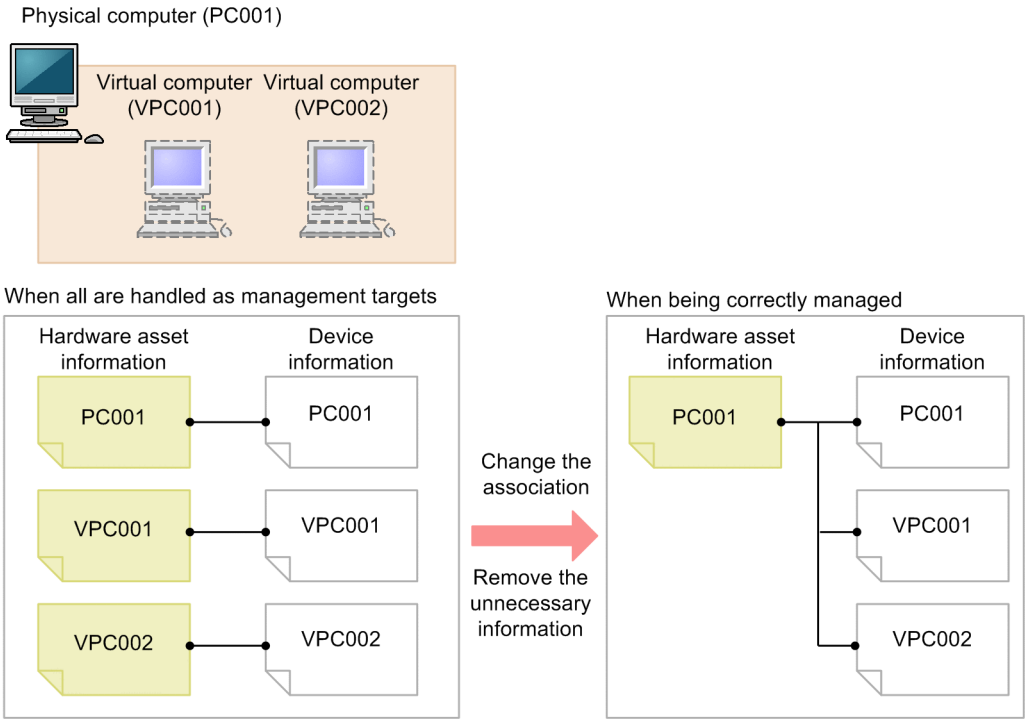
11.1.14 Changing the device information associated with the hardware asset information

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.

Tip

If the device specified as the primary inventory is removed or associated with other hardware asset information, the primary inventory changes as follows:

- When the device specified as the primary inventory is removed, another device associated with the hardware asset is changed to the primary inventory.
- If the association is changed so that the device specified as the primary inventory is associated with another hardware asset, another device that has already been associated with the hardware asset is used as the primary inventory.

In each case, if at least two devices are associated besides the device that is to be removed or whose association is to be changed, the device having the latest update date and time becomes the primary inventory. This also applies when duplicate devices and idle devices are automatically removed by auto maintenance of devices.

Related Topics:

- 11.1.14 Changing the device information associated with the hardware asset information

11.1.16 Automatically changing the asset status of hardware assets associated with deleted devices

You can configure settings so that, when a device is deleted, the asset status of hardware assets associated with that device is automatically changed to the **Disposed** status or to another status.

To configure settings to automatically change the asset status of hardware assets associated with deleted devices:

1. Display the Settings module.

2. In the menu area, select **Assets** and then **Asset Status Settings of Hardware Assets Associated with Deleted Devices**.
3. In the information area, select the **Change the asset status of hardware assets associated with deleted devices** check box.
4. Select the asset status to be set for assets whose associated devices have been deleted, and then click the **Apply** button.

Settings are now configured to automatically change the asset status of hardware assets associated with deleted devices.

Related Topics:

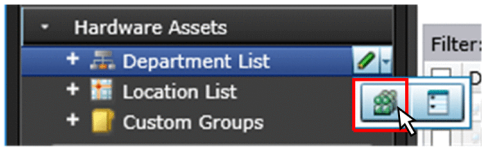
- 6.9 Removing a device
- 6.20 Procedure for deleting (from the local server) a device managed by a management relay server under the local server
- 6.38 Procedure for configuring device maintenance settings and checking detection results
- 11.1.5 Adding an asset status
- 11.1.6 Changing the asset status

11.1.17 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 Inventory 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 **Assets** and then **Asset Field Definitions**. In the window that appears, click either **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

> **Important**
>
> If there is a large number of departments and locations, it might take time to edit them in the **Asset Field Definitions** window. Use the `ioassetsfieldutil import` command to set departments and locations.

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 Inventory module.

Related Topics:

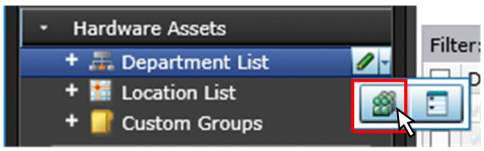
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location

11.1.18 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 Inventory 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 **Assets** and then **Asset Field Definitions**. In the window that appears, either click **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

> **Important**
>
> If there is a large number of departments and locations, it might take time to edit them in the **Asset Field Definitions** window. Use the `ioassetsfieldutil import` command to set departments and locations.

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 Inventory 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 Inventory 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 6.35 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:

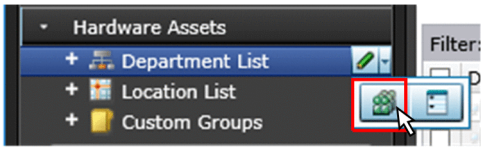
- 6.32 Adding the definition for a department or location
- 6.34 Removing the definition for a department or location

11.1.19 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 Inventory 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 Inventory 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 6.35 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location

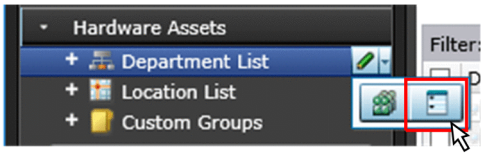
11.1.20 Removing only hierarchies that were used in the old organizational system

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 Inventory 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 Inventory 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 Inventory module is now consistent with the definitions.

11.1.21 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location
- 6.37 Deleting a department or location

11.1.22 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location
- 6.36 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 Inventory 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 Planned License Status** 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 Planned License Status** 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 Planned License Status** 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 2 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 2, 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

If an error occurs when updating the stocktaking date, an asset which is not managed by JP1/IT Desktop Management 2 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 2 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

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.

Note

To transfer, to a new device, the software licenses of a device to be deleted by device maintenance, transfer the software licenses before the device is automatically deleted. Alternatively, temporarily exclude the device from the target of automatic deletion until transfer of the software licenses is completed.

To transfer software licenses:

1. Display the Inventory module.
2. In the Inventory 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 **All Assets Cost** reports, **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 2 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**.
   You can update only registered assets by selecting the **Import only the asset information that matches the mapping key value** check box.
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.

> **Tip**
>
> When the **Import only the asset information that matches the mapping key value** check box is selected in the **Map Fields** view, asset information that is not registered is not imported. The number of rows that are not imported is displayed in **Skipped** of **Check Result Summary**.

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 **Assets** 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**.

> **Note**
>
> If a device corresponding to the mapping key exists in a detected device when the list of hardware assets is imported, an update is performed for the asset information of the device. However, this asset information is not displayed in the hardware asset list window until the device is set to be managed.

Related Topics:

- 11.5 Exporting asset information
- 17.4 ioutils exportasset (Exporting asset information)
- 17.5 ioutils importasset (Importing asset information)
- 17.10 ioutils exporttemplate (exporting template)
- 17.11 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.

> **Tip**
>
> You can also import software license information by executing the `ioutils importasset` command. The use of this command is recommended when software license information is periodically imported from a CSV file.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management 2 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 **Assets** 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
- 17.4 ioutils exportasset (Exporting asset information)
- 17.5 ioutils importasset (Importing asset information)
- 17.10 ioutils exporttemplate (exporting template)
- 17.11 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.

> **Tip**
>
> You can also import managed software information by executing the `ioutils importasset` command. The use of this command is recommended when managed software information is periodically imported from a CSV file.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management 2 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 **Assets** 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
- 17.4 ioutils exportasset (Exporting asset information)
- 17.5 ioutils importasset (Importing asset information)
- 17.10 ioutils exporttemplate (exporting template)
- 17.11 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.

Tip

You can also import contract information by executing the `ioutils importasset` command. The use of this command is recommended when contract information is periodically imported from a CSV file.

The **Import Assets** wizard relates items in a CSV file to the items managed in JP1/IT Desktop Management 2 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 **Assets** 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
- 17.4 ioutils exportasset (Exporting asset information)
- 17.5 ioutils importasset (Importing asset information)
- 17.10 ioutils exporttemplate (exporting template)
- 17.11 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.

> **Tip**
>
> You can also import a contract vendor list by executing the `ioutils importasset` command. The use of this command is recommended when a contract vendor list is periodically imported from a CSV file.

The **Import Assets** wizard relates items in a CSV file to items managed in JP1/IT Desktop Management 2 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 **Assets** 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 **Assets** and then **Last Import Log**. If you started the wizard from the Settings module, in the **Upload CSV file** view, specify **Contract Vendor List** for **Asset Type**.

Related Topics:

- 15.4.12 Exporting contract vendor lists
- 17.4 ioutils exportasset (Exporting asset information)
- 17.5 ioutils importasset (Importing asset information)
- 17.10 ioutils exporttemplate (exporting template)
- 17.11 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 following asset information by executing the `ioutils exportasset` command. We recommend that you use this command if you need to regularly export asset information.

- Hardware asset information
- Software license information
- Managed software information
- Contract information
- Contract vendor list

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.

Tip

When exporting the asset information that you registered in contract information, the items that are output vary depending on the contract type. If the contract type is **Fixed**, **Lease**, or **Rent**, the items **Contract Vendor Name** and **Contract Date** are output. However, if the contract type is **Maintenance** or **Support**, the items **Contract Vendor Name** and **Contract Date** are not output.

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 asset information)

11.6 Importing asset association information

You can import asset association information from a CSV file and add the imported asset associations to the list or edit all asset associations in one go.

You can import asset association information by executing the `ioutils importassetassoc` command.

Remember to confirm if the imported information has been correctly registered. If you find any records that have not been correctly registered, correct the CSV file and then import the asset association information again.

Related Topics:

- 11.7 Exporting asset association information
- 17.6 ioutils exportassetassoc (exporting asset association information)
- 17.7 ioutils importassetassoc (importing asset association information)

11.7 Exporting asset association information

You can export asset association information to a CSV file.

Each of the following assets can be associated with any one of the assets listed under it for export:

Hardware asset

- Device
- Hardware asset
- Contract

Software license

- Managed software
- License to be upgraded
- Device
- Contract

Managed software

- Software
- Software license

Contract

- Hardware asset
- Software license
- Contract vendor list

You can export asset association information by using the `ioutils exportassetassoc` command.

The CSV file is saved to the download destination under the specified name.

Related Topics:

- 11.6 Importing asset association information
- 17.6 ioutils exportassetassoc (exporting asset association information)
- 17.7 ioutils importassetassoc (importing asset association 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 (ITDM-compatible) 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 **Change Applicable 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 (ITDM-compatible) 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.

> **Important**
>
> You can register tasks to install Windows Store apps, but installation will not actually be performed. To install a Windows Store apps, you will need to perform installation on each target computer.

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 (ITDM-compatible) 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 **Change Applicable 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 (ITDM-compatible) 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 (ITDM-compatible) 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**.
   Only the software that completely matches the software name and version specified in the above view will be uninstalled.
6. In the **Select Target Computers** view, click the **Change** button.
7. In the **Change Applicable 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 (ITDM-compatible) 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.

> **Important**
>
> You can register tasks to uninstall Windows Store apps, but uninstallation will not actually be performed. To uninstall a Windows Store apps, you will need to perform uninstallation on each target computer.

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 (ITDM-compatible) 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 (ITDM-compatible) 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 (ITDM-compatible) 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**
>
> 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 (ITDM-compatible) 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 (ITDM-compatible) 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 (ITDM-compatible) 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 (ITDM-compatible) 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 (ITDM-compatible) 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 Inventory module.

> **Tip**
>
> To add a task based on a task that is already registered, copy the registered task.

Related Topics:

- 6.24 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 (ITDM-compatible) 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 (ITDM-compatible) 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**
>
> 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 (ITDM-compatible) 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 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 (ITDM-compatible) 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 (ITDM-compatible) 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 (ITDM-compatible) 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 (ITDM-compatible) 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**
>
> 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 (ITDM-compatible) 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.

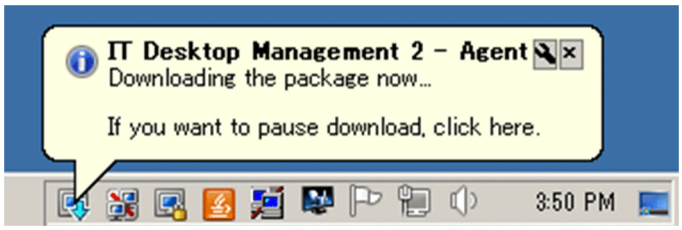
12.6 Postponing downloads and installation as a user

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.

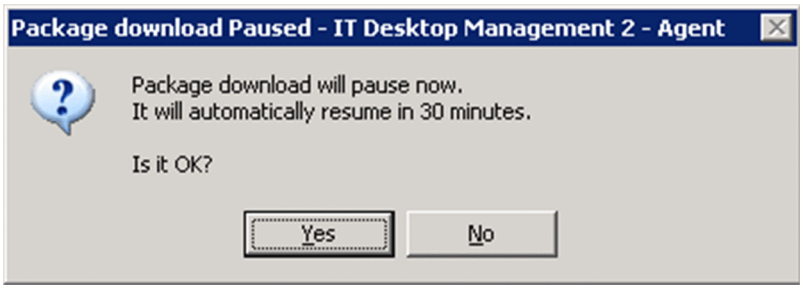
> **Tip**
>
> File distribution or uninstallation can also be postponed.

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 **User notification settings** view during agent setup.



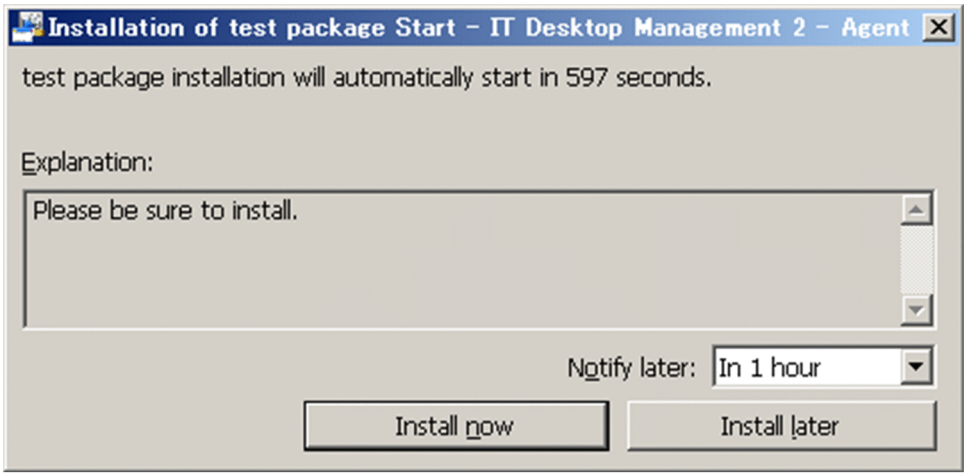
If you click the icon, a dialog box prompting you to temporarily stop package downloads appears.



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 2.

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 2 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 2 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.

Tip

When you install JP1/IT Desktop Management 2 version 12-10 or later for the first time, the **Hardware Assets Cost** report and the **Software License Cost** report display the total costs calculated based on the contract information valid at the time when the report is displayed.

When you upgrade JP1/IT Desktop Management 2 from a version earlier than 12-10 to 12-10 or later, the **Hardware Assets Cost** report and the **Software License Cost** report display the total costs calculated on the start date of each month.

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**
>
> 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 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:

- 15.1.1 Managing agent configurations
- 15.1.8 Regularly updating agentless device information

15.1.1 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 configurations.

To set different monitoring intervals for each computer, create agent configurations. For details about how to create agent configurations, see 15.1.2 Adding agent configurations.

If the operation status changes, edit the agent configurations. For details about how to edit agent configurations, see 15.1.3 Editing agent configurations. For details about how to edit agent configurations to enable a site server and network monitoring, see 15.1.4 Editing agent configurations that enable 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 15.1.5 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 15.1.6 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

15.1.2 Adding agent configurations

To use different agent configurations for different computers, you must add agent configurations.

To add agent configurations:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Windows Agent Configurations and Create Agent Installers**.
3. In the information area, click **Add Agent Configuration**.
4. In the **Add Agent Configuration** dialog box that appears, type the agent configuration information, and then click **OK**.
   For details about agent configuration information, see Agent parameters in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

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 **Windows Agent Configurations Assignment** view.

15.1.3 Editing agent configurations

To change the agent monitoring interval or agent protection settings, you can edit the agent configurations.

To edit agent configurations:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Windows Agent Configurations and Create Agent Installers**.
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:

- 15.1.2 Adding agent configurations
- 15.1.5 Removing agent configurations
- 15.1.6 Assigning agent configurations

15.1.4 Editing agent configurations that enable 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 **Windows Agent Configurations and Create Agent Installers**.

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**:
   - **Communicate with the higher system** check box in the **Basic settings** view
   - **Periodically notify the higher system of the information collected from the computer.** check box in the **Basic settings** view

The agent configuration is updated. In addition, the settings of computers to which the agent configuration is assigned are automatically updated.

15.1.5 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 15.1.6 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 **Windows Agent Configurations and Create Agent Installers**.

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:

- 15.1.2 Adding agent configurations
- 15.1.3 Editing agent configurations

15.1.6 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 **Windows 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 **Assign** 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 **Assign** 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 **Windows 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:

- 15.1.2 Adding agent configurations
- 15.1.3 Editing agent configurations
- 15.1.5 Removing agent configurations

15.1.7 Including remote control agents as agents to be deployed

To include remote control agents as agents to be deployed, from the Settings module, select **Agent** and then **Windows Agent Deployment**, and then change the settings.

To include remote control agents as agents to be deployed:

1. Display the Settings module.
2. From the menu area, select **Agent** and then **Windows Agent Deployment**.
3. In **Settings of the Components of the Agents to Be Deployed**, click the **Edit** button.
4. In the dialog box that appears, select **Include remote control agents**.
5. Click the **OK** button.

Remote control agents are now included as agents to be deployed.

> **Tip**
>
> To include remote control agents in an agent installer, specify the settings in **Components to Be Installed Settings** in the **Create Agent Installer** dialog box. For details, see 6.2 Creating an installation set.

15.1.8 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 2 recommends that you install the agent on managed computers for better security management.

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 the IP addresses for the 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.

   To add a discovery range, click the **Add IP Address Range** button. To modify an existing discovery range, click the **Edit** button associated with the discovery range name. Whether adding or editing a discovery range, a dialog box appears in which you can set the IP addresses to serve as the start and end of the discovery range.

   After setting the IP addresses, you can then set credentials in **Credentials Used**. If no credentials are registered, perform step 4 first.

   To use all registered credentials, select **Any**. To apply only some credentials, click **Select** and select from the credentials registered in Windows or SNMP.
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.

   For details about credentials, see 15.2.3 Credentials used in discovery from IP address.
5. Edit **Auto Discovery Schedule**.

   If you want to regularly perform searches according to a determined schedule, click the **Edit** button and specify the schedule.

   If no schedule is set, discovery will not take place automatically. In this case, you can initiate it as needed by clicking the **Start Discovery** button.
6. Edit **Edit Discovery Option**.

   Specify operations for cases in which a new device is discovered after the device search.

   Click the **Edit** button for the discovery option of a discovered device, and set the discovery option in the **Edit Discovery Option** dialog box that appears. The available options include adding the device as a managed node and automatically distributing the agent to the device.
7. Edit **Notification of Discovery Completion**.

To send a notification email to administrators of JP1/IT Desktop Management 2 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 2 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 2, click the **SMTP Server** link and set the mail server information in the window that appears.

> **Important**
>
> 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

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

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.

Important

When you perform the network discovery using Windows authentication in the environment where the discovery target computers do not have a common account and the discovery needs to use different credential information for the discovery target computers, the account of a discovery target computer might get locked. This problem occurs when all of the following conditions are met:

- Windows authentication is set for the discovery range.
- The account lockout policy is enabled in a discovery target computer.
- The authentication fails with the credential information in the discovery target computer in 2.

  This condition applies to the environment where a common account used by discovery target computers does not exist and the discovery needs to use different credentials for the discovery target computers.
- The network discovery is performed.

When you perform the network discovery by using Windows authentication for a discovery target computer in which the account lockout policy is enabled, divide the discovery range or remove unnecessary credentials to make the number of credentials to be used for the authentication fewer than the account lockout threshold number.

15.2.4 Checking the device discovery status

In JP1/IT Desktop Management 2, 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 2. 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 2. 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 2 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 2 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 Specifying settings for security management

You can change the schedule for judging the security status of a managed computer. You can also specify the settings relating to automatic restoration and export of operation logs.

Related Topics:

- 15.3.1 Changing the schedule for security judgment

15.3.1 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**
>
> The latest updated-program information and anti-virus product information can be downloaded automatically from the support service site. If you enable this function, to use the latest information for security status judgment, we recommend that you specify the schedule so that the information from the support service is updated before judgment.

Related Topics:

- 15.8.3 Setting information for connecting to the support service

15.3.2 Automatically restoring operation logs

You can specify settings to automatically restore operation logs.

To automatically restore operation logs:

1. Display the Settings module.
2. In the menu area, select **Security management**, and then **Operation Log Settings**.
3. In the information area, specify information for **Automatic restoration of operation logs**.
4. Click the **Apply** button.

Operation logs are automatically restored according to the specified settings.

> **Important**
>
> If **Period for storing automatically restored operation logs** is shorter than the currently set number of days, restart the JP1/IT Desktop Management 2 - Manager service.

Related Topics:

- 10.7.1 Importing old operation logs into a management server
- 10.7.2 Importing operation logs from selected computers

15.3.3 Periodically exporting operation logs

You can specify settings to periodically export operation logs in the CSV file format.

To periodically exporting operation logs:

1. Display the Settings module.
2. In the menu area, select **Security management**, and then **Operation Log Settings**.
3. In the information area, specify information for **Export of operation logs**.
4. Click the **Apply** button.

Operation logs are periodically exported according to the specified settings.

> **Tip**
>
> Exported operation logs are stored in the `export` folder under the operation log backup folder, which is specified in the **Operation Log Settings** view during setup.

Related Topics:

- 10.7.1 Importing old operation logs into a management server
- 10.7.2 Importing operation logs from selected computers
- A.4 Output format of exported operation logs

15.3.4 Setting the value displayed as the Windows OS version

You can set the value that is displayed as the OS version in the system information when a Windows update is installed on a managed computer (for example, a computer running Windows 10). To set the value that is displayed as the version, from the Settings module, select **Security** and then **Windows OS Version Settings**, and then change the settings.

Important

You can set only version numbers of versions that have been released on the support service site. For details, see the support service site.

To set the value displayed as the Windows OS version:

1. Display the Settings module.
2. In the menu area, select **Security** and then **Windows OS Version Settings**.
3. Click the **Add** button.
4. In the dialog box that appears, specify values for **OS** and **Version**.
5. Click the **OK** button.

The specified value is set as the value to be displayed as the OS version.

The specified value will be displayed in the **Add OS Service Pack or Version (Mandatory)** dialog box that can be accessed from the **Windows Update** view of the **Add Security Policy** dialog box or the **Edit Security Policy** dialog box of the Security module, and in the **System Details** tab of the Inventory module.

15.3.5 Judgment for cumulative updates and Security Monthly Quality Rollup for Windows

JP1/IT Desktop Management 2 - Manager determines whether cumulative updates or Security Monthly Quality Rollup (rollup updates) for Windows has been applied by using the following methods:

Expiration date of security judgment for cumulative updates and Security Monthly Quality Rollup for Windows

An expiration date is set for security judgment for cumulative updates and Security Monthly Quality Rollup for Windows so that after the expiration date, the security status is not determined.

Security judgment for unknown updates

When unknown updates# not present in the update information posted on the support service site are applied, it is assumed that the latest updates are applied.

#: Unknown updates are only which classification is the security fix program.

Security judgment for updates taking into consideration the grace period

If a grace period is set, which is a time period between the release of new updates and the successful application of the updates, even when the latest rollup updates have not been applied, the security status of managed computers is not assessed as "Not applied" during the set grace period.

Important

The security judgment for updates taking into consideration the grace period must be used together with the security judgment for unknown updates.

Important

If you use the security judgment for unknown updates, you cannot use the expiration date of security judgment for cumulative updates and Security Monthly Quality Rollup for Windows.

Important

If you use the expiration date of security judgment for cumulative updates and Security Monthly Quality Rollup for Windows, you cannot use the security judgment for unknown updates.

Important

If the version of JP1/IT Desktop Management 2 - Agent installed on a managed computer is earlier than 12-00, even when the use of the security judgment for unknown updates is enabled on this computer, this setting is disabled.

Also the setting the expiration date of security judgment for cumulative updates and Security Monthly Quality Rollup for Windows is disabled.

Important

Even when Microsoft releases rollup updates, these updates cannot be automatically distributed to computers until the latest update information is posted on the support service site. To distribute rollup updates under this circumstance, you have to manually distribute them.

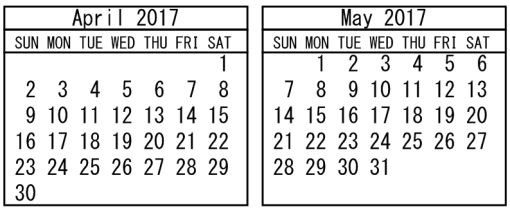
Tip

If you manually add rollup updates to the list, the updates are treated as normal updates instead of as rollup updates subjected to the security judgment.

(1) Expiration date of security judgment for cumulative updates and security monthly quality rollups for Windows

When a cumulative update or security monthly quality rollup (called monthly rollup) is installed on Windows, the last month's rollup is removed from Windows. Normally, JP1/IT Desktop Management 2 - Manager judges that the security level of a device is in danger if a target monthly rollup is not installed on the managed device. To prevent security judgment from being affected by removed monthly rollups, JP1/IT Desktop Management 2 - Manager no longer checks for a monthly rollup after a specified period expires.

For example, monthly rollups are released in April and May, 2017. Microsoft releases a monthly rollup on the second Tuesday of every month (in US time), which falls on April 11, 2017. The support service site releases a patch information file in late April so that JP1/IT Desktop Management 2 - Manager can import the file to start security judgment. In May, Microsoft releases a monthly rollup on the 9th of the month. JP1/IT Desktop Management 2 - Manager no longer checks for the April rollup on May 9 or later.



April 2017						
SUN	MON	TUE	WED	THU	FRI	SAT
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

May 2017						
SUN	MON	TUE	WED	THU	FRI	SAT
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

To change the expiration date, you need to edit the configuration file (jdn_manager_config.conf).

To change the expiration date for monthly rollup:

1. Add the property described below to the configuration file.
   The configuration file (jdn_manager_config.conf) exists in the following location:
   JP1/IT-Desktop-Management-2-installation-folder\mgr\conf

2. Restart the JP1/IT Desktop Management 2 service.

The following table describes the property to be added to the configuration file:

Property	Description	Value	Default
RollUpPatch_ExpirationDate	Expiration date for a monthly rollup judgment. The security judgment for a monthly rollup is no longer made after the specified date. The specified value is interpreted as a date in the Eastern Standard Time in US.	Specify 0 or a value in the format: *nth-week*,*day-of-week*. *nth-week* can be 1 to 5. *day-of-week* can be 1 to 7. The *day-of-week* value represents: 1: Sunday 2: Monday 3: Tuesday 4: Wednesday 5: Thursday 6: Friday 7: Saturday When 0 is specified, no expiration date is set on the judgment.	2,3 (The second Tuesday)

For example, the value 3,1 (the third Sunday) means that the judgment period expires on May 21, 2017.

(2) Security judgment for unknown updates

If you use security judgment for unknown updates#, JP1/IT Desktop Management 2 - Manager determines the security status even on the managed computers on which the unknown rollup updates not present in the update information posted on the support service site are applied.

#: Unknown updates are only which classification is the security fix program.

If you are using security judgment for unknown updates, open the Settings module, and select **Security** and then **Security Judgment Settings for Update Programs**. In the displayed view, select the **Include unsupported monthly rollups and cumulative updates when judging the security status of a computer** check box.

When rollup updates that are of a newer version than that of the update information posted on the support service site are installed on a computer, the rollup updates are treated as unknown rollup updates. Until the latest support service update information is reflected in JP1/IT Desktop Management 2 - Manager, it is assumed that the latest rollup updates

have been applied as long as either the latest rollup updates registered in the support service update information or the unknown rollup updates are applied.

If, on the other hand, the rollup updates applied to a computer are of an older version than that of the latest rollup updates registered in the update information posted on the support service site, it is assumed that the latest rollup updates have not been applied.

Rollup updates manual registration file

When there are serious flaws in rollup updates, modified rollup updates may be released. Adding the modified information to the rollup updates manual registration file described below enables the judgment of the updates with JP1/IT Desktop Management 2.

JP1/IT Desktop Management 2-installation-folder\mgr\conf\jdn_manager_security_patch.properties

The following table describes the specifications of the rollup updates manual registration file:

Item	Description
File format	Comma-separated values (CSV) file
Encoding	UTF-8 (without BOM)

Information inside the rollup updates manual registration file is processed according to the following rules:

- Spaces and tabs at the beginning or end of each line are ignored.
- A line starting with a hash mark (#) is ignored as a comment.

The following table describes the information specified in the rollup updates manual registration file:

Row	Field	Required or optional	Description	Acceptable value
1	Type	Required	Specify `replace`.	replace This means that the flawed rollup updates have been replaced by the modified rollup updates.
2	The article ID of the flawed rollup updates	Required	Specify the article ID of the flawed rollup updates.	A 1- to 10-digit number
3	The article ID of the modified rollup updates	Required	Specify the article ID of the modified rollup updates.	A 1- to 10-digit number
4	The date on which the modified rollup updates are released	Required	Specify the date on which the modified rollup updates are released. Specify the release date in U.S. time that is posted on Microsoft Knowledge Base.	*YYYY*/*MM*/*DD* format, where *YYYY* denotes the year, *MM* the month, and *DD* the date.
5	Exclusion setting	Optional	Specify whether JP1/IT Desktop Management 2 is to assess the security status as "Not applied" when the flawed rollup updates have been applied.	1 The security status is assessed as "Not applied" (rollup updates are not yet applied) when the flawed rollup updates have been applied.

Row	Field	Required or optional	Description	Acceptable value
5	Exclusion setting	Optional	Specify whether JP1/IT Desktop Management 2 is to assess the security status as "Not applied" when the flawed rollup updates have been applied.	Values other than 1 or blank Even when the flawed rollup updates have been applied, the security status is not assessed as "Not applied" (rollup updates are not yet applied). When a grace period is set, the security status is assessed as "Applied" (rollup updates are applied) during the set grace period.

Important

- If the rollup updates manual registration file has any lines that have an incorrect format or that are not correctly specified, the lines in question are ignored.
- This is valid only when "The article ID of the flawed rollup updates" is included in the update information posted on the support service site.
- If there are multiple lines specifying "The article ID of the flawed rollup updates", only the first line is valid.
- If "The article ID of the modified rollup updates" is already included in the update information posted on the support service site, the following operation is performed:
  - If 1 is specified as the "Exclusion setting", the flawed rollup updates are excluded from assessment.
  - "The date on which the modified rollup updates are released" remains unchanged.
  - If the flawed rollup updates are identical to the latest rollup updates and the modified rollup updates provided to address the flawed updates are identical to the old rollup updates, it is assumed that the specified information is incorrect and the line in question is ignored.

The following is an example of how information is specified in the rollup updates manual registration file:

```
replace,123456,55555,2018/01/04
replace,55555,22222,2018/06/07,1
replace, 987654,1543566,2018/07/01,0
```

(3) Security judgment for updates taking into consideration the grace period

It takes a certain period of time to apply updates. Security judgment can be performed by treating this period of time as a grace period. A grace period refers to a time period between the release of new updates from Microsoft and the successful application of the updates.

If you set a grace period, even when the applied rollup updates are not the latest ones, the security status is not assessed as "Not applied" (the latest rollup updates are not yet applied) during the set grace period.

You can set a grace period by using the Settings module. In the Settings module, select **Security**, and then **Security Judgment Settings for Update Programs**. In the displayed view, select the **Include unsupported monthly rollups and cumulative updates when judging the security status of a computer** check box and also the **Set the grace period for judging the security status of updates** check box. For Grace Period, set a value in the range from `1` to `180`. `7` is set by default.

Important

To set a grace period for applying updates, you have to use the security judgment for unknown updates.

Important

If you set a grace period, the updates that have not been applied yet are the latest ones.

15.4 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:

- 15.4.1 Adding asset management items
- 15.4.8 Managing contract vendor information

15.4.1 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 2 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.

15.4.2 Changing the data source or data type of asset management items

You can change the data source or data type 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.

You can change the data source or data type only for asset management items specified from the local server.

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 Inventory module.

Tip

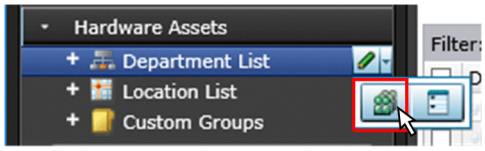
The data type of **Department** or **Location** can be changed. The added asset management items other than those two items cannot be changed to other data types once it has been specified.

15.4.3 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 Inventory 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 **Assets** and then **Asset Field Definitions**. In the window that appears, click either **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

Important

If there is a large number of departments and locations, it might take time to edit them in the **Asset Field Definitions** window. Use the `ioassetsfieldutil import` command to set departments and locations.

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 Inventory module.

Related Topics:

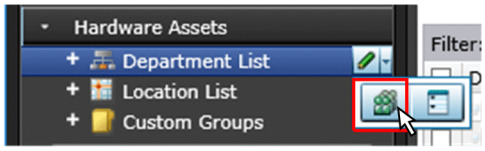
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location

15.4.4 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 Inventory 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 **Assets** and then **Asset Field Definitions**. In the window that appears, either click **Edit** in **Department** or **Location** in **Common Fields (Assets and Device Inventory)**.

> **Important**
>
> If there is a large number of departments and locations, it might take time to edit them in the **Asset Field Definitions** window. Use the `ioassetsfieldutil import` command to set departments and locations.

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 Inventory 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 Inventory 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 6.35 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:

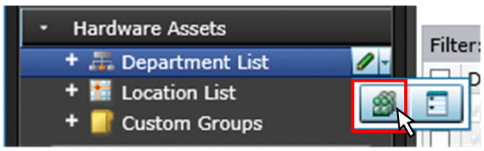
- 6.32 Adding the definition for a department or location
- 6.34 Removing the definition for a department or location

15.4.5 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 Inventory 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 Inventory 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 6.35 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:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location

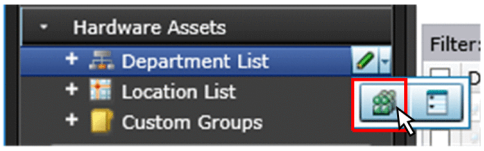
15.4.6 Setting the display names of departments and locations for each language

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. Click the link **Other Language Settings**.
4. In the displayed dialog box, set the display names for each language.
5. Click **OK**.
6. Click **OK**.

The display names of departments and locations for other language environments are set.

Related Topics:

- 6.32 Adding the definition for a department or location
- 6.33 Editing the definition for a department or location
- 6.34 Removing the definition for a department or location
- 6.36 Changing the name of a department or location

- 6.37 Deleting a department or location

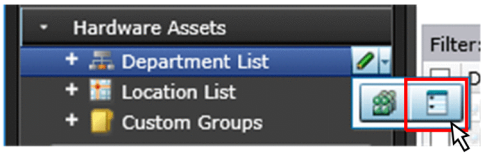
15.4.7 Removing only hierarchies that were used in the old organizational system

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 Inventory 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 Inventory 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 Inventory module is now consistent with the definitions.

15.4.8 Managing contract vendor information

If the contract information for an organization is managed by JP1/IT Desktop Management 2, 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 **Assets** 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 15.4.9 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 15.4.10 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 15.4.12 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 15.4.11 Removing contract vendor information.

Related Topics:

- 1.11 General procedure for managing asset contract information

15.4.9 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 **Assets** 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 **Assets**, 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:

- 15.4.10 Editing contract vendor information
- 15.4.11 Removing contract vendor information
- 11.4.5 Importing a contract vendor list
- 15.4.12 Exporting contract vendor lists

15.4.10 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 **Assets**, 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:

- 15.4.9 Adding contract vendor information
- 15.4.11 Removing contract vendor information
- 11.4.5 Importing a contract vendor list
- 15.4.12 Exporting contract vendor lists

15.4.11 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 **Assets**, 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:

- 15.4.9 Adding contract vendor information
- 15.4.10 Editing contract vendor information
- 11.4.5 Importing a contract vendor list
- 15.4.12 Exporting contract vendor lists

15.4.12 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 **Assets**, 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:

- 15.4.9 Adding contract vendor information
- 15.4.10 Editing contract vendor information
- 15.4.11 Removing contract vendor information

15.4.13 Procedure for applying asset management items to management relay servers under the local server

In a multi-server configuration, the settings of the asset management items specified on a higher management server can be shared by the lower management relay servers by applying those settings to the lower management relay servers. The start date for entry of user information can also be applied.

There are restrictions on asset management items that you can apply. For details, see the descriptions about applying asset management items to management relay servers, in the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

To apply asset management items to the management relay servers under the local server:

1. Display the Settings module.
2. In the menu area, select **Assets**, and then **Asset Field Definitions**.
3. In the information area, in **Apply to Management Server Under the Local Server**, click the **Apply to Management Server Under the Local Server** button.
4. In the displayed dialog box, select the items you want to apply.
   Items that you can select are as follows:
   - **Start Date for Entry of User Information**
   - Items displayed in the **Common Fields (Assets and Device Inventory)** list
   - **Custom Fields (Hardware Assets)**

5. Click **OK**.

6. In the displayed dialog box, click **OK**.

The asset management items are added to the management relay servers under the local server.

> **Tip**
>
> You can use the Events module for the management server from which you applied the asset management items to check whether the asset management items are completely applied to all management relay servers under the local server. In addition, to check whether the asset management items are completely applied to the specific management relay server, you can use the Events module in the operation window for the management relay server. If application fails, check the detailed information about the event, and then re-examine the settings on both of the application source and destination management servers.

Related Topics:

- 15.4.1 Adding asset management items
- 6.15 Obtaining user information

15.5 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:

- 15.5.7 Setting AMT credentials

15.5.1 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:

- 15.5.2 Editing software search conditions
- 15.5.3 Removing software search conditions
- 15.5.4 Importing software search conditions
- 15.5.5 Exporting software search conditions
- 15.5.6 Procedure for applying software search conditions to management relay servers under the local server

15.5.2 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.

Note that on the local server, you can edit only the software search conditions that have been locally set on that server.

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:

- 15.5.1 Adding software search conditions
- 15.5.3 Removing software search conditions
- 15.5.4 Importing software search conditions
- 15.5.5 Exporting software search conditions

15.5.3 Removing software search conditions

You can remove unused software search conditions.

> **Tip**
>
> In a multi-server configuration, you can remove, from the local server, the software search conditions applied from a higher management server. However, if the removed software search conditions are applied again from the higher management server, they are added to the local server again.

> **Tip**
>
> In a multi-server configuration, software search conditions that are removed from an application-source management server are not automatically removed from the application-destination management relay server. In this case, delete the software search conditions manually by using the operation window of the application-destination management relay server.

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:

- 15.5.1 Adding software search conditions
- 15.5.2 Editing software search conditions
- 15.5.4 Importing software search conditions

- 15.5.5 Exporting software search conditions

15.5.4 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:

- 15.5.1 Adding software search conditions
- 15.5.2 Editing software search conditions
- 15.5.3 Removing software search conditions
- 15.5.5 Exporting software search conditions

15.5.5 Exporting software search conditions

You can export (batch output) software search conditions to a CSV file.

In a multi-server configuration, the only software search conditions that can be exported from the local server are those that have been locally set on it. You cannot export software search conditions that have been applied from higher management servers.

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:

- 15.5.1 Adding software search conditions
- 15.5.2 Editing software search conditions
- 15.5.3 Removing software search conditions
- 15.5.4 Importing software search conditions

15.5.6 Procedure for applying software search conditions to management relay servers under the local server

You can apply software search conditions to all the management relay servers under the local server.

To apply software search conditions to management relay servers under the local server:

1. Display the Settings module of the management server from which you want to apply software search conditions.
2. In the menu area, select **Inventory** and then **Software Search Conditions**.
3. Select **Apply to Management Server Under the Local Server**.
4. In the **Apply the Software Search Conditions to a Management Server Under the Local Server** dialog box, select the **Continue Operation** check box.
5. Click **OK**.

All search conditions registered on the local management server are applied to all the management relay servers under the local server.

Tip

You can use the Events module for the management server from which you applied the software search conditions to check whether the software search conditions are completely applied to all management relay servers under the local server. In addition, to check whether the software search conditions are completely applied to the specific management relay server, you can use the Events module in the operation window for the management relay server. If application fails, check the detailed information about the event, and then re-examine the settings on both of the application source and destination management servers.

15.5.7 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 2, you must specify AMT settings for a management server and a user computer.

> **Important**
>
> 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:

- 6.27 Controlling the computer power

15.5.8 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. For a single-server configuration, select **Collect revision history**. For a multi-server configuration, select **Collect the revision history of devices that are directly under the device**.

4. In the case of a multi-server configuration, to acquire change histories sent from management relay servers under the local server, select **Collect the revision history of subordinate devices**.

   This procedure is unnecessary for a single-server configuration.

5. 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.

6. Click **Apply**.

You can now acquire the Revision History. You can view the Revision History in the **Revision History** view of the Inventory module. If, during setup, you set output of the revision history archive, you can output the acquired revision history archive to a file.

15.6 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:

- 15.6.1 Changing the storage period and start date for reports
- 15.6.2 Setting recipients of summary reports

15.6.1 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**.

15.6.2 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 2.

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:

- 15.8.1 Setting up mail servers
- 4. Managing User Accounts

15.7 Setting events

Related Topics:

- 15.7.1 Specifying settings for event notification

15.7.1 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:

- 15.8.1 Setting up mail servers
- 4. Managing User Accounts
- 19.1 List of events

15.8 Setting information about connecting to other systems

You can set the following information necessary for JP1/IT Desktop Management 2 to connect to other systems.

- Mail server information used by JP1/IT Desktop Management 2 to send email notifications
- Domain information of Active Directory to be searched
- Information for connecting to the support service site from which the latest updated program information or anti-virus product information can be obtained
- Information for connecting to MDM systems that are required for the smart device management

Related Topics:

- 15.8.1 Setting up mail servers
- 15.8.2 Setting information for connecting to Active Directory
- 15.8.3 Setting information for connecting to the support service
- 15.8.4 Specifying settings to link with an MDM system

15.8.1 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 2 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 2. 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)
- 15.6.2 Setting recipients of summary reports
- 15.7.1 Specifying settings for event notification

15.8.2 Setting information for connecting to Active Directory

To specify devices registered on Active Directory as a management target of JP1/IT Desktop Management 2 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)

15.8.3 Setting information for connecting to the support service

To determine whether the Windows security update is the latest or to use the latest anti-virus product as the security judgment item, you need to download information about the latest updates or anti-virus product periodically from the support service site. To do this, you must set information for connecting to the support service site.

By connecting to the support service site automatically, you can obtain the latest information about updates and anti-virus products.

By obtaining the latest information from the support service site, you can use the security policy to judge whether the latest updates or anti-virus products are applied to the managed computers.

Important

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 the schedule to obtain the latest information about updates and anti-virus products 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 **Update Customer Support Information Offline** dialog box or 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:

- 17.24 updatesupportinfo (uploading support service information)

15.8.4 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 2, you must specify information for connecting to the MDM system and the schedule for obtaining the smart device information.

Important

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 2 might fail to control smart devices.

To set information for linking with JP1/IT Desktop Management 2 - Smart Device Manager:

1. Display the Settings module of JP1/IT Desktop Management 2.
2. In the menu area, select **General** and then **MDM Linkage Settings**.
3. In the information area, click the **Add** button in the **MDM Linkage Settings**.
4. In the displayed dialog box, specify following information:

   MDM system

   Select `JP1/ITDM2 - SD Manager`.

   Hostname and port number of MDM Server

   Specify the same hostname you installed JP1/IT Desktop Management 2 - Smart Device Manager. Do not specify its IP address. Specify linking SSL port number of JP1/IT Desktop Management 2. Default port number for it is 26055.

   URL

   Specify the URL as follows.

   `https://`*`hostname`*`:`*`port-number`*`/jp1itdm2sdm/jp1itdm2sdm-login.htm`

   hostname is the same hostname you installed JP1/IT Desktop Management 2 - Smart Device Manager. *port-number* is the port number for the Management Console of JP1/IT Desktop Management 2 - Smart Device Manager. Default port number for it is 26080.

   Example: `http://SDMServer:26080/jp1itdm2sdm/jp1itdm2sdm-login.htm`

   User ID and Password

   Specify the user id and password you specified on the Management Console of JP1/IT Desktop Management 2 - Smart Device Manager. The user id must be defined as follows.

   User ID: `JP1MDM`*`YYYXX`*`@server01.jp1mdm.hitachi.jp`

   YYY: a decimal number (range 001 to 999), *XX*: a decimal number (range 01 to 05)

   Rights: Administrator

5. Click the **Test** button to check if a connection to theJP1/IT Desktop Management 2 - Smart Device Manager can be established.
6. Edit **Collection Schedule**.

   Specify the schedule if you want to regularly update the smart device information according to a determined schedule.
7. Click **OK**.
8. In the information area, click the **Edit** button in **Edit Discovery Option**.
9. In the displayed dialog box, specify whether the discovered smart device is to be automatically managed.

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 2 - Manager installation folder\mgr\uCPSB\jdk\jre\bin\keytool.exe -import -keystore *JP1/IT Desktop Management 2 - 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 2.

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.

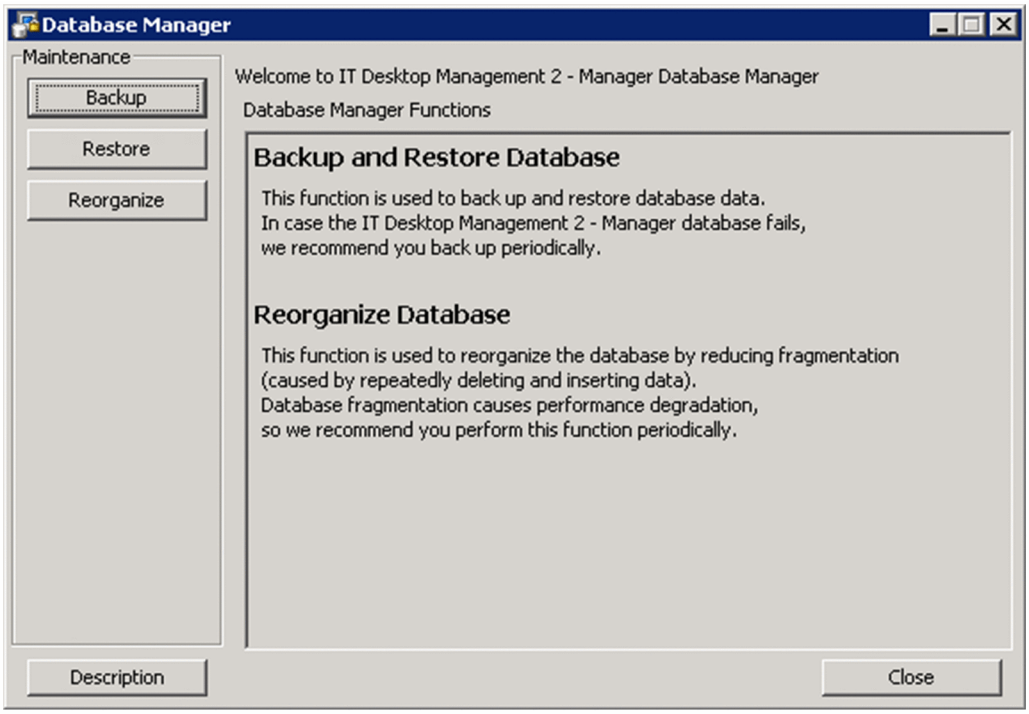
16.1 Starting a database manager

For a system in a database manager can be started from a management server.

Note that you can use a database manager only when the services for JP1_ITDM2_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 2 - 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**
>
> 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
- 16.4 Reorganizing databases

16.2 Backing up databases

This chapter describes how to back up a database by using a database manager.

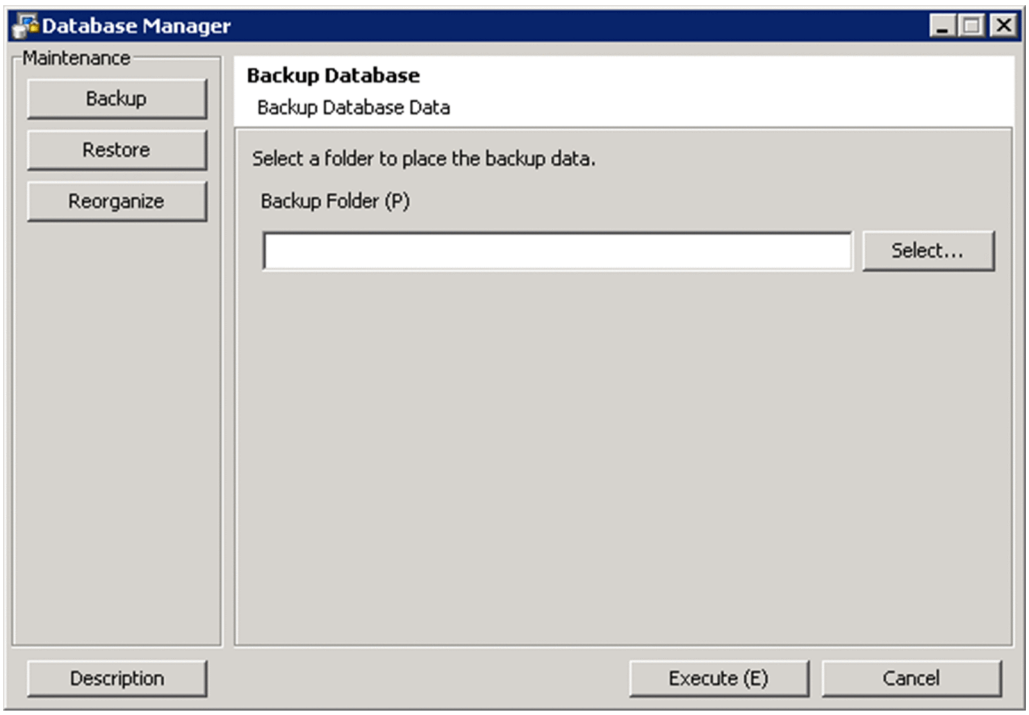
> **Tip**
>
> To back up a database, you must stop the management server. Therefore, choose a day or time of day for the backup that is during a time when the management server is not used.

> **Tip**
>
> The time required for a backup depends on the disc capacity. 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**
>
> If your computer is running Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders for **Backup Folder**.
>
> - *system-drive*:\Program Files\folders-in-WindowsApps
> - A storage folder 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 2 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**
>
> 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
- jdnagent.nid#

  #: Not output for a single-server configuration.

> **Important**
>
> A backup from the database manager might fail while data folders are being backed up. In this case, use the `exportdb.exe` command alternatively. The backup might be completed successfully.

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. 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

If your computer is running Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders for **Data Storage Folder**.

- *system-drive*:\program files\folders-in-WindowsApps
- Storage folders created by using thin provisioning

Important

In a multi-server configuration, if you restore a database on a management relay server, an inconsistency in device information occurs between the management relay server and the higher management server. For example, assume that, on a management relay server, you backed up data in January and then restored that data in February. As a result, the device information registered on the management relay server returns to the data of January, but the device information registered on the higher management server remains the same as the data of January. In such a case, establish consistency by sending the device information of the management relay information to the higher management server in the following procedure:

1. If you use the Remote Install Manager to distribute information, use the Remote Install Manager of the higher management server to execute a *Get system configuration information* job by specifying the management relay server as the destination.

   For creation and execution of jobs with the Remote Install Manager, see the descriptions of job creation in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

2. From the management relay server, notify the higher management server of all device information.

   To notify the higher management server of all device information, from the Inventory module, select **Device Inventory** and display the **Device List** window, and then from **Action**, select **Report all Device Details to the Higher Management Server**.

Important

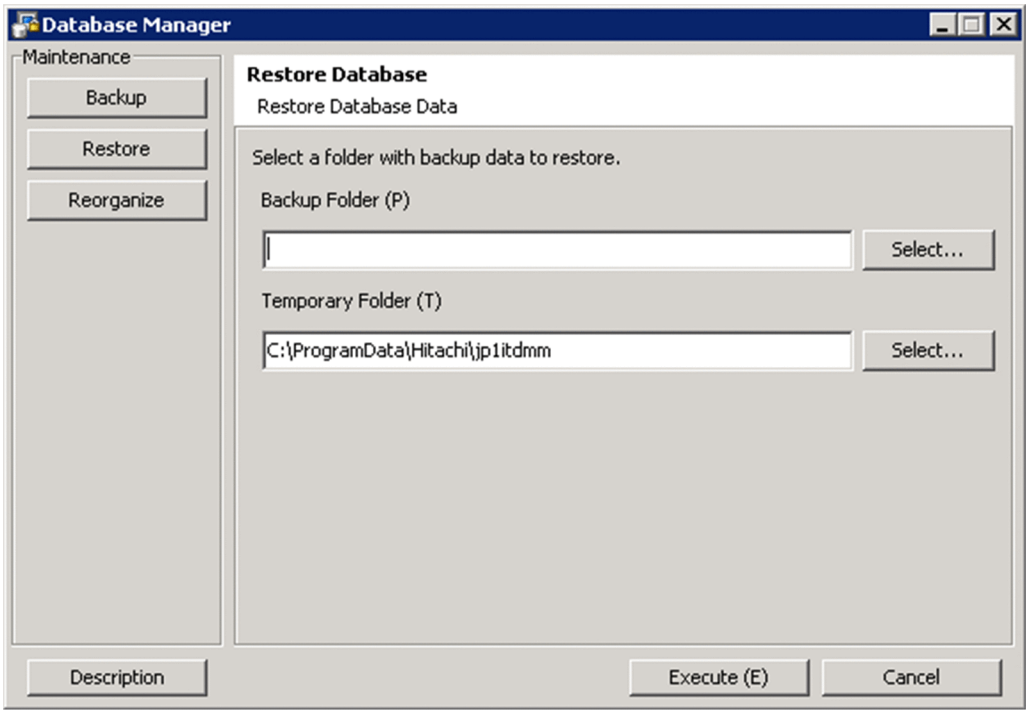
If you are using Asset Console, perform the following before restoring a database:

- Stop the World Wide Web Publishing Service or World Wide Web Publishing service.

- If the `jamTakeITDM2Info.exe` command that acquires information from JP1/IT Desktop Management 2 - Manager is being executed, stop the command.
- Disable the Acquisition of ITDM2 - Manager management information (Asset Console) task if it is registered in the Windows task scheduler.

After restoration of the database is completed, you must execute the `jamTakeITDM2Info.exe` command for Asset Console to acquire management information from JP1/IT Desktop Management 2 - Manager. When acquisition of the information is completed, restart the services, command, and task.

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

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**
>
> 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

If your computer is running Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders when setting folders.

- *system-drive*:\program files\folders-in-WindowsApps
- Storage folders created by using thin provisioning

Important

When executing database reorganization, if the database are being accessed from Remote Install Manager or JP1/IT Desktop Management 2 - Asset Console, the database reorganization may fail. The following measures should be taken before executing database reorganization.

- Terminate the remote installation manager.
- Check whether the command of the distribution function using the Remote Install Manager is not running.
- Check whether JP1/IT Desktop Management 2 - Asset Console is not acquiring management information.

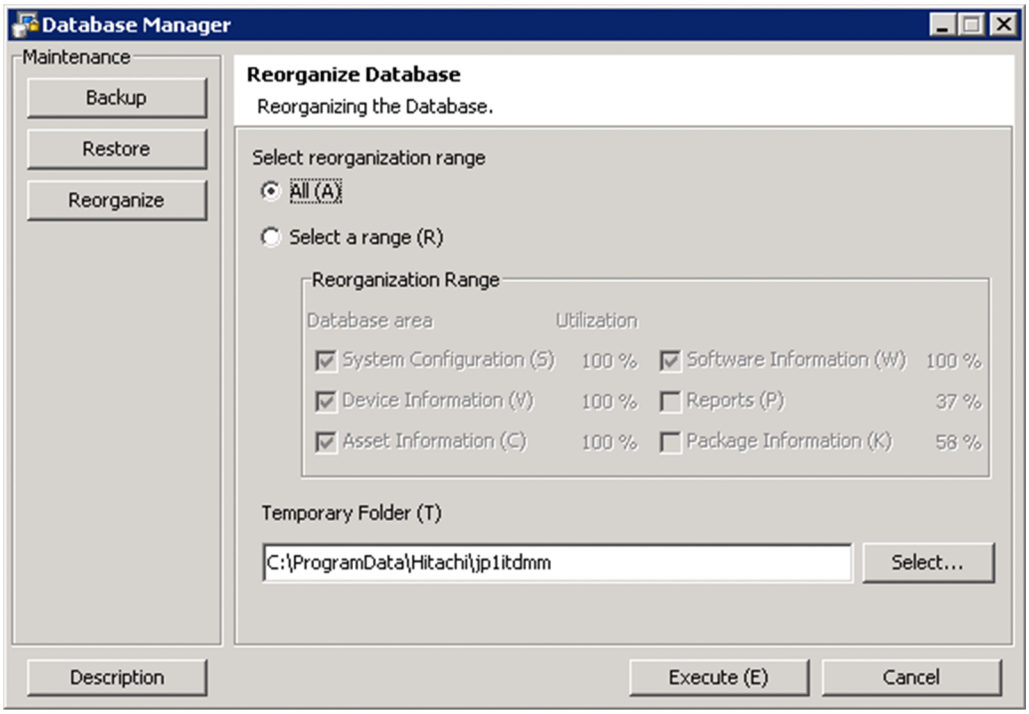
1. In the Database Manager view, from **Maintenance**, click the **Reorganize** button.
2. In the **Database Reorganization** view, select a range that you want to reorganize.

   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**
   >
   > 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 17.27 reorgdb (reorganizing the database).

Related Topics:

- 16.1 Starting a database manager

17 Commands

This section describes JP1/IT Desktop Management 2 commands.

17.1 Executing commands

To execute JP1/IT Desktop Management 2 commands, you can use either the dedicated command prompt (**JP1ITDM2 Utility Console**) or the Windows command prompt.

JP1ITDM2 Utility Console is useful when you execute commands on the management server. **JP1ITDM2 Utility Console** allows you to skip specification of a storage folder for the command execution file when entering a command. By default, when **JP1ITDM2 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, `setsecpolicy.vbs` command, and `upldoplog` command as a user who has administrator permissions. In Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008 R2, if User Account Control (UAC) is enabled, right-click and select **Run as administrator** to open **JP1ITDM2 Utility Console** or the Windows command prompt. Execute the `getinv.vbs` command, `setsecpolicy.vbs`, and `upldoplog` command command as a user who has full control permissions over the folder in which each command is stored.

To execute commands on an agent, use the Windows command prompt.

To execute commands on the management server:

1. From the Windows **Start** menu, select **All programs**, **JP1_IT Desktop Management 2 - 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 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 2 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 must be stopped. Make sure to check which day of the week or time of the day JP1/IT Desktop Management 2 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 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 **JP1ITDM2 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`
- `setsecpolicy.vbs`
- `upldoplog`
- `prepagt.bat`

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 2.

Command name	Functionality	Systems for the command to be executed in
`ioutils exportasset`	Exports asset information.	Management server
`ioutils importasset`	Imports asset information.	Management server
`ioutils exportassetassoc`	Exports asset association information.	Management server
`ioutils importassetassoc`	Imports asset association 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 exportupdatelist`	Exports a list of program updates that were manually registered with the management server (a CSV file containing patch information).	Management server
`ioutils importupdatelist`	Imports a list of program updates (a CSV file containing patch information) that was exported from a management server.	Management server
`ioutils exportoplog`	Export operation logs stored in a management server.	Management server
`ioutils exportfilter`	Exports filter settings.	Management server
`ioutils importfilter`	Imports filter settings.	Management server
`ioutils importexlog`	Imports CSV-format operation logs (external logs) collected from systems other than JP1/IT Desktop Management 2 into JP1/IT Desktop Management 2.	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

Command name	Functionality	Systems for the command to be executed in
`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 • Computer on which Remote Install Manager is installed
`getinstlogs`	Collects troubleshooting information about the installation process.	• Management server • Computer on which Remote Install Manager is installed
`addfwlist.bat`	Sets up Windows Firewall exceptions for JP1/IT Desktop Management 2.	• Management server • Computer on which Remote Install Manager is installed
`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
`distributelicense`	Permits distribution or registration of a license to a management relay server.	Primary management server
`itdm2nodecount`	Outputs the number of all managed devices under the control of the primary management server.	Primary management server
`deletenwgroup`	Deletes an unused network group registered on the management server.	Management server
`jdnrnetctrl`	Controls network access of devices by updating the network control list of the management server.	• Computers that can interact with the management server • Management server
`setsecpolicy.vbs`	Applies a security policy to an offline-managed computer and collects device information.	Agent
`deletelicense`	Deletes all product licenses registered in JP1/IT Desktop Management 2.	Management server
`upldoplog`	Uploads to the manager the agents' operation logs that have not been uploaded yet.	Agent
`prepagt.bat`	Deletes program-specific information from an agent to generalize it.	Agent
`deletepackage`	Delete unnecessary packages registered on the management server.	Management server
`softwaresearch`	Searches for software installed in the device with the agent.	Agent

Tip

The data I/O command (ioutils xxxx) also outputs information about UNIX or Mac devices. The `ioutils exportdevicedetail` command also outputs the kernel versions. Because kernel version is only for Linux, it is always empty for non-Linux devices.

17.4 ioutils exportasset (Exporting asset information)

Functionality

This command exports asset information to a CSV file.

This command can export the following asset information:

- Hardware asset information
- Software license information
- Managed software information
- Contract information
- Contract vendor list

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 management server.

Format

```
ioutils exportasset -export export-file-name [ -assettype asset-information-type] [ -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.

-assettype *asset-information-type*

Specify the type of asset information to be exported. The available types of asset information are provided below. If you omit this argument, `hardware` (hardware asset information) is specified.

hardware

Hardware asset information

license

Software license information

mngsoftware

Managed software information

contract

Contract information

vendor

Contract vendor list

-filter *filter-name*

To export 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 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the services on the management server are 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`

- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 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 asset information)

Functionality

This command imports asset information using a CSV file.

This command can import the following asset information:

- Hardware asset information
- Software license information
- Managed software information
- Contract information
- Contract vendor list

For details about asset items and the CSV file description format, see the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

When a CSV file is imported, asset information is updated with the values set in the CSV file. However, items whose values are empty (meaning, no values are enclosed in double quotation marks) in the CSV file will not be updated after importing (that is, hardware asset information is not overwritten with a null value).

Tip

If a single-byte space enclosed in double quotation marks (") is specified for a value, the value is processed depending on the condition, as follows:

- If the item is **Department** or **Location**, the value is updated to **Unknown**.
- If the data type of the item is **Text**, the value is updated to a blank.
- If the data type of the item is **Enumeration** or **Hierarchy**, the value is not updated.

When the CSV file contains an invalid value, the corresponding item does not get updated. If you specify the `-detaildisplay` option as an argument, information regarding the invalid value is printed on the standard output.

Execute this command on the management server.

Format

```
ioutils importasset -import import-file-name [ -assettype asset-information-type] -template template-name [ -encoding character-encoding] [ -prefix prefix] [ -detaildisplay]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to import.

-assettype *asset-information-type*

Specify the type of asset information to be imported. The available types of asset information are provided below. If you omit this argument, `hardware` (hardware asset information) is specified.

hardware
: Hardware asset information

license
: Software license information

mngsoftware
: Managed software information

contract
: Contract information

vendor
: Contract vendor list

-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 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

-prefix *prefix*

Specify a prefix to be assigned to the values of the following asset items:

- Asset numbers corresponding to hardware asset information
- License numbers corresponding to software license information
- Contract numbers corresponding to contract information

The specified prefix is assigned to the values of the above asset items.

> **Tip**
>
> If you specify the prefix, you can import the numbers so that they are not duplicated when you import asset information from other systems.

Specify a string of no more than eight ASCII characters except control characters as a prefix. When data with the prefix exceeds the maximum length of data allowed (32 characters), the data items in the corresponding row of the CSV file will not be imported.

When this argument is specified for importing asset information other than hardware assets, software licenses, and contracts, the argument is ignored.

-detaildisplay

Specify this argument when you want the following messages to be additionally printed to the standard output. For details about what cause these messages to be output, see the *JP1/IT Desktop Management 2 Messages*. When this argument is specified, the dots that are usually displayed to show the progress of processing do not show up in the window.

- Detection of invalid values in the imported data (KDEX4476-W)
- Row numbers corresponding to the error rows (rows that cannot be added or updated) (KDEX4477-W)

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`

- ioutils exportupdatelist
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

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 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 exportassetassoc (exporting asset association information)

Functionality

This command exports asset association information to a CSV file.

Each of the following assets can be associated with any one of the assets listed under it for export:

Hardware asset

- Device
- Hardware asset
- Contract

Software license

- Managed software
- License to be upgraded
- Device
- Contract

Managed software

- Software
- Software license

Contract

- Hardware asset
- Software license
- Contract vendor list

> **Note**
>
> Hereafter, an asset association will be expressed as follows:
>
> *asset-information -> relevant-asset-information*
>
> For example, hardware asset information associated with device information can be expressed as "Hardware asset -> Device."

When no exportable information exists, this command outputs an empty file.

> **Note**
>
> This command does not output a header row.

Execute this command on the management server.

Format

```
ioutils exportassetassoc -export export-file-name -assoc asset-association-information-to-be-exported[ -encoding character-encoding][ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to export.

-assoc *asset-association-information-to-be-exported*

Specify the asset association information to be exported. The following types of asset association information are available:

asset-device

Hardware asset -> Device

asset-asset

Hardware asset -> Hardware asset

asset-contract

Hardware asset -> Contract

license-mngsoftware

Software license -> Managed software

license-upglicense

Software license -> License to be upgraded

license-device

Software license -> Device

license-contract

Software license -> Contract

mngsoftware-software

Managed software -> Software

mngsoftware-license

Managed software -> Software license

contract-asset

Contract -> Hardware asset

contract-license

Contract -> Software license

contract-vendor

Contract -> Contract vendor list

-encoding *character-encoding*

Specify a character code for assert association 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the services on the management server are 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 exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`

- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

Return values

The following table shows the return values of the `ioutils exportassetassoc` 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.
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 the Hardware asset -> Device associations to C:¥temp ¥assetdeviceexpo.csv.

ioutils exportassetassoc -export C:\temp\assetdeviceexpo.csv -assoc asset-device -encoding UTF-8 -s

Related Topics:

- 17.1 Executing commands

17.7 ioutils importassetassoc (importing asset association information)

Functionality

This command imports asset association information to a CSV file.

Each of the following assets can be associated with any one of the assets listed under it for import:

Hardware asset

- Device
- Hardware asset
- Contract

Software license

- Managed software
- License to be upgraded
- Device
- Contract

Managed software

- Software
- Software license

Contract

- Hardware asset
- Software license
- Contract vendor list

Note

Hereafter, an asset association will be expressed as follows:

asset-information -> relevant-asset-information

For example, hardware asset information associated with device information can be expressed as "Hardware asset -> Device."

Note

This command imports all rows, including the first row, as data rows.

When the CSV file contains an invalid value, the corresponding item does not get updated. If you specify the `-detaildisplay` option as an argument, information regarding the invalid value is printed on the standard output.

Execute this command on the management server.

Format

```
ioutils importassetassoc -import import-file-name -assoc asset-association-i
nformation-to-be-imported[ -encoding character-encoding][ -asset#prefix pref
ix][ -license#prefix prefix][ -contract#prefix prefix][ -detaildisplay]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to import.

-assoc *asset-association-information-to-be-imported*

Specify the asset association information to be imported. The following types of asset association information are available:

asset-device

Hardware asset -> Device

asset-asset

Hardware asset -> Hardware asset

asset-contract

Hardware asset -> Contract

license-mngsoftware

Software license -> Managed software

license-upglicense

Software license -> License to be upgraded

license-device

Software license -> Device

license-contract

Software license -> Contract

mngsoftware-software

Managed software -> Software

mngsoftware-license

Managed software -> Software license

contract-asset

Contract -> Hardware asset

contract-license

Contract -> Software license

contract-vendor

Contract -> Contract vendor list

-encoding *character-encoding*

Specify a character code for assert association 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

-asset#prefix *prefix*

Specify a prefix to be assigned to the asset numbers corresponding to the hardware assets to be imported.

Specify a string of no more than eight ASCII characters except control characters as a prefix. When data with the prefix exceeds the maximum length of data allowed (32 characters), the data items in the corresponding row of the CSV file will not be imported.

When any data items to be imported do not have asset numbers, this argument is ignored.

-license#prefix *prefix*

Specify a prefix to be assigned to the license numbers corresponding to the software licenses to be imported.

Specify a string of no more than eight ASCII characters except control characters as a prefix. When data with the prefix exceeds the maximum length of data allowed (32 characters), the data items in the corresponding row of the CSV file will not be imported.

When any data items to be imported do not have license numbers, this argument is ignored.

-contract#prefix *prefix*

Specify a prefix to be assigned to the contract numbers corresponding to the contracts to be imported.

Specify a string of no more than eight ASCII characters except control characters as a prefix. When data with the prefix exceeds the maximum length of data allowed (32 characters), the data items in the corresponding row of the CSV file will not be imported.

When any data items to be imported do not have contract numbers, this argument is ignored.

-detaildisplay

Specify this argument when you want the following messages to be additionally printed to the standard output. For details about what cause these messages to be output, see the *JP1/IT Desktop Management 2 Messages*. When this argument is specified, the dots that are usually displayed to show the progress of processing do not show up in the window.

- Detection of invalid values in the imported data (KDEX4476-W)
- Row numbers corresponding to the error rows (rows that cannot be added or updated) (KDEX4477-W)

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc
- ioutils exportdevice
- ioutils exportdevicedetail
- ioutils exportfield
- ioutils exportfilter
- ioutils exportoplog
- ioutils exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

Return value

The following table shows the return values of the `ioutils importassetassoc` command.

Return values	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.

Return values	Description
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 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 the exported Hardware asset -> Device association information (assetdeviceexpo.csv) to C:¥temp¥ with host01 prefixed to the asset numbers.

ioutils importassetassoc -import C:\temp\assetdeviceexpo.csv -assoc asset-device -encoding UTF-8 -asset#prefix host01

Related Topics:

- 17.1 Executing commands

17.8 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 management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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.

Return value	Description
54	The management 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.
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

17.9 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 management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`

- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 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

17.10 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
- Contract Vendor List

If you have multiple JP1/IT Desktop Management 2 systems configured, this command enables a template created on one management server to be reused on another management server.

Execute this command on a management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
  - `deletenwgroup`
  - `deletepackage`
  - `distributelicense`

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 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

17.11 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 2 systems configured, this command enables a template created on one management server to be reused on another management server.

Execute this command on a management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`

- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 has not been set up.
74	An invalid template name is specified.
80	The format of the file being imported is invalid.

Return value	Description
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

17.12 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 2 systems configured, device information in one system can be reused in another system.

Execute this command on the management server.

Format

```
ioutils exportdevice -export export-file-name[ -filter filter-name][ -encodi
ng 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
  - `deletenwgroup`
  - `deletepackage`
  - `distributelicense`

- The argument `-s` cannot be specified in a cluster environment. 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 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

17.13 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 2 systems configured, device information in one system can be reused in another system.

Execute this command on the management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`

- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- The argument `-s` cannot be specified in a cluster environment. 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.
1	The command finished normally, but there is some invalid device information.
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.
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

17.14 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 2 systems configured, this command enables security policy settings created on one management server to be reused on another management server.

Execute this command on a management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`

- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- 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 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.

Return value	Description
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

17.15 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 2 systems configured, security policy settings created on one management server can be reused on another management server.

Execute this command on a management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
- `ioutils exportdevice`
- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- 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.

Return value	Description
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.
51	You do not have the permissions to execute this command.
54	The management 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 "updates not to import in Windows 7."

ioutils importpolicy -import C:\temp\exportpolicy.xml -name "policy for development group" -excludegroup "updates not to import in Windows 7." -s

Related Topics:

- 17.1 Executing commands

17.16 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 2 systems configured, an update group setting in one system can be reused in another system.

Execute this command on the management server.

Format

```
ioutils exportupdategroup -export export-file-name -name update-group-name[
-u][ -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.

-u

Specify this argument if you want to simultaneously export the settings of the update group to which the manually registered program update belongs.

-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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`

- `ioutils exportdevicedetail`
- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 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.

Return value	Description
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

17.17 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 2 systems configured, an update group setting in one system can be reused in another system.

Execute this command on the management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`

- ioutils exportfield
- ioutils exportfilter
- ioutils exportoplog
- ioutils exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

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 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.

Return value	Description
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

Furthermore, if you want to apply the manually added program update information to an update group on another system, first apply the manually added program update information to that system. To apply the update group settings on management server A to management server B, execute the commands in the following order:

1. On management server A, export the program update information.
2. On management server A, export the update group information.
3. On management server B, import the program update information output in step 1.
4. On management server B, import the update group information output in step 2.

Related Topics:

- 17.1 Executing commands

17.18 ioutils exportupdatelist (exporting the updated program list)

Functionality

This command exports the updated program list to a CSV file.

Note that this command must be executed on a management server.

Format

```
ioutils exportupdatelist -export export-file-name[ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of a CSV file to be exported.

-s

Overwrites an existing file with the same name at the export destination without confirmation. If this argument is not specified and a file with the same file name exists, an overwrite confirmation message appears. In this case, the system cancels the export or overwrites the file according to the administrator's reply.

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`

- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

Return value

The following table shows the return values of the `ioutils exportupdatelist` 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, appropriate access permissions are not set, or the disk capacity is not enough.
15	A file access error occurred when writing to the file, or the disk capacity is not enough.
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.
101	The command execution failed due to memory shortage or other reasons.
120	A database access error occurred.

Example

The following example shows use of this command to export an updated program list into C:\temp\updatelist.csv.

ioutils exportupdatelist -export C:\temp\updatelist.csv -s

Related Topics:

- 9.8.4 Manually registering program updates
- 9.8.11 Registering the same updated programs with multiple management servers

- 17.1 Executing commands
- A.5 Format of the updated program list (patch information CSV file)

17.19 ioutils importupdatelist (importing the updated program list)

Functionality

This command imports the updated program list (also called patch information CSV file). Note that executing this command clears the information of updated programs that were manually registered with the destination management server.

To prevent security judgment from being executed, stop the service (JP1_ITDM2_Service) and then execute the command.

Also note that this command must be executed on a management server.

Format

```
ioutils importupdatelist -import import-file-name[ -c]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the patch information CSV file to be imported.

-c

Checks whether the patch information CSV file contains valid information. The file is not actually imported.

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`

- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- This command assumes that the service (JP1_ITDM2_Service) is stopped. Therefore, execute this command at time when the operation is not obstructed.
- Because program update information that has been manually registered to the import-destination management server is cleared, you need to add the program updates to a program update group again.

  If a security judgment is executed before the program updates are added again, the program updates that had been manually registered are not evaluated, so please execute according to the following procedure.

  1. Stop the following service.
     - JP1_ITDM2_Service
  2. Execute the `ioutils importupdatelist` command.

     Tip

     When you execute the command, the program update information is cleared from the program update group, so execute the `ioutils exportupdategroup` (-u option) command in advance to export the program update group settings.
  3. Execute the `ioutils importupdategroup` command to add the imported program updates to a program update group.
  4. After command execution completed, start the following service.
     - JP1_ITDM2_Service

Return value

The following table shows the return values of the `ioutils importupdatelist` 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, appropriate access permissions are not set, or the disk capacity is not enough.
31	Another command is being executed.
39	The service (JP1_ITDM2_Service) is starting.
51	You do not have the permissions to execute this command.
54	The management server has not been set up.
80	The specified file contains invalid information.
101	The command execution failed due to memory shortage or other reasons.
120	A database access error occurred.
150	The command execution failed due to some other error.

Example

The following example shows use of this command to import the exported updated program list (updatelist.csv) from C:\temp\.

ioutils importupdatelist -import C:\temp\updatelist.csv

Related Topics:

- 9.8.4 Manually registering program updates
- 9.8.11 Registering the same updated programs with multiple management servers
- 17.1 Executing commands
- A.5 Format of the updated program list (patch information CSV file)

17.20 ioutils exportoplog (exporting operation logs)

Functionality

This command exports operation logs on the management server into a CSV file at a specified time.

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.4 Output format of exported operation logs.

Execute this command on the management server.

Format

```
ioutils exportoplog -export export-file-name{ -range export-period-of-time|
-within export-number-of-days}[ -encoding character-encoding][ -filter filte
r-name][ -linenumber-of-lines-to-export][ -timezone time-zone-type][ -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.

When setting the following filter conditions, add the Operation Type in parentheses to the filter condition. If not added to the filter condition, the output might be incorrect.

- Process Name (when the Operation Type is a Process/Program Operation)
- Destination File Drive Type (when the Operation Type is a File Operation)
- Operation Target File Name (when the Operation Type is a File Operation)
- Printed Document Name (when the Operation Type is a Print Operation)
- Device Name (when the Operation Type is a Device Operation)
- Device Catefory (when the Operation Type is a Device Operation)
- URL (when the Operation Type is a Web Access)
- Window Title (when the Operation Type is a Window Operation)

-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.

-timezone *time-zone-type*

Specify the time zone for the operation date and time to output.

The types of time zone are listed below. If you omit this argument, the system uses the `OpLog_ExportSouceDateAndTime` property defined in the configuration file (`jdn_manager_config.conf`). For details about the `OpLog_ExportSouceDateAndTime` property, see Lists of properties in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*. If the property is not defined, `local` is specified.

- `local`: Outputs the operation date and time of the agent with the time zone of the management server.
- `source`: Specify it when you want to output additional operation log information of the agent (Operation Date/Time (Agent), Operation Date/Time (UTC), and Time Zone).

-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 2-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 2.

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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
  - `deletenwgroup`
  - `deletepackage`
  - `distributelicense`

Return value

The following table shows the return values of `ioutils exportoplog` command.

Return value	Description
0	The command finished normally.

Return value	Description
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

17.21 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 2 systems configured, a filter in one system can be reused in another system.

Execute this command on the management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`

- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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.

Return value	Description
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.
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

17.22 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 2 systems configured, a filter in one system can be reused in another system.

Execute this command on the management 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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`

- ioutils exportoplog
- ioutils exportpolicy
- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- reorgdb
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- deletepackage
- distributelicense

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 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

17.23 ioutils importexlog (importing external logs)

Functionality

This command imports CSV-format operation logs (external logs) collected from systems other than JP1/IT Desktop Management 2 into JP1/IT Desktop Management 2.

The external logs are stored in the operation log backup folder that is configured during the setup. Also, if the system is configured to automatically restore operation logs in the Settings for Operation Logs view, they are automatically imported into the operation log database.

To execute the command, specify 1 for the `HibunLogImport` value in the configuration file for the external log import command.

You can import HIBUN logs into JP1/IT Desktop Management 2 by using this command. For details about the procedure, see *10.9 Importing HIBUN logs*.

Format

```
ioutils importexlog -import folder-where-the-CSV-format-log-file-to-be-imported-is-stored -log type-of-the-log-to-be-imported
```

Arguments

-import *folder-where-the-CSV-format-log-file-to-be-imported-is-stored*

Specify the absolute path within 200 byte length to the CSV-format log file folder to be imported.

-log *type-of-the-log-to-be-imported*

Specify the type of the log to be imported. One of the following can be specified:

- HA: HIBUN access log
- HE: HIBUN event log
- HO: HIBUN extended operation log

Storage location

JP1/IT Desktop Management 2-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 2.

Format of the configuration file for the external log import command

The following table lists and describes the specifications of the configuration file for the external log import command. Note that after you change settings in this file, restart the JP1/IT Desktop Management 2 service:

Item	Description
File name	`jdn_manager_importexlog_config.properties`
Storage location	*JP1/IT Desktop Management 2-installation-folder*\mgr\conf

The following table lists and describes the format of the configuration file for the external log import command:

Property	Description	Default value	Acceptable value
HibunLogImport	Specify 1 if HIBUN logs are imported.	0	0 or 1
UnknownLogImport.*type-of-log*	Specify 1 if unknown logs are imported. type-of-log One of the following can be specified: • HA: HIBUN access log • HE: HIBUN event log • HO: HIBUN extended operation log	0	0 or 1
Deny.*type-of-log*.*CSV-column-number*	Specify the log or logs you do not want to import, separated by commas (,). This property can be specified multiple times. type-of-log One of the following can be specified: • HA: HIBUN access log • HE: HIBUN event log • HO: HIBUN extended operation log CSV-column-number One of the following can be specified: • HIBUN access log: 12 or 13 • HIBUN event log: 12 • HIBUN extended operation log: 12 or 15	Deny.HA.12=NRD Deny.HA.13=CFL,OPN,WRI,COM	String

Important

If the value of `HibunLogImport` is set back to 0 from 1, filters do not work properly for the **Operation Type** and **Operation Type (Detail)** filters starting with `[HIBUN]` or the **Operations Logs** filter for which one of the device categories below is applied. You therefore need to re-create the filter.

- Removable media
- External hard disk
- CD or DVD drive
- Infrared device
- Wireless LAN
- Modem
- Windows Mobile device
- Palm handheld device
- BlackBerry device
- Serial or parallel port
- Other controlled device
- Wired LAN (USB connections)
- Wired LAN (non-USB connections)

The following example shows the configuration file for the external log import command:

HibunLogImport=1

Deny.HA.13=CFL,OPN

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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
  - `deletenwgroup`
  - `deletepackage`
  - `distributelicense`

- If the Task Scheduler is used to execute this command during operation, redirect the standard output and standard error to a file, so that you can view messages from the command.
- You can check the execution result of the command in the Events module. The event numbers are 1165, 1166, and 1167.
- The command skips processing of an invalid CSV file after printing a message (KDEX4129-W or KDEX4130-W) to the standard output, and then continues subsequent processing.
- In the multi-server configuration, the relay management server does not inform external logs it imported of the upper-level management server.
- In the cluster configuration, specify the folder on the shared disk for *folder-where-the-CSV-format-log-file-to-be-imported-is-stored*, so that the primary and standby servers can refer to the folder.

Return values

The following table shows the return values of the `ioutils importexlog` 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	Failed to store the file due to insufficient disk space or a disk access error.
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.
57	The configuration or environment for executing the command is invalid.
101	Command execution failed because there is not enough memory, or due to some other reason.
120	A database access error occurred.

Example

The following example shows how to use the command when HIBUN access log exported in CSV format found in the C:\temp\hibunlog folder is imported into JP1/IT Desktop Management 2:

ioutils importexlog -import C:\temp\hibunlog -log HA

Related Topics:

- 17.1 Executing commands

17.24 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 or when you want to update information in the SAMAC software dictionary, 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. Manually copy the downloaded information to the management server, and then execute this command to register the latest information to the management server.

Execute this command on the management server.

Format

```
updatesupportinfoΔ-iΔsupport-information-file-name-or-name-of-SAMAC-software
-dictionary-file-for-offline-update
```

Argument

-iΔ*support-information-file-name-or-name-of-SAMAC-software-dictionary-for-offline-update*

Specify the absolute path to the file to be registered to the management server (a support information file or a SAMAC software dictionary file for offline update). To specify a path containing a space, enclose the strings with double quotation marks (").

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`

- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- This command cannot be executed while a setup or database manager is running on the management 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.
51	You do not have the permissions to execute this command.
53	Services on the management server have not started.
54	The management 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

17.25 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 management 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 2 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 2 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 2-installation-folder\mgr\backup*YYYYMMDDhhmmss*

Example:

If the command is executed on January 1, 2011 at 2:30:00:

JP1/IT Desktop Management 2-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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is stopped.
- 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`
  - `stopservice`
  - `updatesupportinfo`
  - `deletenwgroup`
  - deletepackage
  - `distributelicense`
- The argument `-s` cannot be specified in a cluster environment. 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 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.
53	The management server is not stopped.
54	The management 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

17.26 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 management 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 2 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 2-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 2 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 2-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 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is stopped.
- 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`

- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- The argument `-s` cannot be specified in a cluster environment. 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 was in the process of starting when the command was 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.
53	The management server is not stopped.
54	The management 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.
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

17.27 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 management 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 2 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 2-installation-folder\mgr\temp

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management server setup is completed and the management server is stopped.
- 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 exportassetassoc`
    - `ioutils exportdevice`
    - `ioutils exportdevicedetail`
    - `ioutils exportfield`
    - `ioutils exportfilter`
    - `ioutils exportoplog`
    - `ioutils exportpolicy`
    - `ioutils exporttemplate`
    - `ioutils exportupdategroup`
    - `ioutils exportupdatelist`
    - `ioutils importasset`
    - `ioutils importassetassoc`
    - `ioutils importexlog`
    - `ioutils importfield`
    - `ioutils importfilter`
    - `ioutils importpolicy`
    - `ioutils importtemplate`
    - `ioutils importupdategroup`
    - `ioutils importupdatelist`
    - `startservice`
    - `stopservice`
    - `updatesupportinfo`
    - `deletenwgroup`
    - `deletepackage`
    - `distributelicense`
- The argument `-s` cannot be specified in a cluster environment. If you specify this argument, the command fails.
- When executing database reorganization, if the database are being accessed from Remote Install Manager or JP1/IT Desktop Management 2 - Asset Console, the database reorganization may fail. The following measures should be taken before executing database reorganization.
    - Terminate the remote installation manager.
    - Check whether the command of the distribution function using the Remote Install Manager is not running.
    - Check whether JP1/IT Desktop Management 2 - Asset Console is not acquiring management information.

Return value

The following table shows the return values of the `reorgdb` command.

Return value	Description
0	The command finished normally.

Return value	Description
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 was in the process of starting when the command was 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.
53	The management server is not stopped.
54	The management 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 services on the management server, reorganize the database, and automatically start the services on the management server.

reorgdb -s

Related Topics:

- 17.1 Executing commands

17.28 stopservice (stopping services)

Functionality

This command stops the JP1/IT Desktop Management 2 - Manager services to stop the management server.

Execute this command on the management server.

Format

```
stopservice
```

Arguments

No arguments are available for this command.

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`

- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 has already stopped.
11	The format for specifying the command arguments is invalid.
31	Another command is being executed.
35	The management server was in a startup process when the command is executed.
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 has not been set up.
101	Failed to stop the services on the management 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

17.29 startservice (starting services)

Functionality

This command starts the services associated with the management server to start the management server.

Execute this command on the management server.

Format

```
startservice
```

Arguments

No arguments are available for this command.

Storage location

JP1/IT Desktop Management 2-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 2.

Notes

- Execute this command when the management 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`

- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 is already running.
11	The format for specifying the command arguments is invalid.
31	Another command is being executed.
35	The management server was in a shutdown process when the command was executed.
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 has not been set up.
101	An attempt to start a service on the management 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

17.30 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.

When you execute the `getlogs` command on a management relay server, you also acquire troubleshooting information on the agents for the management relay server. Troubleshooting information on the agents for the management relay server is stored in *JP1/IT Desktop Management 2 installation destination folder* \mgr\log. For details, see the description on troubleshooting during agent installation in the *JP1/IT Desktop Management 2 Configuration Guide*.

Execute this command on the management server or a computer on which Remote Install Manager is installed.

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 2-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 2-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 2.

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

17.31 getinstlogs (collecting troubleshooting information about installation)

This section describes the `getinstlogs` command, which collects troubleshooting information during installation of JP1/IT Desktop Management 2 - Manager or Remote Install Manager.

Functionality

This command collects troubleshooting information in a batch. You, an administrator, require this information to contact the support service if you encounter a problem with an unknown cause or unresolved issues when installing JP1/IT Desktop Management 2 - Manager or Remote Install Manager.

Execute this command on the management server or a computer on which Remote Install Manager is installed.

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-2-distribution-media*_PPDIR*8-to-11-alphanumeric-characters*\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

17.32 addfwlist.bat (setting Windows firewall exceptions)

When you install JP1/IT Desktop Management 2 - Manager or Remote Install Manager on 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. Therefore, if you enable Windows Firewall after installing JP1/IT Desktop Management 2 - Manager or Remote Install Manager, use this command to set Windows Firewall exceptions.

Functionality

This command sets up Windows Firewall exceptions for JP1/IT Desktop Management 2 - Manager or Remote Install Manager.

Execute this command on the management server or a computer on which Remote Install Manager is installed.

Format

```
addfwlist.bat
```

Arguments

No arguments available for this command.

Storage location

JP1/IT Desktop Management 2-installation-folder\mgr\bin\

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 2.

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

17.33 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 duplicate an agent-installed virtual environment such as a VMWare environment, execute the `resetnid.vbs` command.

Important

When you manage shared VDI-based virtual computers, you cannot reset host IDs by using the `resetnid.vbs` command.

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 2, the host IDs assigned to the computer before and after the command execution are both registered to JP1/IT Desktop Management 2. 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.

Important

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.

To display return codes, execute `Cscript.exe` with the `/wait` option specified for the Windows `start` command, as described in the example below.

Format

```
resetnid.vbs△/nodeid [△/i |△/s]
```

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. Even when you omit this argument, the dialog box is displayed.

/s

Executes the command without displaying a dialog box. For the execution result of the command, check the return value.

Storage location

agent-installation-folder\bin\

Notes

When the `resetnid.vbs` command is executed, the time required to create a new host ID is equal to the shortest of the intervals specified for the items shown below. These items are defined under **Timing of communication with the higher system** in the **Basic settings** view for the agent configuration.

- **Monitoring Interval (Security) (min)**
- **Monitoring Interval (Others) (min)**
- Interval specified for the polling settings

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 how to use this command to reset the host ID when the agent installation folder is `C:\Program Files\Hitachi\jp1itdma`:

cd "C:\Program Files\Hitachi\jp1itdma\bin"

start /wait Cscript.exe resetnid.vbs /nodeid

echo %errorlevel%

Related Topics:

- 17.1 Executing commands

17.34 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
- To collect 64-bit OS machine (device) data by executing the Information Collection Tool, do not place the Information Collection Tool in the path (example: `C:\Windows\system32`) where the file system redirector is run by OS.

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
```

17.35 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 this command on the management server. Before executing the command, make sure that the management server setup is completed and the services on the management server are running.

Format

```
ioassetsfieldutil export -field export-file-name[ -encoding character-encodi
ng][ -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 2-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 2.

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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`
  - `reorgdb`
  - `startservice`
  - `stopservice`

- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

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 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

17.36 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 this command on the management server. Before executing the command, make sure that the management server setup is completed and the services on the management server are running.

Format

```
ioassetsfieldutil import -field import-file-name[ -agentupdate timing-for-st
arting-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 **Assets** 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 2-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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`

- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`
- `distributelicense`

- Do not execute this command while distribution is being executed. If you do, processing of the service (JP1_ITDM2_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 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

17.37 distributelicense (distributing licenses)

Functionality

This command is used to distribute licenses to a management relay server or to grant a management relay server permission to register licenses.

Note that you must execute this command on the primary management server.

Format

```
distributelicense{Δ-iΔfile-name|Δ-d}
```

Arguments

-i

Use an absolute path of 259 bytes or less to specify the name of the file in which you set distribution destinations, the number of licenses to be distributed, and other information.

-d

This option initializes the license distribution and license registration permission settings for the management relay servers under the local server. All the distributed licenses are collected into the primary management server. If you specify the -d option, a confirmation message is displayed.

Storage location

JP1/IT Desktop Management 2installation-destination-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided byJP1/IT Desktop Management 2.

File coding format

The following table describes the coding format of the file to be specified for the -i argument. Use a comma (,) to separate items.

Item	Required/ optional	Description	Input value
Host name of the management relay server	Required	Specify the host name of the management relay server to which the license is distributed. Make sure that the host name you specify is unique within the file.	Format of the host name
Processing mode	Required	Specify whether to distribute a license or to permit registration of a licence. • For distribution DIST • For registration permission REG	REG or DIST
Number of product licenses to be distributed	Required for distribution	Specify the number of licenses to be distributed to the management relay server. • For distribution Specify an integer of 1 or greater. • For registration permission No need to set a value	Integer of 1 or greater

Item	Required/ optional	Description	Input value
Comment	Optional	Set a comment.	Any character string of up to 128 characters

The following are coding examples:

Host1,DIST,100,comment

Host2,DIST,50,

Host3,REG,,

Notes

- Execute this command when the database services are running.
- Two or more instances of this command cannot be simultaneously executed.
- This command cannot be executed simultaneously with any of the following commands:
  - `exportdb`
  - `importdb`
  - `ioassetsfieldutil export`
  - `ioassetsfieldutil import`
  - `ioutils exportasset`
  - `ioutils exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`
  - `ioutils exportfield`
  - `ioutils exportfilter`
  - `ioutils exportoplog`
  - `ioutils exportpolicy`
  - `ioutils exporttemplate`
  - `ioutils exportupdategroup`
  - `ioutils exportupdatelist`
  - `ioutils importasset`
  - `ioutils importassetassoc`
  - `ioutils importexlog`
  - `ioutils importfield`
  - `ioutils importfilter`
  - `ioutils importpolicy`
  - `ioutils importtemplate`
  - `ioutils importupdategroup`
  - `ioutils importupdatelist`

- `reorgdb`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletenwgroup`
- `deletepackage`

Return values

The following table lists the return values of the `distributelicense`command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
12	The specified file path is invalid, or you do not have permission to access the file.
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.
58	The command was executed from other than a management server.
80	The format of the specified file is invalid.
101	Command execution was interrupted due to some other error.
110	The command execution failed due to a problem with a license.
120	A database access error occurred.

Example

The following example shows use of this command to distribute licenses by using license-distribution.csv (license distribution information) created in C:\temp\.

distributelicense -i C:\temp\license-distribution.csv

Related Topics:

- 17.1 Executing commands

17.38 itdm2nodecount (counting the number of managed devices)

Functionality

Executing this command outputs the number of all managed devices under the primary management server. However, management relay servers (which are not included in the count of licenses used) are excluded from the count of managed devices.

You must execute this command on the primary management server.

Format

```
itdm2nodecount
```

Arguments

None

Storage location

JP1/IT Desktop Management 2 installation-destination-folder\mgr\bin\

By using the command prompt provided by JP1/IT Desktop Management 2, you can execute this command without specifying the storage location for the executable file.

Notes

Execute this command when the primary management server setup is completed and the services are running.

Return values

The following table lists the return values of the `itdm2nodecount` command.

Return value	Description
0	The command finished normally.
4	Command execution was canceled.
84	The format for specifying the command arguments is invalid.
85	You do not have the permissions to execute this command.
86	The count of the number of managed devices failed.
127	Execution of the command failed.

Example

The following example shows use of this command to count the number of managed devices.

itdm2nodecount

Related Topics:

- 17.1 Executing commands

17.39 deletenwgroup (deleting network groups)

Functionality

This command deletes unused network groups registered in management servers. By periodically executing this command, you can prevent increase in the number of unused network groups.

A network group that matches all of the following conditions is determined as not in use, and is deleted. If there is no network group to be deleted, the command terminates normally.

- Network group to which no device belongs
- Network group to which no security policy has been applied
- Network group to which agent configurations have not been applied
- Network group not managed by the network monitor
- Network group that is not set in any user-defined group conditions
- Network groups to which no management relay server device belongs

Format

```
deletenwgroup[Δ-allseg]
```

Arguments

-allseg

Specify this argument to delete all network groups to which no device belongs. If you omit this argument, network groups with subnet mask 255.255.255.255 to which no devices belong are deleted.

Storage location

JP1/IT Desktop Management 2-installation-destination-folder\mgr\bin\

By using the command prompt provided by JP1/IT Desktop Management 2, you can execute this command without specifying the storage location for the executable file.

Notes

- Execute this command when the management server setup is completed and the services on the management server are 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 exportassetassoc`
  - `ioutils exportdevice`
  - `ioutils exportdevicedetail`

- `ioutils exportfield`
- `ioutils exportfilter`
- `ioutils exportoplog`
- `ioutils exportpolicy`
- `ioutils exporttemplate`
- `ioutils exportupdategroup`
- `ioutils exportupdatelist`
- `ioutils importasset`
- `ioutils importassetassoc`
- `ioutils importexlog`
- `ioutils importfield`
- `ioutils importfilter`
- `ioutils importpolicy`
- `ioutils importtemplate`
- `ioutils importupdategroup`
- `ioutils importupdatelist`
- `startservice`
- `stopservice`
- `updatesupportinfo`
- `deletepackage`
- `distributelicense`

- When executing this command at first, the large number of network groups to delete is expected, so please execute according to the following procedure.

  1. Stop the following services.
     - JP1_ITDM2_Agent Control
     - JP1_ITDM2_Service
     - JP1_ITDM2_Web Container
     - JP1_ITDM2_Web Server
     - JP1_ITDM2_Relay Manager Service#
  2. Execute the `deletenwgroup` command.
  3. After command execution completed, start the following services.
     - JP1_ITDM2_Agent Control
     - JP1_ITDM2_Service
     - JP1_ITDM2_Web Container
     - JP1_ITDM2_Web Server
     - JP1_ITDM2_Relay Manager Service#

  #: In case of the management server in a single-server configuration, stopping or starting of this service is not required.

Return value

The following table lists the return values of the `deletenwgroup`command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
53	Services on the management server have not started.
54	The primary management server has not been set up.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to delete all unused network groups.

deletenwgroup -allseg

Related Topics:

- 17.1 Executing commands

17.40 jdnrnetctrl (controlling network access)

Functionality

This command controls network access of devices by updating the network control list of the management server.

Messages generated while this command is running are written into the network control command message file. For details about the causes and actions concerning the output messages, see the *JP1/IT Desktop Management 2 Messages*.

Format

```
jdnrnetctrl -action {allow|deny}{ -hostname host-name| -ip IP-address| -host
name host-name -ip IP-address| -controlfile network-connection-control-file}
[ -matchoption {exact|forward}] -settingfile network-control-command-configu
ration-file
```

Arguments

-action {allow|deny}

Specify whether to allow the network access of the device.

allow: Allows the network access of the device.

deny: Does not allow the network access of the device.

-hostname *host-name*

Specify the host name of a device whose network access you want to control. When this argument is combined with -ip, the system finds a device that has the specified host name and the specified IP address to control network access.

-ip *IP-address*

Specify the IP address of a device whose network access you want to control. When this argument is combined with -hostname, the system finds a device that has the specified host name and the specified IP address to control network access.

-controlfile *network-connection-control-file*

Specify the absolute path of a CSV file (network connection control file) that contains the device information of network-connected devices.

-matchoption {exact|forward}

Specify how to match the specified host name to a host name of the device managed in JP1/IT Desktop Management 2.

exact (default): The system controls the network access of a device managed in JP1/IT Desktop Management 2 when its host name exactly matches the host name specified with the command.

forward: If the host name specified with the command is not an FQDN, the system controls the network access of a device managed in JP1/IT Desktop Management 2 when the device's host name part matches the host name specified with the command. If the host name specified with the command is an FQDN, the system controls the network access of a device managed in JP1/IT Desktop Management 2 when the device's host name exactly matches the host name specified with the command. We recommend that you specify this option value when there is a device that joins a domain group.

-settingfile *network-control-command-configuration-file*

Specify the absolute path of the network control command configuration file (ini file).

Storage location

Executing this command in an environment other than that of the management server

Store the files listed below in any folder located in the environment in which you are going to execute this command, and then execute the command.

JP1/IT Desktop Management 2-installation-folder\mgr\remote\

jdnrnetctrl.exe

jdnrnetctrl.ini

Executing this command on the management server

JP1/IT Desktop Management 2-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 2.

Edit the network control command configuration file shown below. Specify this as the argument of the command.

JP1/IT Desktop Management 2-installation-folder\mgr\conf\jdnrnetctrl.ini

Format of the network connection control file

The following table describes the specifications of the network connection control file:

Item	Description
File format	Comma-separated values (CSV) file
Encoding	UTF-8 (without BOM)

The following table describes the format of the network connection control file:

Row	Field	Required or optional	Description	Acceptable value
1	Host name	At least, either the host name or the IP address must be specified.	Host name	A character string of 1 to 256 characters
2	IP address		IP address (IPv4)	A character string in the format xxx.xxx.xxx.xxx xxx: A number from 0 to 255

The following example shows lines of code in the network connection control file:

Host-A

,192.168.1.2

Host-C,192.168.1.3

Format of the network control command configuration file

The following table describes the format of the network control command configuration file:

Section	Key	Value	Default value	Acceptable value
settings	host	The host name or IP address of a management server	Blank	A character string of 1 to 256 characters
	port	The connection port number on the management server	31080	A number from 2 to 49,151

Section	Key	Value	Default value	Acceptable value
settings	user	The ID of the JP1/IT Desktop Management 2 user who can execute the command	Blank	A character string of 1 to 64 characters
	pass	The password of the JP1/IT Desktop Management 2 user ID#	Blank	A character string of 1 to 32 characters
	sys	A property for the internal process of JP1/IT Desktop Management 2 (not editable)	Blank	None

#: When the command is executed and the user authentication succeeds on the management server, pass becomes empty. To set the password again, set a character string for pass.

The following example shows lines of code in the network control command configuration file:

[settings]

host=SERVER-A

port=31080

user=userA

pass=password01

sys=

Output format of the network control command message file

The following table describes the specifications of the network control command message file:

File name	Output folder	Number of retained files	Size
jdnrnetctrlC*n*.log (*n*:1 to 2)	*folder-containing-the-jdnrnetctrl-command* \log, or *JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\log	2	1 MB

The following shows the output format of the network control command message file:

date time process-ID message-ID message-text CRLF (end of line)

Notes

- Execute this command when the management server setup is completed and the management server is running.
- This command cannot be simultaneously executed by multiple users.
- A remote server cannot connect to a management server via a proxy server.
- You must note points listed below on the execution user specified with the command:
  - Notes when users are managed without using JP1/Base:
    - The user authentication fails if the command is executed with the initial password that was set when the user was created in the operation window of JP1/IT Desktop Management 2. You must execute the command with the new password that was reset when the user logged in to JP1/IT Desktop Management 2 for the first time.
    - The command can be executed even after the password expires.

        - When you change the password of the user, you must also edit the network control command configuration file to specify the new password.
    - Notes when users are managed using JP1/Base:
        - Set the linked directory server, taking care not to cause the password to expire.
        - When you change the password of the user, you must also edit the network control command configuration file to specify the new password.
- You must note the following points when configuring the command:
    - If you change the host name, IP address, or port number of the management server you want to interact with, reconfigure the network control command.
    - If you are executing the command in an environment other than that of the management server, set up the firewall and the communication environment so that the device can communicate with the management server by using the connection information set with the network control command.
- You must note the following point regarding the device information to be specified with the command:
    - In a DHCP environment, set a host name rather than IP address as the command argument that specifies the device to which to apply network access control.

Return value

The following table shows the return values of the `jdnrnetctrl` command:

Return value	Description
0	The command finished normally.
1	The command finished normally. However, an invalid line is found in the specified network connection control file.
11	The format for specifying the command arguments is invalid.
21	Failed to connect to the management server.
22	Authentication failed on the management server.
31	Another command (or another network control command) is being executed.
51	You do not have the permissions to execute this command.
150	The command execution failed.

Example

The following example shows how to configure this command when you want to execute the network control command on the management server set in C:\temp\jdnrnetctrl.ini and block the network access of the device whose host name is hostname001.

jdnrnetctrl -action deny -hostname hostname001 -settingfile C:\temp\jdnrnetctrl.ini

Collecting troubleshooting information

When you execute the network control command, you might encounter a problem with an unknown cause or unresolved issues. In this case, you need to collect troubleshooting information to make inquiries to the support service. If you have executed the network control command in an environment other than that of the management server, you need to collect troubleshooting information from both the management server and the environment (computer) in which you have executed the command.

The procedure below describes how to collect troubleshooting information from the environment (computer) in which you have executed the command. You must have Administrator permission to carry out this procedure.

1. Open the command prompt and move to the folder in which the network control command is stored.
2. Create a troubleshoot folder, and then move to the created folder.
   mkdir troubleshoot
   cd troubleshoot
3. Execute the commands for collecting troubleshooting information.
   Execute the commands shown below. If a system information dialog box appears, do not click the Cancel button. Instead, wait until the dialog box closes.
   systeminfo > systeminfo.txt
   netstat -a > netstat_a.txt
   netstat -nr > netstat_nr.txt
   netstat -no > netstat_no.txt
   ipconfig -all > ipconfig.txt
   wevtutil qe Application /f:text /rd:true > event.txt
   wevtutil qe Security /f:text /rd:true >> event.txt
   wevtutil qe System /f:text /rd:true >> event.txt
   tasklist /V > tasklist.txt
   sc query > service.txt
   msinfo32.exe /report msinfo32.txt
4. Close the command prompt.

You will find the folders shown below under the folder in which the network control command is stored. These folders contain troubleshooting information. After making inquiries to the support service, delete the troubleshoot folder.

- troubleshoot
- log

To collect troubleshooting information from the management server, execute the getlogs command.

If you have executed the network control command stored in the JP1/IT Desktop Management 2-installation-folder\mgr\bin folder on the management server, information collected by the getlogs command contains troubleshooting information for the command as well. On the other hand, if you have executed a network control command that is stored in a location other than the JP1/IT Desktop Management 2-installation-folder\mgr\bin folder, collect also the log folder located under the folder in which the network control command is stored as the troubleshooting information.

Related Topics:

- 17.1 Executing commands

17.41 setsecpolicy.vbs (applying a security policy to the offline-managed computer and collecting device information)

Functionality

This command applies a security policy to the offline-managed computer and collects device information.

The following are the pre-requisitions for this command:

- The services on the agent are already started.
- The agent version is 11-51 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

```
setsecpolicy.vbs[ /silent][ /u][ /s]
```

Arguments

/silent
: Prevents displaying the view from an end-user's computer.

/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.

Storage location

Same storage location as the tool for applying policy offline (where the tool is extracted to).

Notes

- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with the command to collect information of the offline-managed computer.
- In the following cases, you need to re-create the tool for applying policy offline, and then re-execute this command to apply the security policy and collect the device information. For details about the conditions where the command must be re-executed, see *A.11 Conditions where the tools must be re-executed on an offline-managed computer*.
  - If the anti-virus product that is judged by the security policy is changed
  - If the configuration of the additional management fields are modified
  - If the content of the security policy is modified#

#: Except for Operations Logs, Common settings for prohibited operations and operation logs, Collect List of USB Device Files, and Action Items.

Return values

The following table shows the return values of the `setsecpolicy.vbs` command.

Return value	Description
0	The command finished normally.
10001	The process of applying the security policy 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.
10035	The security policy application command is already being executed.
10051	The process was aborted due to the path to the storage folder being too long.
10052	The security policy application command is not installed on the local disk.
10101	Failed to apply the security policy.
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 applying the security policy to the offline-managed computer.
10105	The tool for applying policy offline might be corrupted.
10106	The agent environment is corrupted.

Example

The following example shows use of this command to apply the security policy and collect information without displaying the **End User Form** view on the end-user's computer.

setsecpolicy.vbs /u

17.42 deletelicense (delete licenses)

Functionality

This command deletes all product licenses registered in JP1/IT Desktop Management 2.

This command is used when moving license registered on the management server to another management server.

Execute this command on the management server.

Format

```
deletelicenseΔ-passwordΔ5yYdRhx7
```

Arguments

-passwordΔ5yYdRhx7
: This is the argument for executing this command. You need to specify this argument.

Storage location

JP1/IT Desktop Management 2installation-destination-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided byJP1/IT Desktop Management 2.

Notes

- Execute this command when the management server setup is completed and the management server is stopped.
- This command cannot be executed simultaneously with any of the commands.

Return values

The following table lists the return values of the `deletelicense` command.

Return value	Description
0	The command finished normally.
0	The command cannot be executed because no license exists.
11	The specified format for the argument is incorrect.
22	The management server has not been stopped.
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.
111	An attempt to delete product licenses failed.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command.

deletelicense -password 5yYdRhx7

Related Topics:

- 17.1 Executing commands

17.43 upldoplog (uploading operation logs)

Functionality

This command uploads to the management server the agents' operation logs that have not been uploaded yet.

Execute this command on a computer on which the agent is already installed.

Format

```
upldoplogΔ/upload[Δ/timeoutΔtimeout-period]
```

Argument

/upload
: Always specify this argument. If this argument is omitted, the command cannot be executed.

/timeoutΔ*timeout-period*
: Specify a timeout period for the command in seconds. You can specify a value in the range from 10 to 3,600 seconds. If you omit this argument, 60 is specified.

Storage location

agent-installation-folder\bin\

Notes

- You have to execute this command while the operation log service (`JP1_ITDM2_Agent Remote Control`) is up and running.
- This command cannot be simultaneously executed by multiple users.

Return value

The following table shows the return values of the `upldoplog` command.

Return value	Description
0	The command finished normally.
11	The specified format for the argument is incorrect.
31	Another command is being executed.
53	The operation log service is not up and running.
101	An attempt to upload operation logs failed.

Example

The following example shows use of this command to upload operation logs with the timeout period set to `120`.

upldoplog /upload /timeout 120

Related Topics:

- 17.1 Executing commands

17.44 prepagt.bat (generalizing an agent)

This section describes the `prepagt.bat` command that is used to generalize an agent by deleting program-specific information from it.

Functionality

When you install an agent on a computer, program-specific information regarding the agent is retained in a temporary file or other similar location inside the agent.

In the case of a shared VDI, virtual computers are created from the master image. When you install an agent on a virtual computer to create a master image, you have to first generalize the agent by deleting program-specific information from it. You can generalize the agent by executing the `prepagt.bat` command on the virtual computer that is used for creating the master image.

Important

- This command works only with Windows agents. It does not work with UNIX agents or Mac agents.
- This command does not work with agents on the relay system or the management relay server.

Execute this command on a computer on which the agent is already installed.

Format

```
prepagt.bat△/prep[△/password:password]
```

Argument

/prep

Always specify this argument. If this argument is omitted, the command cannot be executed.

/password:*password*

If you have set a password in **Settings to Protect Agents**, specify the set password. If you have not set a password in **Settings to Protect Agents**, do not specify this argument.

Storage location

agent-installation-folder\bin\

Notes

This command cannot be simultaneously executed by multiple users.

Return value

The following table shows the return values of the `prepagt.bat` command.

Return value	Description
0	The command finished normally.
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.

Return value	Description
101	An attempt to generalize the agent failed.

Example

The following example shows use of this command to generalize the agent for which `Password1234` is set as a password in **Settings to Protect Agents**.

```
prepagt.bat /prep /password:Password1234
```

Related Topics:

- 17.1 Executing commands

17.45 deletepackage (deleting packages)

Functionality

This command deletes unnecessary packages registered in management servers.

By periodically executing this command, you can prevent increase in the number of unnecessary packages.

Packages that matches all of the following conditions is determined as not in use, and is deleted. If there are no packages to be deleted, the command terminates normally.

- Update packages added in the support information file (update program information)
  The update packages added by the user are not included.
- Update packages that are excluded in the support information file (update information)
- There are no tasks associated with the package.

Format

```
deletepackage
```

Arguments

None.

Storage location

JP1/IT Desktop Management 2-installation-destination-folder\mgr\bin\

You can execute this command without specifying the storage location for the executable file, by using the command prompt provided byJP1/IT Desktop Management 2.

Notes

- Execute this command when the management 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 exportassetassoc
  - ioutils exportdevice
  - ioutils exportdevicedetail
  - ioutils exportfield
  - ioutils exportfilter
  - ioutils exportoplog
  - ioutils exportpolicy

- ioutils exporttemplate
- ioutils exportupdategroup
- ioutils exportupdatelist
- ioutils importasset
- ioutils importassetassoc
- ioutils importexlog
- ioutils importfield
- ioutils importfilter
- ioutils importpolicy
- ioutils importtemplate
- ioutils importupdategroup
- ioutils importupdatelist
- startservice
- stopservice
- updatesupportinfo
- deletenwgroup
- distributelicense

- When executing this command at first, the large number of network groups to delete is expected, so please execute according to the following procedure:

  1. Stop the following services:
     - JP1_ITDM2_Agent Control
     - JP1_ITDM2_Service
     - JP1_ITDM2_Web Container
     - JP1_ITDM2_Web Server
     - JP1_ITDM2_Relay Manager Service#
  2. Execute the `deletepackage` command.
  3. After command execution completed, start the following services:
     - JP1_ITDM2_Agent Control
     - JP1_ITDM2_Service
     - JP1_ITDM2_Web Container
     - JP1_ITDM2_Web Server
     - JP1_ITDM2_Relay Manager Service#

  #: In case of the management server in a single-server configuration, stopping or starting of this service is not required.

Return values

The following table lists the return values of the `deletepackage` command.

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
53	Services on the management server have not started.
54	The management server has not been set up.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to delete unnecessary packages. deletepackage.

deletepackage

Related Topics:

- 17.1 Executing commands

17.46 softwaresearch (searching for software installed in an agent device)

This section describes the `softwaresearch` command that is used to search for software installed in a device with a Windows agent installed.

Functionality

The command can be used to search for software installed in the device with the Windows agent at any time. The search of software is done according to the conditions defined in the software search conditions file. If the software search conditions file does not exist, the command will not search for software even when executed. Place the software search conditions file in the installation path of the agent before executing the command.

You can view the information of software found by this command in the **Software List** view and **Installed Software** tab of the Inventory module, or in the **Managed Software** view of the Assets module.

Execute this command with administrator privileges.

Up to 64 pieces of software can be discovered using this command. Up to the 64th piece of software detected under the search conditions is searched. However, for search conditions that are not searched, the command terminates without executing the software search.

> **Important**
>
> Even if more than 64 pieces of software information are detected by the command, no notification will be made for software information that is the same as that in **Add/Remove Software** or the software information obtained by software search.
>
> As overlapping software information is removed from the software information managed on the **Software List** view and **Installed Software** tab of the Inventory module as well as the **Managed Software** view of the Assets module, the window display may be for up to 64 hits.

Format

```
softwaresearch△[/START]
```

Arguments

/START
Specify it when you perform software search. If you omit it, software search will not be performed.

Storage location

agent-installation-folder\bin\

Notes

- The software search conditions file must be placed in the installation path of JP1/IT Desktop Management 2 - Agent.
- If the information of software found is the same as that in **Add/Remove Software** or the software information obtained by software search, no notification will be made.
- If you cannot view the software information correctly, take the following actions:
  - Check if the software search conditions file contains correct information.
  - Check if an error message has been logged in the publishing log (`SWSEARCH.log`).

The publishing log file (SWSEARCH.log) is stored in:
JP1/IT Desktop Management 2 - Agent-installation-folder\log

- This command cannot be executed simultaneously with any of the commands.

Return values

The following table lists the return values of the `softwaresearch` command.

Return value	Description	System action	Operator action
0	The command started.	--	--
0	The command finished normally.	--	--
1	The number of software information hits detected by the command exceeded the upper limit (64).	Search will halt.	Review and revise the definition and then re-execute the command.
11	The specified argument is incorrect. `Usage: softwaresearch /START /START Specify the argument when you perform software search.`	No search is performed.	Correct the argument and then re-execute the command.
21	The software search conditions file does not exist.	No search is performed.	Place the file and then re-execute the command.
22	An incorrect definition was found in the software search conditions file.	No search is performed.	Review and revise the definition and then re-execute the command.
24	The software search conditions file is inaccessible.	No search is performed.	Check the access permissions of the file, change them to those allowing access, and then re-execute the command.
25	The search conditions defined in the software search conditions file exceed the upper limit (500 rows).	No search is performed.	Set the search conditions to within 500 rows and then re-execute the command.
31	The command is already being executed.	No search is performed.	Check if this command is running elsewhere, and if not, re-execute the command.
32	You do not have permissions to execute the command.	No search is performed.	Re-execute the command with administrator privileges.
150	The command execution was interrupted due to some other error.	Search will halt.	Collect data by using the `getlogs` command, and then contact the system administrator.

Example

The following example shows how to use the command when you perform software search.

softwaresearch /START

Related Topics:

- 17.1 Executing commands

17.46.1 Format of the software search conditions file

The file defines the conditions when you search for software information using the `softwaresearch` command. Created by the administrator, it is placed under the folder for the agent that performs software search.

The following table lists and describes the specifications of the software search conditions file:

Item	Description
File name	`softwaresearch.csv`
File format	Each items separated by comma (,)
Character code	UTF-8 (without BOM)
Storage location	*agent-installation-folder*\conf\

The following table lists and describes what items are in the software search conditions file. All the items are required.

Item	Description	Format
Software name	The name of the software program that is notified of as installed software information	Any character string from 1 to 512 characters
Search file name	The name of the file to be searched for	• A character string of up to 255 characters • A regular expression is available in the file name. Add a wildcard character (*) just before the extension.# • The following symbols cannot be used: \, /, :, ?, ", <, >, |
Search path	The name of the path to be searched	• Specify the absolute path from 2 to 259 characters (including the drive letter). • The following symbols cannot be used: ", *, /, <, >, ?, | • A network drive cannot be used.

#: The wildcard character can be used as follows:

- It can be placed at the end of the file name (excluding the extension), but cannot at the beginning of the character string or in the middle of the file name.
- It is not available in the file extension.
- You can use it only once in the file name, but cannot twice or more.

Coding example of the software search conditions file

```
Softname001,soft*.exe, C:\Program Files (x86)
Softname001,soft*.exe, C:\Windows
Softname002,a*.exe, C:\Program Files
Softname003,soft.exe, C:\Program Files
```

Notes when creating the software search conditions file

- If you specify only a drive letter, all files in that drive will be a search target. The device will then be under high load during the search. We recommend that you specify a path taking the load into account.
- If the total number of characters in the search path and file name defined is more than 259 characters, no software search is performed. In addition, when the wildcard character is used in the name of the file to be searched for, no search is performed if the name of the found software, including its search path, is more than 259 characters.
- Multiple software search conditions can be specified, with one condition in one row. The condition in each row must have all the items specified. If a required item is missing or if the defined data is in invalid format, an error occurs causing no search to be performed.
- Specify the name of an executable to be searched for in the software search conditions file.
- The maximum number of rows that can be defined in the software search conditions file is 500.

Related Topics:

- 17.1 Executing commands

18 Troubleshooting

This section describes the actions to be taken when a problem occurs in JP1/IT Desktop Management 2.

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

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 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 2.

FPH
   Indicates that the message is a database-related message from JP1/IT Desktop Management 2.

nnnn
   Indicates the serial number of the message. Serial numbers for database-related messages from JP1/IT Desktop Management 2are 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 Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2, or Windows Vista, check whether User Account Control (UAC) is enabled. If UAC is enabled, use a built-in user that has Administrator permission. Alternatively, 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 tools fail

If notification of device information which was collected with the the Information Collection Tool or the tool for applying policy offline 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 Divisioner
r,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:

- 17.36 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 2 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 Management 2uses, and to take action when this space runs low.

You can check the free space on the disk that JP1/IT Desktop Management 2uses 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.

Important

When a failover occurs during a cluster system operation, the status and result of an import are not displayed in the following windows. In this case, import items again.

- **Home - Background Task**
- **Settings - Assets - Last Import Log**

18.9 Troubleshooting problems on the management server

When an error occurs, a message will appear in the JP1/IT Desktop Management 2view. 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_ITDM2_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	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

Event number	Type	Message	Cause	Actions to be taken
055	Error	Failed to send an e-mail notification to the System Administrator.	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.	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 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_ITDM2_Service). The operation (JP1_ITDM2_Service) will be stopped.	A critical internal error occurred in the service (JP1_ITDM2_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 Inventory 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 Inventory 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 (ITDM-compatible) module, check the execution result of the task

Event number	Type	Message	Cause	Actions to be taken
1017	Distribution	Prohibited software will be deleted.	It was detected that unauthorized software is installed.	An Auto Enforce will be performed. In the Distribution (ITDM-compatible) module, check the execution result of the task
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 (ITDM-compatible) 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	Error	An error occurred during the processing to store operation 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

Event number	Type	Message	Cause	Actions to be taken
1032	Error	An error occurred during the processing to store operation 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.	move the operation log backup folder to a disk that has sufficient free space.
1034	Error	An error occurred during the processing to acquire operation logs manually.	• 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. • Cause 6 There are no backup files in the operation log backup folder. • Cause 7 The backup file in the operation log backup folder is corrupted.	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. • For Cause 6 If the backup files were moved to another folder, copy them to the operation log backup folder, and

Event number	Type	Message	Cause	Actions to be taken
1034	Error	An error occurred during the processing to acquire operation logs manually.	• 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. • Cause 6 There are no backup files in the operation log backup folder. • Cause 7 The backup file in the operation log backup folder is corrupted.	then restore the operation logs again. • For Cause 7 Delete the file displayed in the detailed information of the operation log backup folder.
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. • Cause 3 The specified domain cannot be found. • Cause 4 The OU information that is specified on the Active Directory server cannot be found.	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 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

Event number	Type	Message	Cause	Actions to be taken
1037	Error	Failed to retrieve inventory and organizational information from Active Directory Server.	• Cause 5 Encrypted communication with the Active Directory server has failed.	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.	An error occurred while connecting to the Product Update server.	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 **Product Update** 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 The administrator does not have an email address set, or the administrator's email address is invalid. • Cause 2	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
1056	Error	Failed to notify System Administrators by e-mail.	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.	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.
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	Select and take the appropriate actions from the list below: • Cause 1

Event number	Type	Message	Cause	Actions to be taken
1076	Security	The Operations log was deleted.	The agent was unable to connect to the management server for a long time.	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.
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.

Event number	Type	Message	Cause	Actions to be taken
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_ITDM2_DB Service) might not have started.	Start the database service (JP1_ITDM2_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. • 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	Select and take the appropriate actions from the list below: • For Cause 1 Uninstall the product that cannot coexist with the site server

Event number	Type	Message	Cause	Actions to be taken
1106	Error	Installation of the site server program failed.	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.	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.
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	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

Event number	Type	Message	Cause	Actions to be taken
1108	Error	Failed to synchronize device information with MDM (*product-name*).	An error occurred while obtaining the settings information of the MDM server.	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 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.	Select and take the appropriate actions from the list below: • For Cause 1

Event number	Type	Message	Cause	Actions to be taken
1113	Error	Failed to reset the password of a smart device.	• 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.	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.
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

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.	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 An error occurred while settings information of the MDM server was being obtained. • Cause 7 The server certificate of the MDM server is invalid.	• 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 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

Event number	Type	Message	Cause	Actions to be taken
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 An error occurred while settings information of the MDM server was being obtained. • Cause 7 The server certificate of the MDM server is invalid.	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.

Event number	Type	Message	Cause	Actions to be taken
1138	Error	An error occurred during the processing to export operation logs periodically.	• 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.
1139	Error	An error occurred during the processing to acquire operation logs automatically.	• 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

Event number	Type	Message	Cause	Actions to be taken
1139	Error	An error occurred during the processing to acquire operation logs automatically.	• 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.	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.
1140	Error	An error occurred during the processing to update the date information of operation 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.
1144	Assets	Failed to register the USB device.	The serial number is the same as that of a registered USB device.	To ensure unique serialnumbers, change the serialnumber of the USB device to be registered to the device instance ID, and then register the USB device again. To change the

Event number	Type	Message	Cause	Actions to be taken
1144	Assets	Failed to register the USB device.	The serial number is the same as that of a registered USB device.	serialnumber to the device instance ID, in the **Advanced** dialog box that is displayed from the **Register USB Device** dialog box, enter the device instance ID in **Registration condition for device instance ID**.

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 2-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 2.
	JP1/IT Desktop Management 2-installation-destination-folder\mgr\log	JDNSTRC*n*.log# (*n* = 1 to 9)	Outputs information that you can use to check the change results of configuration of JP1/IT Desktop Management 2.
Event logs	Operating system event log	--	Outputs information on the startup of, the shutdown of, and critical errors generated byJP1/IT Desktop Management 2. 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 17.30 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 2 - Agent was deployed, please check the Events module.

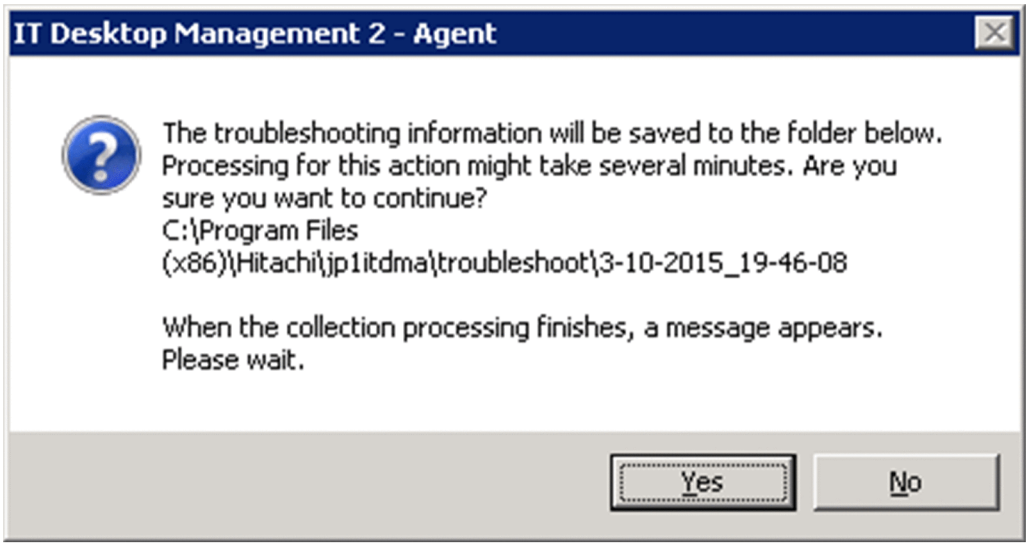
To obtain troubleshooting information for an agent:

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 or the tool for applying policy offline.

1. Double click `getlogs.vbs`.

   A dialog box confirming that you want to obtain troubleshooting information is displayed.

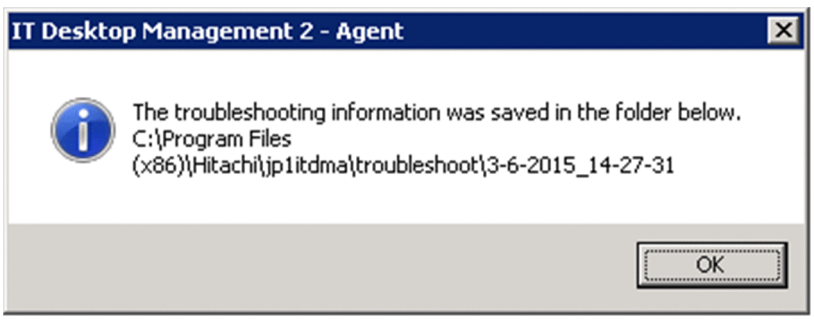


   The location of `getlogs.vbs` is as follows:

   JP1/IT-Desktop-Management-2-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-2-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 2-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. Registry entries that are located under HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices. • Device information Properties and status of the device. • File information A list of sub-folders and files that are located under *JP1/IT Desktop Management 2-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 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 or Windows Server 2008 R2 does not start after installing the Agent

If another company's remote control product is already installed, Windows 7 or Windows Server 2008 R2 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.

18.12 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 Inventory 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, on a computer that has the network monitor enabled, open the Windows **Control Panel**, select **Administrative Tools**, double-click **Services**, and then stop the service JP1_ITDM2_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

18.13 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 2 might be in conflict. Because JP1/IT Desktop Management 2 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.

18.14 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.

18.15 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 2 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.

18.16 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 2 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:

- 17.28 stopservice (stopping services)
- 17.29 startservice (starting services)

18.17 Troubleshooting problems with the Internet gateway

This section describes what actions to take for problems that occur with an Internet gateway.

To obtain troubleshooting information for an Internet gateway:

To collect troubleshooting information, execute the `getlogs.vbs` command on the computer on which the problem has occurred. For details, see 18.10 Troubleshooting problems with agents.

And, collect folders and files of the following table:

Folders and Files	Contents
Log folder of the Internet gateway	*Internet-gateway-installation-folder*\log
Log folder of the Microsoft Internet Information Services	%SystemDrive%\inetpub\logs\LogFiles (Default)
Configuration file of Microsoft Internet Information Services	%windir%\System32\inetsrv\config\ApplicationHost.config (Default)

In addition, check Microsoft Internet Information Services to confirm if any event log indicating an error has been output.

The following table describes the log files that are output when an error occurs:

Log type	Output destination	File name	Description
Message log file	*Internet-gateway-installation-folder*\log	JDNGWMAIN*nn*.log[#] (*nn* = 01 to 05)	Information that allows you to check the operating status of the Internet gateway is output.

An agent cannot connect to the Internet gateway

When an agent cannot connect to the Internet gateway, refer to the agent's log file to check the connection status.

The following information is output to a log file:

```
KDSF0350-I Connect to internet gateway. URL=URL-of-Internet-gateway
KDSF0351-I Connect result=connection-result
KDSF0352-I HTTP response code=HTTP-response-code
```

Take appropriate action based on the output *connection-result* and *HTTP-response-code*.

The following table describes information displayed for *connection-result* as well as the causes of the error and the corrective action.

Connection result	Causes of the error and corrective action
SUCCESS	A connection was successfully established.
ERROR_INTERNET	One of the following causes is likely, which can be solved by the corrective action described below. [Cause] • The server cannot interpret requests. • A server certificate has not been installed.

Connection result	Causes of the error and corrective action
ERROR_INTERNET	[Corrective action] • Review the host set with **Host Name or IP address** and the port set with **Port Number** which you can set by opening the Agent Configurations view of the Settings module, and under **Basic settings**, selecting **Internet Connection Settings**, and then **Internet Gateway**. • Install a server certificate on the Internet gateway.
ERROR_INTERNET_MIXED_SECURITY	[Cause] The issuer of the server certificate cannot be trusted. [Corrective action] Install client certificates (a root certificate, an intermediate certificate, and a cross root certificate) on the managed computer, which are necessary to trust the server certificate installed on the Internet gateway.
ERROR_INTERNET_SEC_CERT_DATE_INVALID	[Cause] The certificate has expired. [Corrective action] Install a valid server certificate and client certificates.
ERROR_INTERNET_SEC_CERT_CN_INVALID	[Cause] The domain name of the URL does not match the host name of the Internet gateway. [Corrective action] Install the server certificate on the server (Internet gateway server) that has the common name specified when a request for a server certificate was made, and specify the common name to the Connection-destination settings of the Internet gateway.

The following table describes information displayed for *HTTP-response-code* as well as the causes of the error and the corrective action.

HTTP response code	Connection status	Error cause	Corrective action
200	S	Ended in success.	Not applicable.
400	F	The server cannot interpret requests.	Check the server and the port number at the connection destination.
401	F	The user authentication failed.	Check the authentication user ID and password for the Internet gateway. Alternatively, check the connection destination.
403	F	Access was denied.	Check the authority of the authentication user. Alternatively, check the connection destination.
404	F	The request was not accepted.	Check the connection destination.
405	F		
406	F		
407	F	The proxy authentication failed.	Check the user and password for the proxy server. Alternatively, check the host name and port number of the proxy server.
408	F	A timeout occurred.	Establish a connection again. If the problem persists, collect troubleshooting information by executing a command for collecting troubleshooting information, and then contact Support Service.
409	F	The connection failed due to a temporary failure.	
410	F	Information was not found.	

HTTP response code	Connection status	Error cause	Corrective action
411	F	The request was denied due to an invalid sequence.	Establish a connection again. If the problem persists, collect troubleshooting information by executing a command for collecting troubleshooting information, and then contact Support Service.
412	F	The request was invalid and therefore denied.	
413	F		
414	F		
415	F		
500	F	Processing was discontinued due to an internal error that occurred on the server.	
501	F		
502	F		
503	F		
504	F		
505	F		
Other than the above	F		

Legend: S: Connection successful, F: Connection failed

18.18 Actions to be taken when a search target cannot be found with the softwaresearch command

To see if the `softwaresearch` command is executed successfully when the administrator ran it on the agent, check whether the software information of the search target is displayed in the following:

- **Software List** view of the Inventory module
- **Installed Software** tab
- **Managed Software** view of the Assets module

No discovery of the search target software even after the `softwaresearch` command is executed means that the software does not exist. If you cannot find software information in spite of no problem with the software information on the device, try the following steps:

1. Review the search conditions. Review the contents of the software search conditions file used by the `softwaresearch` command.

2. If you find the search conditions file correct in step 1, the device might be experiencing a problem. Use the file collection function to obtain the publishing logs of the software search command. Check the publishing logs you obtained for any error messages. If you see an error message, follow the response to the error in the error message to handle the error, and then retry the software search command. If you see the KDEX7009-E message, execute the log collection (`getlogs`) command on the device and then contact the support service.

   The storage location and file name of the publishing log file are as follows:

   - Location: *JP1/IT Desktop Management 2 - Agent-installation-path*`\log`
   - File name: `SWSEARCH.log`

Related Topics:

- 17.1 Executing commands

19 Events

This chapter lists and describes the JP1/IT Desktop Management 2 events.

19.1 List of events

Event number	Severity	Type	Event
0	Information	Settings	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	Settings	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	Settings	The status of the device has been changed to Ignored.
3	Information	Settings	The device has been deleted.
4	Warning	Settings	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	Type	Event
4	Warning	Settings	• Unknown • (User definition)
5	Warning	Settings	The agent has been uninstalled. Confirm if agent uninstallation (from the computer) is allowed.
6	Information	Settings	The agent settings have been updated. Agent setting name=*agent-configuration-name*
7	Information	Inventory	Memory capacity has been changed. Before change=*memory-capacity* After change=*memory-capacity*
8	Information	Inventory	Hardware has been added. Interface type=*interface-type* Model name=*model-name* Capacity=*capacity*
9	Information	Inventory	Hardware has been deleted. Interface type=*interface-type* Model name=*model-name* Capacity=*capacity*
19	Warning	Error	Failed to obtain detailed information from *function-name*. Confirm the settings (authentication information, discovery range) and the operational status of the service (JP1_ITDM2_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	Settings	The agent installer has been launched. Model name=*model-name* Version=*version* IP address=*IP-address*
56	Information	Security	Message notification to the user has been sent.
57	Warning	Error	Failed to send a message notification to the user. Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
58	Information	Security	Connection to the network has been denied.

Event number	Severity	Type	Event
60	Information	Security	Network connection has been allowed.
62	Information	Security	Antivirus software settings have been changed. Product name=*product-name* Engine version=*engine-version* File definition version=*file-definition-version*
63	Information	Security	Update information has been added. Update information=*update-information*
69	Information	Security	Security policy has been added. Security policy name=*security-policy-name*
70	Information	Security	Security policy content has been updated. Security policy name=*security-policy-name*
71	Information	Security	Security policy has been deleted. Security policy name=*security-policy-name*
72	Information	Security	Security policy assignment has been changed. Security policy name=*security-policy-name* Assigned group=*assigned-group*
75	Information	Security	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	Security	Printing operation has been blocked. Account login=*account-login* Printer name=*printer-name* Printing job name=*printing-job-name*
77	Information	Security	Printing operation has been unblocked. Account login=*account-login*
78	Warning	Error	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	Error	An error occurred in the operation (JP1_ITDM2_Service). The operation (JP1_ITDM2_Service) will be stopped. Collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service. ErrCode=*error-code*
208	Warning	Error	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	Error	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*

Event number	Severity	Type	Event
209	Warning	Error	The following is displayed for *function-name*. • Device Discovery • Inventory Collection • On-demand inventory collection • Agent Deployment
210	Warning	Error	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. If the error is repeated, then collect troubleshooting information (launch [Command] and execute getlogs command), and contact Support Service.
211	Warning	Error	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	Error	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	Settings	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	Inventory	New software has been discovered. Software name=*software-name* Version=*version*
1006	Warning	Error	Failed to stop the prohibited operation. Service name=*service-name*
1007	Information	Security	Antivirus software information has been added.
1008	Information	Settings	Agent patch has been updated. Agent version=*agent-version*
1009	Information	Settings	Action definition file (manager) has been updated.
1011	Information	Security	A device used to suppress operation was disconnected. Logon account name = *logon-account-name* Drive name = *drive-name* Drive type = *drive-type* Device name = *device-name* Device instance ID = *device-instance-ID* Device category = *device-category* The following is displayed for *drive-type*: • Unknown • Local Disk

Event number	Severity	Type	Event
1011	Information	Security	• Network Drive • Removable Disk • CD-ROM Drive • RAM Disk The following is displayed for *device-category*: • Unknown • USB device • Internal CD or DVD drive • Internal floppy disk drive • IEEE1394 device • Internal SD card • Bluetooth device • Imaging device • Windows portable device
1016	Information	Distribution (ITDM-compatible)	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	Distribution (ITDM-compatible)	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	Distribution (ITDM-compatible)	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* 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. • Cannot unzip package. • Failed to start the command. • Command processing has stopped. • Execution command has terminated abnormally.
1019	Warning	Distribution (ITDM-compatible)	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	Distribution (ITDM-compatible)	Task *task-name* has been started according to the schedule. Task *task-name* has been started at its scheduled starting time *scheduled-starting-time*.

Event number	Severity	Type	Event
1021	Information	Distribution (ITDM-compatible)	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	Assets	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	Settings	IP Discovery is complete.
1029	Information	Settings	Active Directory synchronization is complete.
1032#	Warning	Error	An error occurred during the processing to store operation logs. *cause-of-error* The following is displayed for *cause-of-error*: • An internal error occurred. If this error occurs repeatedly, contact the support service. • An I/O error occurred in a data folder or local data folder. Check whether the data folder or the local folder is accessible and whether the disk space is sufficient. • An error occurred while connecting to operation log backup folder (specified during Setup). Check whether the backup destination folder exists, and then re-establish the connection. • Authentication to operation log backup folder (specified during Setup) has failed. Check the Username and Password (specified during Setup), and then re-establish the connection. • An I/O error occurred while connecting to operation log backup folder (specified during Setup). Make sure that the operation log backup folder is accessible, and the hard disk space is sufficient. • Backup files do not exist in operation log backup folder (specified during Setup). If the backup files have been moved to any other folder, then restore the files. Else you can remove the backup files and the improper catalog file, and then try operation log restoration. • Check whether the operation log backup folder was specified during Setup. • Connection to the operation log backup folder could not be established, because the anonymous access to shared folders is restricted on the management server. Create a user account in management server by using the Username and Password specified during Setup.
1033	Information	Security	The processing to manually acquire operation logs ended. The range manually acquired: *start-date-and-time-end-date-and-time*

Event number	Severity	Type	Event
1034	Warning	Error	An error occurred during the processing to acquired operation logs manually. *cause-of-error* Detailed information =*detailed-information* The following is displayed for *cause-of-error*: • An internal error has occurred. If this error occurs repeatedly, contact the support service. • An I/O error occurred in a data folder or local data folder. Check whether the data folder or the local folder is accessible and whether the disk space is sufficient. • An error occurred while connecting to operation log backup folder (specified during Setup). Check whether the backup destination folder exists, and then re-establish the connection. • Authentication to operation log backup folder (specified during Setup) has failed. Check the Username and Password (specified during Setup), and then re-establish the connection. • An I/O error occurred while connecting to operation log backup folder (specified during Setup). Make sure that the operation log backup folder is accessible, and the hard disk space is sufficient. • Backup files do not exist in operation log backup folder (specified during Setup). If the backup files have been moved to any other folder, then restore the files. Else you can remove the backup files and the improper catalog file, and then try operation log restoration. • Check whether the operation log backup folder was specified during Setup. • Connection to the operation log backup folder could not be established, because the anonymous access to shared folders is restricted on the management server. Create a user account in management server by using the Username and Password specified during Setup. • The operation log file cannot be imported to the database because the operation log files displayed in the detailed information are corrupt. Delete the operation log files displayed in the detailed information. If the cause of the error is a file corruption, the file name is displayed for *detailed-information*.
1036#	Critical	Error	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	Error	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* For *cause*, the cause of the error is displayed depending on the situation.

Event number	Severity	Type	Event
1038	Information	Settings	Action definition file (agent) has been updated.
1039	Information	Distribution (ITDM-compatible)	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	Distribution (ITDM-compatible)	Because the error occurred during a distribution task to update a program, the task was ended. *cause-of-error* The following is displayed for *cause-of-error*: Task name=*task-name* • The downloading Windows update file failed. • Windows Update File was not registered when you added Windows Update manually.
1048	Warning	Suspicious Operations	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	Suspicious Operations	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	Suspicious Operations	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	Suspicious Operations	Mass-Printing has been detected. Login account name=*login-account-name* Print pages=*print-pages*
1055#	Warning	Error	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. For *cause-of-error*, the cause of the error is displayed depending on the situation.
1056#	Critical	Error	Failed to notify System Administrators by e-mail. *cause-of-error* Please use Test Mode to check the SMTP server settings. For *cause-of-error*, the cause of the error is displayed depending on the situation.
1057#	Warning	Error	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	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.

Event number	Severity	Type	Event
1058#	Critical	Error	*FolderType* (*Specified folder*) Available disk space=*available disk space of the drive*
1059	Warning	Settings	The product license will expire soon. Expiration date: *expiration-date* Please purchase a new license key.
1060	Information	Inventory	Software has been added. Software=*software-name version*
1061	Information	Inventory	Software has been either deleted or the software retrieval condition was changed. Software=*software-name version*
1062	Information	Inventory	Software has been updated. Before change Software=*software-name version* After change Software=*software-name* Version=*version*
1063	Information	Security	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	Error	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	Error	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	Inventory	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 • Restriction of anonymous connections • Firewall settings • Automatic Updates • Remote desktop

Event number	Severity	Type	Event
1066	Information	Inventory	The following is displayed for *value*. • Disabled • Enabled • None • Exist • Unknown • Permit • Not permit
1067	Information	Inventory	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	Inventory	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	Inventory	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) The following is displayed for *value-before-change* and *value-after-change*. • Password Strength

Event number	Severity	Type	Event
1069	Information	Inventory	Compliant Not Compliant • Password Never Expires, Screensaver settings, Password (Screen Saver) Disabled Enabled • Startup Time (Screen Saver)
1070	Information	Security	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 Firewall • Enable Automatic Update • Disable Administrative Share • Disable DCOM • Disable Remote Desktop • Execute Automatic Update • Stop and Disable Windows services
1071	Warning	Error	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 Firewall • Enable Automatic Update • Disable Administrative Share • Disable DCOM • Disable Remote Desktop • Execute Automatic Update • Stop and Disable Windows services
1072	Warning	Error	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 Firewall • Enable Automatic Update • Execute Automatic Update • Disable Remote Desktop
1073	Information	Security	The start of a prohibited operation has been detected. Service name=*service-name*
1074	Information	Security	The completion of a prohibited operation has been detected.

Event number	Severity	Type	Event
1074	Information	Security	Service name=*service-name*
1076	Warning	Security	The Operations log was deleted. The operation log was discarded because the data that has exceeded the storage period was received. The date and time setting of the device might be incorrect.
1077	Information	Settings	The network access control is enabled. Network address=*network-address*
1078	Information	Settings	The network access control is disabled. Network address=*network-address*
1079#	Warning	Security	The device has been disconnected. MAC address=*MAC-address* IPaddress=*IP-address*
1081	Information	Security	The network access control has started.
1082#	Warning	Security	The network access control has stopped running.
1085	Warning	Settings	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	Settings	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	Assets	Asset information import is complete. The asset information was imported. Asset Type=Hardware Asset add=*number-of-information-items* update=*number-of-information-items* error=*number-of-information-items*
1088	Warning	Error	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	Error	AMT authentication failed. (AMT Settings) [AMT Settings] - [admin Password] to access the settings, please change the AMT credentials. http://*host-name*:16992
1090	Warning	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. Free disk space = *free-disk-space* MB

Event number	Severity	Type	Event
1091#	Critical	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. Free disk space =*free-disk-space* MB
1092	Warning	Error	Free space for the site server database has become scarce. % of database used = *database-usage*%
1093#	Critical	Error	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	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. Free disk space = *free-disk-space* MB
1095#	Critical	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. Free disk space = *free-disk-space* MB
1096	Information	Inventory	The site server has been installed.
1097	Information	Inventory	The site server has been uninstalled.
1098	Information	Inventory	The site server service has started.
1099	Information	Inventory	The site server service has stopped.
1100	Critical	Error	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	Error	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	Error	A database access error occurred on the site server. The database service (JP1_ITDM2_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	Error	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*

Event number	Severity	Type	Event
1105	Warning	Settings	Failed to enable network access control. *cause-of-error* network address = *network-address* For *cause-of-error*, the cause of the error is displayed depending on the situation.
1106	Critical	Error	Installation of the site server program failed. *cause-of-error* For *cause-of-error*, the cause of the error is displayed depending on the situation.
1110	Information	Inventory	A smart device was locked. MDM setting name = *MDM-setting-name*
1111	Warning	Error	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	Inventory	The password of a smart device was reset. MDM setting name = *MDM-setting-name*
1113	Warning	Error	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	Inventory	A smart device was initialized. MDM setting name = *MDM-setting-name*
1115	Warning	Error	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	Error	Failed to delete a smart device. A database access error might have occurred. In the settings window, select [Discover Devices] and [Managed Devices]. Then, select the devices that you want to delete, and delete them. (error code = *internal-error-code*)

Event number	Severity	Type	Event
1117	Information	Inventory	Synchronization of device information with the MDM system (*product-name*) is complete. MDM setting = *MDM-setting-name*
1118#	Warning	Error	Synchronization of device information with the MDM system (*product-name*) failed. cause = *cause* 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 *cause*, the cause of the error is displayed depending on the situation.
1120	Warning	Error	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*)
1122	Warning	Inventory	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	Error	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*)
1124	Information	Settings	Software dictionary information was updated.
1127	Critical	Security	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	Type	Event
1127	Critical	Security	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 • Firewall settings • Settings for automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
1128	Warning	Security	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	Type	Event
1128	Warning	Security	• Days since the password was updated • Automatic logon settings • Power-on password settings • Shared folder settings • Restriction of anonymous connections • Status of unnecessary services • Firewall settings • Settings for automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
1129	Information	Security	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 • Firewall settings • Settings for automatic updates • Screensaver password protect • Setting for waiting time until starting of Screensaver • Administrative shared folder settings • DCOM settings • Remote desktop settings
1130	Information	Inventory	Processing to collect the revision history started.
1131	Information	Inventory	Processing to collect the revision history is complete.

Event number	Severity	Type	Event
1132#	Warning	Error	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	Error	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	Security	A request to allow connections to the network was sent to JP1/NETM/NM - Manager.
1135#	Warning	Security	A request to reject connections to the network was sent to JP1/NETM/NM - Manager.
1136#	Warning	Error	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	Error	Failed to allow 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.
1138	Warning	Error	An error occurred during the processing to export operation logs periodically. *cause-of-error* The following is displayed for *cause-of-error*: • An internal error occurred. If this error occurs repeatedly, contact the support service. • An I/O error occurred in a data folder or local data folder. Check whether the data folder or the local folder is accessible and whether the disk space is sufficient. • An error occurred while connecting to operation log backup folder (specified during Setup). Check whether the backup destination folder exists, and then re-establish the connection. • Authentication to operation log backup folder (specified during Setup) has failed. Check the Username and Password (specified during Setup), and then re-establish the connection. • An I/O error occurred while connecting to operation log backup folder (specified during Setup). Make sure that the operation log backup folder is accessible, and the hard disk space is sufficient. • Backup files do not exist in operation log backup folder (specified during Setup). If the backup files have been moved to any other folder, then restore the files. Else you can remove the backup files

Event number	Severity	Type	Event
1138	Warning	Error	and the improper catalog file, and then try operation log restoration. • Check whether the operation log backup folder was specified during Setup. • Connection to the operation log backup folder could not be established, because the anonymous access to shared folders is restricted on the management server. Create a user account in management server by using the Username and Password specified during Setup.
1139	Warning	Error	An error occurred during automatic restoration of operation logs. *cause-of-error* The following is displayed for *cause-of-error*: • An internal error has occurred. If this error occurs repeatedly, contact the support service. • An I/O error occurred in a data folder or local data folder. Check whether the data folder or the local folder is accessible and whether the disk space is sufficient. • An error occurred while connecting to operation log backup folder (specified during Setup). Check whether the backup destination folder exists, and then re-establish the connection. • Authentication to operation log backup folder (specified during Setup) has failed. Check the Username and Password (specified during Setup), and then re-establish the connection. • An I/O error occurred while connecting to operation log backup folder (specified during Setup). Make sure that the operation log backup folder is accessible, and the hard disk space is sufficient. • Backup files do not exist in operation log backup folder (specified during Setup). If the backup files have been moved to any other folder, then restore the files. Else you can remove the backup files and the improper catalog file, and then try operation log restoration. • Check whether the operation log backup folder was specified during Setup. • Connection to the operation log backup folder could not be established, because the anonymous access to shared folders is restricted on the management server. Create a user account in management server by using the Username and Password specified during Setup.
1140	Warning	Error	An error occurred during the processing to update the date information of operation logs. *cause-of-error* The following is displayed for *cause-of-error*: • An internal error has occurred. If this error occurs repeatedly, contact the support service. • An I/O error occurred in a data folder or local data folder. Check whether the data folder or the local folder is accessible and whether the disk space is sufficient. • An error occurred while connecting to operation log backup folder (specified during Setup). Check whether the backup destination folder exists, and then re-establish the connection. • Authentication to operation log backup folder (specified during Setup) has failed. Check the Username and Password (specified during Setup), and then re-establish the connection. • An I/O error occurred while connecting to operation log backup folder (specified during Setup). Make sure that the operation log backup folder is accessible, and the hard disk space is sufficient.

Event number	Severity	Type	Event
1140	Warning	Error	• Backup files do not exist in operation log backup folder (specified during Setup). If the backup files have been moved to any other folder, then restore the files. Else you can remove the backup files and the improper catalog file, and then try operation log restoration. • Check whether the operation log backup folder was specified during Setup. • Connection to the operation log backup folder could not be established, because the anonymous access to shared folders is restricted on the management server. Create a user account in management server by using the Username and Password specified during Setup.
1141#	Warning	Error	Errors occurred during the processing to delete the operation logs that exceeded the storage period from the operation log database, and the processing to re-create the index information of the operation log database. Cause of error=*cause-of-error* The following is displayed for *cause-of-error*: • A temporary error occurred while data was being processed. If this error occurs repeatedly, contact the support service. • An I/O error occurred in a data folder or local data folder. Check whether the data folder or the local folder is accessible and whether the disk space is sufficient. If the disk does not have enough free space, increase the free disk space, or specify (during setup) a folder on a disk that has enough free space, and then restart the management server. • An error occurred while connecting to operation log backup folder (specified during Setup). Check whether the backup destination folder exists, and then reestablish the connection. • Authentication to operation log backup folder (specified during Setup) has failed. Check the Username and Password (specified during Setup), and then reestablish the connection. • An I/O error occurred while connecting to operation log backup folder (specified during Setup). Check whether the operation log backup folder is accessible, and the hard disk space is sufficient. • Backup files do not exist in operation log backup folder (specified during Setup). If the backup files has been moved to any other folder, then restore the files. Else you can remove the backup files and the improper catalog file, and then try operation log restoration. • Check whether the operation log backup folder was specified during Setup. • Connection to the operation log backup folder could not be established, because the anonymous access to shared folders is restricted on the management server. Create a user account in management server by using the Username and Password specified during Setup. • The operation log file cannot be imported to the database because the operation log files displayed in the detailed information are corrupt. Delete the operation log files displayed in the detailed information. • An error occurred in the operation log database. The free disk space might have become insufficient when the database was being expanded. In the settings window, reconfigure the server, and then restore the database by using the database manager. • The total number of dates of automatically-acquired operation logs and dates of manually-acquired operation logs exceeded the maximum value that can be specified for the number of dates to be stored in the operation log database. In the Operations Log List

Event number	Severity	Type	Event
1141#	Warning	Error	in the security window, delete any unnecessary operation logs that were manually acquired. • An error occurred in the operation log database. Use Setup to rebuild the server, then use Database Manager to restore the database.
1142	Information	Security	The deletion of the operation logs that exceeded the storage period from the operation log database, and the recreation of the index information of the operation log database started.
1143	Information	Security	The deletion of the operation logs that exceeded the storage period from the operation log database, and the recreation of the index information of the operation log database finished.
1144	Warning	Assets	Failed to register the USB device. The serial number is the same as that of a registered USB device. To ensure unique serial numbers, change the serial number of the USB device to be registered to the device instance ID, and then register the USB device again. To change the serial number to the device instance ID, in the **Advanced** dialog box that is displayed from the **Register USB Device** dialog box, enter the device instance ID in **Registration condition for device instance ID**. Serial number = *serial-number* Device name = *device-name* Device instance ID = *device-instance-ID*
1145	Information	Relay	Processing to send information to a lower management server has started.
1146	Information	Relay	Information sent to a lower management server was correctly applied.
1148	Information	Relay	Information sent from a higher management server was applied to a local server.
1149#	Warning	Error	An error occurred while information was being sent to, or applied to, the management server.
1150	Information	Relay	All of the device details were reported to a higher management server.
1151	Information	Relay	The hierarchy configuration of a lower management server was changed.
1152	Information	Settings	The distribution of licenses and the permissions required to register licenses for lower management servers, including the initialization of settings, were successfully completed.
1154	Information	Settings	Old devices that have the same device information will be deleted.
1155	Information	Settings	Devices that have not been run for a long time will be deleted.
1156	Warning	Error	Devices information was deleted, but some hosts could not be deleted from the system configuration information. Use Remote Install Manager to delete hosts from the system configuration information as appropriate. Host ID = *Host ID*
1157#	Warning	Error	An error occurred during device maintenance. Set the correct system time on the server. If the problem persists, collect troubleshooting information (using appropriate command), and contact Support Service.
1158	Information	Assets	The primary inventory was deleted. A different inventory was set as the primary inventory.

Event number	Severity	Type	Event
1159	Warning	Security	The network control command has been received.
1160#	Warning	Security	The network control command has been received. However, the device whose network connection is to be blocked or allowed was not found.
1161#	Warning	Security	The network control command was executed. The network connection of multiple devices was blocked or allowed.
1162	Information	Security	An attempt to connect to the network was rejected as the result of the network control command.
1163	Information	Security	An attempt to connect to the network was approved as the result of the network control command.
1164	Information	Assets	Asset information import is complete. Asset Type=Hardware Asset add=*number-of-information-items* update=*number-of-information-items* error=*number-of-information-items*
1165	Information	Security	The import of the external log files is complete.
1166#	Warning	Error	An error occurred in the command ioutils importexlog.
1167#	Warning	Error	Part of the log import processing by the command ioutils importexlog was skipped.
1168	Warning	Inventory	No host ID could be generated based on virtual computer information.
1169	Warning	API	Failed to operate part of the API.
1170	Warning	API	Failed to authenticate the API user.
1171	Warning	API	Failed to run the API.
1172	Warning	API	The API request is incorrect.
1173	Warning	API	The expiration date of the user password authenticated by the API is near.
1174	Information	Assets	Asset information import is complete. Asset Type=Software License add=*number-of-information-items* update=*number-of-information-items* error=*number-of-information-items*
1175	Information	Assets	Asset information import is complete. Asset Type=Managed Software add=*number-of-information-items* update=*number-of-information-items* error=*number-of-information-items*
1176	Information	Assets	Asset information import is complete. Asset Type=Contract add=*number-of-information-items* update=*number-of-information-items* error=*number-of-information-items*
1177	Information	Assets	Asset information import is complete. Asset Type=Contract Vendor List add=*number-of-information-items*

Event number	Severity	Type	Event
1177	Information	Assets	update=*number-of-information-items* error=*number-of-information-items*
1178	Information	Assets	The import of asset association information is complete. association=*asset-association-information* update=*number-of-information-items* error=*number-of-information-items* The following is displayed for *asset-association-information*. • Hardware Asset-Devices • Hardware Asset-Asset • Hardware Asset-Contract
1179	Information	Assets	The import of asset association information is complete. association=*asset-association-information* update=*number-of-information-items* error=*number-of-information-items* The following is displayed for *asset-association-information*. • Software Licence-Managed Software • Software Licence-Upgrade Licence • Software Licence-Devices • Software Licence-Contract
1180	Information	Assets	The import of asset association information is complete. association=*asset-association-information* update=*number-of-information-items* error=*number-of-information-items* The following is displayed for *asset-association-information*. • Managed Software-Software • Managed Software-Software Licence
1181	Information	Assets	The import of asset association information is complete. association=*asset-association-information* update=*number-of-information-items* error=*number-of-information-items* The following is displayed for *asset-association-information*. • Contract-Hardware Asset • Contract-Software Licence • Contract-Contract Vendor List
1182#	Warning	Security	A device to be blocked was detected. Check the settings of the network control list. MAC address=*MAC-address* IPaddress=*IP-address*

#: When linked to JP1/IM, the ID displayed in JP1/IM for the JP1 event.

19.2 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_ITDM2_Service). The operation (JP1_ITDM2_Service) will be stopped.
extended attributes	common information	severity	SERVERITY	Emergency
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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 during the processing to store operation logs.
extended attributes	common information	severity	SERVERITY	Alert
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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 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

Attribute type		Item	Attribute name	Content
extended attributes	common information	issued host name	JP1_SOURCEHOST	The name of the management server in which an event occurred
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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/ITDM2
		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/ITDM2
		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	--	An error occurred while connecting to the Product Update server.*cause-of-error* Please check the Product Update settings, by using Test mode. For *cause-of-error*, the cause of the error is displayed depending on the situation.

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/ITDM2
		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 *cause-of-error*, the cause of the error is displayed depending on the situation.

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/ITDM2
		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 1058

Attribute type	Item	Attribute name	Content
basic attributes	event ID	--	0000690A

Attribute type		Item	Attribute name	Content
basic attributes		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/ITDM2
		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	MAC address(IP address)
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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/ITDM2
		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/ITDM2
		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
		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/ITDM2

Attribute type		Item	Attribute name	Content
extended attributes	common information	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/ITDM2
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	The database service (JP1_ITDM2_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/ITDM2
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	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/ITDM2
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	cause = *cause* 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 *cause*, the cause of the error is displayed depending on the situation.

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/ITDM2
		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

Attribute type		Item	Attribute name	Content
extended attributes	common information	issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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/ITDM2
		object type	OBJECT_TYPE	ITDM_SECURITY
		start time	START_TIME	event occurrence time
	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/ITDM2
		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

Attribute type		Item	Attribute name	Content
basic attributes		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/ITDM2
		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 1141

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000691a
		message	--	Errors occurred during the processing to delete the operation logs that exceeded the storage period from the operation log database, and the processing to re-create the index information of the operation log database.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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 1149

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000691B
		message	--	An error occurred while information was being sent to, or applied to, the management server.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		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	--	Information type = *information-type* Start date and time of transmission = *start-date-and-time-of-transmission* Host name of transmission source = *host-name-of-transmission-source* Host name of transmission destination = *host-name-of-transmission-destination* Details = *details* Cause of error = *cause-of-error*

For event number 1157

Attribute type		Item	Attribute name	Content
basic attributes		event ID	--	0000691C
		message	--	An error occurred during device maintenance.
extended attributes	common information	severity	SERVERITY	Alert
		issued host name	JP1_SOURCEHOST	Target server name
		product name	PRODUCT_NAME	/HITACHI/JP1/ITDM2
		object type	OBJECT_TYPE	ITDM_ERR
		start time	START_TIME	event occurrence time
	program-specific information	message details	--	Set the correct system time on the server. If the problem persists, collect troubleshooting information (using appropriate command), and contact Support Service.

20 API

This chapter describes the API provided by JP1/IT Desktop Management 2.

20.1 Overview of the API

By using the API provided by JP1/IT Desktop Management 2, you can register device information in JP1/IT Desktop Management 2 from an external system.

The API provided by JP1/IT Desktop Management 2 is compliant with the Representational State Transfer (REST) architecture style.

20.2 Common API specifications

This section presents the specifications common to the APIs provided by JP1/IT Desktop Management 2.

Communication method

The following communication protocols and port numbers are used by APIs.

Communication protocols

HTTP protocol and HTTPS protocol are supported by APIs. For both protocols, version 1.1 is supported. For the detailed specifications of the communication protocols, see the following standards:

- HTTP protocol: RFC2616
- HTTPS protocol: RFC2818

When HTTPS is used as the communication protocol, TLS 1.2 and SHA-2 (SHA-256) are used.

> **Important**
>
> The SSL server certificate is necessary to use HTTPS. For details, see the JP1/IT Desktop Management 2 Configuration Guide for information on how to build an environment for using HTTPS with the external system linkage configuration.

Port number

The port number is set to 31030 by default. To change the port number, perform a setup on the management server.

Security and authentication

To send an API request and get a response, you have to undergo user authentication.

To undergo user authentication, specify authentication information in the request header as follows:

```
X-ITDM-Authorization1:user-ID
X-ITDM-Authorization2:password
```

user-ID

Specify a character string generated from a Base64-encoded user ID. API permission must be assigned to the specified user ID.

password

Specify a character string generated from the Base64-encoded password that corresponds to the set user ID.

I/O format

APIs use the JSON format for both requests and responses. Specify data format in the request header as follows:

```
Content-Type:application/json
```

Use UTF-8 as the character encoding.

For details about the data type of the value set in the message body of requests and responses, see the applicable description provided by respective APIs.

Request format

The request format consists of the request line, the request header, and the request message body. Specify ASCII characters in the request line and the request header. URL encoding is necessary if you specify illegal URL characters.

Format

```
method△/jp1itdm/api/apiVersion/resource/other?query△HTTP/1.1
Host:host:port
Accept-Language:lang
Content-Type:application/json
Accept:application/json
X-ITDM-Authorization1:userID
X-ITDM-Authorization2:password

messageBody
```

Item			Category	Description
Request line		*method*	Mandatory	Specify one of the following methods: • GET • POST • PUT • DELETE The specifiable methods vary with each API. For details, see the applicable description provided by each API.
		apiVersion	Mandatory	Specify an API version. For details, see the applicable description provided by each API.
		resource	Mandatory	Specify a resource. The specifiable resources vary with each API. For details, see the applicable description provided by each API.
		other	Optional	If necessary, specify a value that can uniquely identify a resource or resource operation. For details, see the applicable description provided by each API.
		?*query*	Optional	If necessary, specify a query string. For details, see the applicable description provided by each API.
Request header	Host:	*host*	Mandatory	Specify either the host name or IP address of the management server.
		port	Mandatory	Specify the port number of the management server.

	Accept-Language:	*lang*	Mandatory	Specify one of the following language codes in the message of responses:
				`ja`
				Japanese
				`en`
				English
				`zh`
				Simplified Chinese

	Content-Type:	application/json	#	Always specify `application/json`.
	Accept:	application/json	Mandatory	Always specify `application/json`.

Item			Category	Description
Request header	X-ITDM-Authorization1:	*userID*	Mandatory	Specify a character string generated from a Base64-encoded user ID.
	X-ITDM-Authorization2:	*password*	Mandatory	Specify a character string generated from the Base64-encoded password that corresponds to the set user ID.
Request message body		*messageBody*	Optional	If necessary, specify the message body in JSON format. For details, see the applicable description provided by each API.

#:

When *method* is set to `GET`

No need to specify

In all other cases

Mandatory

Important

Specify data within 30 MB in the request message body.

Response format

The format of a response to a request consists of the status line, the response header, and the response message body. Specify ASCII characters in the status line and the response header.

Format

```
HTTP/1.1Δstatus CodeΔstatusCodeText
Content-Type:application/json
Cache-Control:no-store, no-cache, max-age=0
X-Content-Type-Options:nosniff

messageBody
```

Item			Description
Status line		*statusCode*	The status code is stored. For details, see *Status codes* in this section.
		statusCodeText	The text of the status code is stored. For details, see *Status codes* in this section.
Response header	Content-Type:	application/json	Always return `application/json`.
	Cache-Control:	no-store, no-cache, max-age=0	Always return `no-store, no-cache, max-age=0`.
	X-Content-Type-Options:	nosniff	Always return `nosniff`.
Response message body		*messageBody*	The response data returned when an API is called is stored in JSON format. For details, see the applicable description provided by each API. In addition, when an error occurs, error information is stored in JSON format. For details, see *Error information* in this section.

Status codes

The following table describes the status codes that can be contained in the response message returned following the execution of an API:

Status code	Text of the status code	Description
100	Continue	The client can continue with the remainder of its request.
200	OK	The request ended successfully.
206	Partial Content	A partial resource is returned.
207	Multi-Status	An error occurred during the operation of multiple resources.
300	Multiple Choices	The use of multiple pages is possible.
301	Moved Permanently	The resource has permanently moved to another location.
302	Found	The resource has temporarily moved to another location.
303	See Other	The resource has moved to another location.
304	Not Modified	The requested contents have not been modified.
400	Bad Request	• The argument is invalid. • The request format is incorrect.
401	Unauthorized	• An ID or password has not been specified. • The specified ID or password is incorrect. • The account is locked.
403	Forbidden	• The client does not have the permission to execute the resource. • The user does not have the API permission.
404	Not Found	The client attempted to access a nonexistent resource.
405	Method Not Allowed	The client attempted to access an unauthorized resource.
406	Not Acceptable	The specified data format is not supported.
408	Request Time-out	The request timed out.
410	Gone	The resource is no longer available.
411	Length Required	The client must specify the `Content-Length` header.
412	Precondition Failed	One or more preconditions the client specified by the `If-Unmodified-Since` header, the `If-Matched` header, or the like failed.
413	Request Entity Too Large	The message body of the request is too long.
414	Request-URI Too Long	The request line is too long.
416	Requested Range Not Satisfiable	The range specified with the `Range` header is out of range of the resource in question.
417	Expectation Failed	The request to extend the `Expect` request header field was not accepted.
429	Too Many Requests	The request was rejected because the user has sent too many requests.
453	Expiration Password	The password has expired.
500	Internal Server Error	The request could not be processed because an error occurred inside the server.
501	Method Not Implemented	The requested HTTP method is not supported.
502	Bad Gateway	The proxy server received an invalid request.

Status code	Text of the status code	Description
503	Service Unavailable	The service on the management server is not completely up and running.
506	Variant Also Negotiates	The server has an internal configuration error.
512	License Error	No license is registered.
513	Temporary Error	A temporary error occurred.
514	JP1/Base Error	An error occurred on the JP1/Base authentication server.

Error information

When an API request is not successful, error information in JSON format is stored in the message body of a response and then returned. Error information has the following format.

Format

```
{
  "errorSource":"the-URL-triggered-the-error"
  "message":"message",
  "messageID":"message-ID",
  "application":"jp1itdm"
}
```

Attribute	Data type	Description
errorSource	string	The URL that triggered the error
message	string	The message
messageID	string	The message ID

Example: A response returned when the user ID does not exist

```
HTTP/1.1 401 Unauthorized
Content-Type: application/json
Cache-Control: no-store, no-cache, max-age=0
X-Content-Type-Options: nosniff

{
"errorSource": "http://example.com:31030/jp1itdm/api/v1/objects/devices",
"message": "Authentication failed. The possible causes are as follows:
- The user ID or password (case-sensitive) is incorrect.
- The user account is locked.
You have to contact the administrator to find out if the user account is loc
ked.",
"messageID": "KDEX2016-E",
"application": "jp1itdm"
}
```

Supported data types

Set a message body of a request or response by specifying a string enclosed in double quotation marks (""). The following table describes the character string format used with each data type.

Data type	Description
int	An integer in the range -2,147,483,647 to 2,147,483,647 enclosed in "". Example: "123"
unsigneInt	An integer in the range 0 to 2,147,483,647 enclosed in "". Example: "123"
long	An integer in the range -9,223,372,036,854,775,807 to 9,223,372,036,854,775,807 enclosed in "". Example: "123"
unsignedLong	An integer in the range 0 to 9,223,372,036,854,775,807 enclosed in "". Example: "123"
string	Text data. Specify a string except control characters of ASCII characters. Any numerics specified in string-type data are treated as decimal numbers, unless otherwise specified. Example: "sample text"
dateTime	Specify date and time or date. In case of date and time, specify "*YYYY-MM-DD*T*HH*:*MM*:*SS*.*sss*Z" in UTC format. *YYYY* Specify four digits for the year. *MM* Specify two digits for the month. *DD* Specify two digits for the date. *HH* Specify two digits for the hour. *MM* Specify two digits for the minute. *SS* Specify two digits for the second. *sss* Specify three digits for the millisecond. Example of the value specified to indicate 6:52:16.000 on May 8, 2019: "2019-05-08T06:52:16.000Z" Incase of date, specify "*YYYY-MM-DD*T00:00:00.000Z" format. Example of the value specified to indicate May 8, 2019: "2019-05-08T00:00:00.000Z"

Simultaneous Execution

Up to 4 APIs can be executed at the same time.

20.3 List of APIs

The following list shows the APIs provided by JP1/IT Desktop Management 2:

Function	Description
Device registration	Registers device information in the management server.
Device information list acquisition	Acquires a device information list from the management server.
Installed software information list acquisition	Acquires an installed software information list (list that shows information regarding the software programs installed on devices) from the management server.

20.3.1 Device registration

This API registers device information in the management server.

Note

You can register multiple device information in the management server with just one request. When specified information regarding one of the devices to be registered contains an error, the registration of the erroneous device information is skipped, and the processing continues.

Note

Device registration is executed asynchronously. For this reason, even when a response is successfully returned, it does not necessarily mean that the devices have already been registered in the management server.

Note

The security judgment is performed when all of the following conditions are met. The violation level becomes **Unknown** when the information necessary for security status judgment is insufficient. Disable the security setting items of security policies as necessary.

- The `SystemInventory` object exists.
- The `SecurityInventory` object exists.
- The device type is PC or Server, and the OS type is Windows or Mac OS.
- Windows or Mac OS is specified as the OS code.
- In case of Windows, an OS language is specified.

Execution permission

You need the following permission:

- API permission

API version

v1

Request format

Request line

```
POST /jp1itdm/api/v1/objects/devices HTTP/1.1
```

Request header

```
Host:host-name-or-IP-address-of-management-server:port-number-of-managemen
t-server
Accept-Language:language-code-in-the-message-of-response
Accept:application/json
Content-Type:application/json
X-ITDM-Authorization1:Base64-encoded-user-ID
X-ITDM-Authorization2:Base64-encoded-password
```

Request message body

Specify information regarding the devices to be registered in JSON format. For details, see *Data format of information regarding the devices to be registered* in this section.

Data format of information regarding the devices to be registered

Information regarding the devices to be registered must be specified in the following format:

```
{
    "Device-Inventory": [
        {
            "Report": {
                "@Version": "0250",
                "ID": "identifier",
                "@CreationDate": "YYYY-MM-DDTHH:MM:SS.sssZ",
                "Agent": {
                    "Type": "REST",
                    "DeviceStatus": "device-status",
                    "Status": "management-status-registered-device",
                    "DistributionStatus": "0",
                    "DiscoveryProtocol": "7",
                    "LastAliveDate": "YYYY-MM-DDTHH:MM:SS.sssZ"
                },
                "Inventory": {
                    "Equipment": {
                        "Type": "device-type",
                        "UserType": "device-type-added-by-user"
                    },
                    "SystemInventory": {
                        "@LastUpdateTime": "YYYY-MM-DDTHH:MM:SS.sssZ",
                        "BaseBoard": {
                            "SerialNumber": "motherboard-serial-number"
                        },
                        "BIOS": {
                            "Manufacturer": "BIOS-manufacturer",
                            "Name": "BIOS-name",
                            "ReleaseDate": "BIOS-released-date",
                            "SerialNumber": "BIOS-serial-number",
```

```
                        "SMBIOSBIOSVersion": "BIOS-version-(SMBIOS)",
                        "Version": "BIOS-version"
                    },
                    "CDROMDriveList": {
                        "CDROMDrive": [
                            {
                                "Name": "CD-ROM-drive-name"
                            }, ...
                        ]
                    },
                    "ComputerSystem": {
                        "CurrentTimezone": "current-timezone",
                        "Domain": "domain-workgroup",
                        "DomainRole": "domain-role",
                        "Manufacturer": "manufacturer",
                        "Model": "model-name",
                        "Name": "computer-name",
                        "NumberOfProcessors": "number-of-processors",
                        "TotalPhysicalMemory": "physical-memory",
                        "UserName": "user-name"
                    },
                    "ComputerSystemProduct": {
                        "IdentifyingNumber": "machine-serial-number",
                        "UUID": "machine-UUID"
                    },
                    "DesktopMonitorList": {
                        "DesktopMonitor": [
                            {
                                "Name": "monitor-name"
                            }, ...
                        ]
                    },
                    "DiskDriveList": {
                        "DiskDrive": [
                            {
                                "DeviceID": "device-ID-of-harddisk",
                                "InterfaceType": "interface-type-of-hard
disk",
                                "Model": "model-name-of-harddisk",
                                "Size": "harddisk-size"
                            }, ...
                        ]
                    },
                    "KeyboardList": {
                        "Keyboard": [
                            {
                                "Description": "keyboard-name"
                            }, ...
                        ]
                    },
                    "LogicalDiskList": {
                        "LogicalDisk": [
                            {
                                "DeviceID": "drive-letter",
                                "DriveType": "drive-type",
                                "FileSystem": "file-system",
                                "FreeSpace": "drive-free-space",
                                "Size": "drive-size"
```

```
                        }, ...
                    ]
                },
                "DiskDriveToLogicalDiskList": {
                    "DiskDriveToLogicalDisk": [
                        {
                            "DiskDriveDeviceID": "harddisk-device-ID
",
                            "LogicalDiskDeviceID": "drive-letter"
                        }, ...
                    ]
                },
                "BitLocker": {
                    "DriveList": {
                        "Drive": [
                            {
                                "DriveLetter": "drive-letter",
                                "ProtectionStatus": "BitLocker-prote
ction-status",
                                "LockStatus": "lock-status"
                            }, ...
                        ]
                    }
                },
                "NetworkAdapterList": {
                    "NetworkAdapter": [
                        {
                            "DeviceID": "device-ID-of-network-adapte
r",
                            "Name": "name-of-network-adapter"
                        }, ...
                    ]
                },
                "NetworkAdapterConfigurationList": {
                    "NetworkAdapterConfiguration": [
                        {
                            "DefaultIPGatewayList": {
                                "DefaultIPGateway": [
                                    {
                                        "_value": "default-gateway",
                                        "@Index": "index"
                                    }
                                ]
                            },
                            "DHCPEnabled": "DHCP-enable-or-disable",
                            "DHCPLeaseExpires": "DHCP-lease-expires"
,
                            "DHCPLeaseObtained": "DHCP-lease-obtaine
d",
                            "DHCPServer": "DHCP-server-address",
                            "DNSServerSearchOrderList": {
                                "DNSServerSearchOrder": [
                                    {
                                        "_value": "DNS-server-addres
s",
                                        "@Index": "index"
                                    }, ...
                                ]
```

```
                                    },
                                    "Index": "setting-ID-of-network-adapter-
configuration-information",
                                    "IPAddressList": {
                                        "IPAddress": [
                                            {
                                                "_value": "IP-address",
                                                "@Index": "index"
                                            }, ...
                                        ]
                                    },
                                    "IPSubnetList": {
                                        "IPSubnet": [
                                            {
                                                "_value": "subnet-mask",
                                                "@Index": "index"
                                            }
                                        ]
                                    },
                                    "MACAddress": "MAC-address",
                                    "WINSPrimaryServer": "primary-WINS-serve
r-address",
                                    "WINSSecondaryServer": "secondary-WINS-s
erver-address"
                                }, ...
                            ]
                        },
                        "NetworkAdapterToNetworkAdapterConfigurationList": {
                            "NetworkAdapterToNetworkAdapterConfiguration": [
                                {
                                    "NetworkAdapterDeviceID": "device-ID-of-
network-adapter",
                                    "NetworkAdapterConfigurationIndex": "set
ting-ID-of-network-adapter-configuration-information"
                                }, ...
                            ]
                        },
                        "HostName": "host-name",
                        "OperatingSystem": {
                            "OSKind": "OS-kind",
                            "Caption": "OS-name",
                            "KernelVersion": "kernel-version",
                            "CSDVersion": "service-pack-or-OS-version",
                            "Description": "description-of-computer",
                            "Locale": "locale",
                            "Organization": "organization",
                            "OSCode": "OS-code",
                            "OSLanguage": "OS-language",
                            "RegisteredUser": "registered-user-name",
                            "SerialNumber": "OS-serial-number",
                            "TotalVirtualMemorySize": "total-virtual-memory-
size"
                        },
                        "PhysicalMemoryList": {
                            "PhysicalMemory": [
                                {
                                    "Capacity": "physical-memory-capacity"
                                }, ...
```

```
                    ]
                },
                "PointingDeviceList": {
                    "PointingDevice": [
                        {
                            "Name": "mouse-name"
                        }
                    ], ...
                },
                "PrinterList": {
                    "Printer": [
                        {
                            "Attributes": "printer-attributes",
                            "DriverName": "printer-driver-name",
                            "Name": "printer-name",
                            "PortName": "printer-port-name",
                            "ServerName": "printer-server-name",
                            "ShareName": "printer-shared-name"
                        }, ...
                    ]
                },
                "ProcessorList": {
                    "Processor": [
                        {
                            "Name": "processor-name"
                        }, ...
                    ]
                },
                "SoundDeviceList": {
                    "SoundDevice": [
                        {
                            "Manufacturer": "sound-device-manufactur
er",
                            "Name": "sound-device-product-name"
                        }, ...
                    ]
                },
                "UserAccount": {
                    "Description": "user-description",
                    "FullName": "user-name"
                },
                "VideoControllerList": {
                    "VideoController": [
                        {
                            "AdapterRAM": "VRAM-capacity",
                            "Name": "video-driver-name",
                            "VideoProcessor": "video-processor"
                        }, ...
                    ]
                },
                "AMTFirmwareVersion": "AMT-firmware-version",
                "WindowsInstaller": "Windows-Installer-version",
                "IEVersion": "Internet-Explorer-version",
                "IEServicePack": "Internet-Explorer-service-pack",
                "PowerManagement": {
                    "VideoTimeoutAC": "video-timeout-AC",
                    "VideoTimeoutDC": "video-timeout-DC",
                    "SpindownTimeoutAC": "spindown-timeout-AC",
```

```
                        "SpindownTimeoutDC": "spindown-timeout-DC",
                        "StandbyTimeoutAC": "standby-timeout-AC",
                        "StandbyTimeoutDC": "standby-timeout-DC",
                        "HibernateTimeoutAC": "hibernate-timeout-AC",
                        "HibernateTimeoutDC": "hibernate-timeout-DC",
                        "ThrottlePolicyAC": "throttle-policy-AC",
                        "ThrottlePolicyDC": "throttle-policy-DC"
                    },
                    "property": [
                        {
                            "@category": "category-name",
                            "@key": "key",
                            "@value": "value",
                            "@type": "type",
                            "@record": "record-number"
                        }, ...
                    ]
                    "SmartDeviceInformation": {
                        "UUID": "device-identifier",
                        "IMEI": "IMEI",
                        "UDID": "UDID",
                        "ICCID": "ICCID",
                        "IMSI": "IMSI",
                        "PhoneNumber": "phone-number",
                        "mail": "E-mail-address",
                        "Carrier": "carrier",
                        "PasscodeSetting": "passcode-setting",
                        "PhisicalMemory": {
                            "Size": "physical-memory-size",
                            "FreeSpace": "physical-memory-free-size"
                        },
                        "Storage": {
                            "Size": "storage-size",
                            "FreeSpace": "storage-free-space"
                        },
                        "Media": {
                            "Size": "external-media-size",
                            "FreeSpace": "external-media-free-space"
                        }
                    }
                },
                "InstalledSoftware": {
                    "@ReportType": "All",
                    "@LastUpdateTime": "YYYY-MM-DDTHH:MM:SS.sssZ",
                    "SoftwareList": {
                        "Software": [
                            {
                                "@Type": "software-type",
                                "SourceID": "source-ID",
                                "InstallPath": "install-path",
                                "Name": "software-name",
                                "Version": "software-version",
                                "Publisher": "software-publisher",
                                "InstallDate": "YYYY-MM-DDTHH:MM:SS.sssZ
",
                                "HelpLink": "support-URL",
                                "AppType": "app-type"
                            }, ...
```

```
                        ]
                    }
                },
                "Update": {
                    "@ReportType": "All",
                    "@LastUpdateTime": "YYYY-MM-DDTHH:MM:SS.sssZ",
                    "SoftwareList": {
                        "Software": [
                            {
                                "HotFixID": "hotfix-ID",
                                "Description": "hotfix-description",
                                "InstallDate": "YYYY-MM-DDTHH:MM:SS.sssZ
",
                                "Type": "hotfix-type"
                            }, ...
                        ]
                    }
                },
                "SecurityInventory": {
                    "@LastUpdateTime": "YYYY-MM-DDTHH:MM:SS.sssZ",
                    "AccountList": {
                        "Account": [
                            {
                                "Name": "account-name",
                                "LastPasswordModifiedDate": "last-passwo
rd-modified-date",
                                "WeakPassword": "weak-password",
                                "UnexpirePassword": "unexpire-password",
                                "ScreenSaverEnabled": "screen-saver-enab
led",
                                "ScreenSaverIsSecure": "screen-saver-is-
secure",
                                "ScreenSaverTimeout": "screen-saver-time
out"
                            }, ...
                        ]
                    },
                    "PowerOnPassword": "power-on-password",
                    "GuestAccount": "Guest-account",
                    "AutoLogin": "auto-login",
                    "SharedDirectory": "shared-directory",
                    "AutoShareServer": "auto-share-server",
                    "DCOM": "DCOM",
                    "RestrictAnonymous": "restrict-anonymous-access",
                    "WindowsFirewall": "Windows-firewall-setting",
                    "WindowsUpdate": "Windows-update",
                    "DenyTSConnections": "remote-desktop-connection"
                },
                "ExtendedInventory": {
                    "@LastUpdateTime": "YYYY-MM-DDTHH:MM:SS.sssZ",
                    "ExtendInventoryList": {
                        "ExtendInventoryItem": [
                            {
                                "@InformationType": "information-type",
                                "ItemName": "additional-management-item"
,
                                "Value": "input-item-value",
                                "ValueList": {
```

```
                                        "Value": "setelcted-item-value", ...
                                    },
                                    "ValueTree": {
                                        "Value": {
                                            "Data": "value-of-tier-1",
                                            "Value": {
                                                "Data": "value-of-tier-2",
                                                    "Value": {
                                                        "Data": "value-of-ti
er-3",
                                                        "Value": {
                                                            ...
                                                        }
                                                    }
                                                }
                                            }
                                        }
                                    }, ...
                                ]
                            }
                        }
                    }
                }
            }, ...
        ]
}
```

Legend:

`, ...`: Iterations of the previous object or data definition

...: Iterations of the previous layer

Note

When there are duplicate elements like shown on the following JSON example, the last element is selected. In addition, if an element not defined in the API is specified, it is ignored.

```
{
  "Device-Inventory": [
    {
      "Report": {
        (omitted)
        "Agent": {                  //Duplicate element
          (omitted)
        },
        "Agent": {                  //Duplicate element, the last one
 is selected
          (omitted)
        },
        "UndefinedItem" : "xxx",    //Undefined element, it is ignore
d
        "Inventory": {
          (omitted)
```

Device-Inventory

Item name	Data type	Mandatory / Optional	Description
Device-Inventory	Array	Mandatory	Root name of information regarding the devices to be registered. Specify at least one but no more than 1,000 `Report` objects.
Report	Object	Mandatory	Object name of the device information. For details, see *Report object*.

Important

One `Report` object should be within 1 MB of data size.

Report object

Item name	Data type	Mandatory / Optional	Description
@Version	string	Mandatory	Always specify `0250`.
ID	string	Mandatory	ID that uniquely identifies the device. Specify a string of ASCII characters except control characters.
@CreationDate	dateTime	Mandatory	Specify the date and time when the `Report` object was generated.
Agent	Object	Mandatory	Object name of basic information regarding the device. For details about this object, see *Agent object*.
Inventory	Object	Optional	Object name of information regarding the inventory. For details about this object, see *Inventory object*.

Agent object

Item name	Data type	Mandatory / Optional	Description
Type	string	Mandatory	Always specify `REST`.
DeviceStatus	int	Mandatory	Device status. Specify one of the following: • `0`: Up and running • `1`: Down • `2`: Warning • `3`: Failure • `999`: Unknown
Status	int	Mandatory	Management status at the time the device is registered. Specify one of the following: • `0`: Managed • `2`: Discovered
DistributionStatus	int	Mandatory	Always specify `0`.
DiscoveryProtocol	int	Mandatory	Always specify `7`.
LastAliveDate	dateTime	Optional	Specify the last date and time the device was checked. If you omit this item, the date and time when the device is registered is set.

Inventory object

Item name	Data type	Mandatory / Optional	Description
Equipment	Object	Mandatory	Object name of the device information. For details, see *Equipment object*.
SystemInventory	Object	Optional	Object name of system information and hardware information. For details, see *SystemInventory object*.
InstalledSoftware	Object	Optional	Object name of information regarding installed software. For details see *InstalledSoftware object*.
Update	Object	Optional	Object name of update information. For details, see *Update object*.
SecurityInventory	Object	Optional	Object name of security and OS setting information. For details, see *SecurityInventory object*.
ExtendInventory	Object	Optional	Object name of common management fields of asset information and device information, and additional management fields of hardware asset information. For details, see *ExtendedInventory object*.

Equipment object

Item name	Data type	Mandatory / Optional	Description
Type	string	Mandatory	Device type. Specify one of the following: • `EquipmentTypeComputer`: PC • `EquipmentTypeServer`: Server • `EquipmentTypeNetworkDevice`: Network device • `EquipmentTypePrinter`: Printer device • `EquipmentTypeStorage`: Storage device • `EquipmentTypePeripheralDevice`: Peripheral device • `EquipmentTypeUSBMemory`: USB memory • `EquipmentTypeSmartDevice`: Smart device • `EquipmentTypeUser`: Device type added by the user • `EquipmentTypeOther`: Other device
UserType	string	This item is mandatory if `EquipmentTypeUser` is specified as `Type`, and optional in all the other cases.	If you specified `EquipmentTypeUser` as `Type`, specify the device type added by the user.

SystemInventory object

Item name	Data type	Mandatory / Optional	Description
@LastUpdateTime	dateTime	Mandatory	Specify the date and time when the `SystemInventory` object was generated.
BaseBoard	Object	Optional	Object name of motherboard information. For details, see *BaseBoard object*.
BIOS	Object	Optional	Object name of BIOS information. For details, see *BIOS object*.
CDROMDriveList	Object	Optional	Object that puts together CD-ROM drive information. For details, see *CDROMDriveList object*.

Item name	Data type	Mandatory / Optional	Description
ComputerSystem	Object	Optional	Object name of computer information. For details, see *ComputerSystem object*.
ComputerSystemProduct	Object	Optional	Object name of computer product information. For details, see *ComputerSystemProduct object*.
DesktopMonitorList	Object	Optional	Object that puts together monitor information. For details, see *DesktopMonitorList object*.
DiskDriveList	Object	Optional	Object that puts together hard disk information. For details, see *DiskDriveList object*.
KeyboardList	Object	Optional	Object that puts together keyboard information. For details, see *KeyboardList object*.
LogicalDiskList	Object	Optional	Object that puts together Logical drive information. For details, see *LogicalDiskList object*.
DiskDriveToLogicalDiskList	Object	Optional	Object representing information that associates hard disk information with logical drive information. For details, see *DiskDriveToLogicalDiskList object*.
BitLocker	Object	Optional	Object name of BitLocker drive encryption information. For details, see *BitLocker object*.
NetworkAdapterList	Object	Optional	Object that puts together network adapter information. For details, see *NetworkAdapterList object*.
NetworkAdapterConfigurationList	Object	Optional	Object that puts together network adapter configuration information. For details, see *NetworkAdapterConfigurationList object*.
NetworkAdapterToNetworkAdapterConfigurationList	Object	Optional	Object representing information that associates network adapter information with network adapter configuration information. For details, see *NetworkAdapterToNetworkAdapterConfigurationList object*.
HostName	string	Optional	Specify a host name, which must be ASCII characters and no more than 256 characters.
OperatingSystem	Object	Optional	Object name of operating system information. For details, see *OperatingSystem object*.
PhysicalMemoryList	Object	Optional	Object that puts together physical memory information. For details, see *PhysicalMemoryList object*.
PointingDeviceList	Object	Optional	Object that puts together mouse information. For details, see *PointingDeviceList object*.
PrinterList	Object	Optional	Object that puts together printer information. For details, see *PrinterList object*.
ProcessorList	Object	Optional	Object that puts together processor information. For details, see *ProcessorList object*.
SoundDeviceList	Object	Optional	Object that puts together sound card information. For details, see *SoundDeviceList object*.
UserAccount	Object	Optional	Object name of user account information. For details, see *UserAccount object*.
VideoControllerList	Object	Optional	Object that puts together video controller information. For details, see *VideoControllerList object*.
AMTFirmwareVersion	string	Optional	Specify the AMT firmware version, which must be no more than 128 characters.

Item name	Data type	Mandatory / Optional	Description
WindowsInstaller	string	Optional	Specify the Windows Installer version, which must be no more than 1,024 characters.
WindowsUpdateAgent	string	Optional	Specify the Windows Update Agent version, which must be no more than 1,024 characters.
OSLastStartupTime	dateTime	Optional	Specify the last date and time the OS was started.
WindowsDirectory	string	Optional	Specify the Windows directory, which must be no more than 255 characters.
IEVersion	string	Optional	Specify the Internet Explorer version, which must be no more than 64 characters.
IEServicePack	string	Optional	Specify the Service Pack applied to Internet Explorer, which must be no more than 1,024 characters. Enclose the specified character string in semicolons (`;`), as in `;SP2;`.
PowerManagement	Object	Optional	Object name of power management information. For details, see *PowerManagement object*.
property	Array	Optional	Array whose elements consist of one or more objects representing general inventory information. For details, see *property array*. Specify up to 512 objects for this array.
SmartDeviceInformation	Object	Optional	Object name of smart device information. For details, see *SmartDeviceInformation object*.

BaseBoard object

Item name	Data type	Mandatory / Optional	Description
SerialNumber	string	Optional	Specify the serial number of the motherboard, which must be no more than 1,024 characters.

BIOS object

Item name	Data type	Mandatory / Optional	Description
Manufacturer	string	Optional	Specify the manufacturer of the BIOS, which must be no more than 1,024 characters.
Name	string	Optional	Specify the name of the BIOS, which must be no more than 1,024 characters.
ReleaseDate	dateTime	Optional	Specify the date and time when the BIOS was released.
SerialNumber	string	Optional	Specify the serial number of the BIOS, which must be no more than 1,024 characters.
SMBIOSBIOSVersion	string	Optional	Specify the SMBIOS version of the BIOS, which must be no more than 1,024 characters.
Version	string	Optional	Specify the version of the BIOS, which must be no more than 1,024 characters.

CDROMDriveList object

Item name	Data type	Mandatory / Optional	Description
CDROMDrive	Array	Mandatory	Array whose elements consist of one or more objects representing CD-ROM drive information. You have to specify 1 to 26 objects for this array.
Name	string	Optional	This item is part of each object in the `CDROMDrive` array. Specify the CD-ROM drive name, which must be no more than 1,024 characters.

ComputerSystem object

Item name	Data type	Mandatory / Optional	Description
CurrentTimeZone	int	Optional	Specify the current time zone in minutes. For example, specify `540` (9 hours) for Japan Standard Time.
Domain	string	Optional	Specify the name of the domain or work group, which must be no more than 1,024 characters.
DomainRole	string	Optional	Domain role. Specify one of the following: • `DomainRoleStandaloneWorkstation`: Standalone Workstation • `DomainRoleMemberWorkstation`: MemberWorkstation • `DomainRoleStandaloneServer`: Standalone Server • `DomainRoleMemberServer`: Member Server • `DomainRoleBackupDomainController`: Backup Domain Controller • `DomainRolePrimaryDomainController`: PrimaryDomainController
Manufacturer	string	Optional	Specify the manufacturer of the computer, which must be no more than 1,024 characters.
Model	string	Optional	Specify the model name of the computer, which must be no more than 1,024 characters.
Name	string	Optional	Specify the computer name, which must be no more than 1,024 characters.
NumberOfProcessors	unsignedInt	Optional	Specify the number of processors installed on the computer, which must be 0 to 65535.
TotalPhysicalMemory	unsignedLong	Optional	Specify the amount of memory installed on the computer in bytes.
UserName	string	Optional	Specify the user of the physical console session who last logged in, which must be no more than 1,024 characters. If the user is currently logged in, specify the current user.

ComputerSystemProduct object

Item name	Data type	Mandatory / Optional	Description
IdentifyingNumber	string	Optional	Specify the serial number of the machine, which must be no more than 1,024 characters.
UUID	string	Optional	Specify the machine UUID, which must be no more than 1,024 characters.

DesktopMonitorList object

Item name	Data type	Mandatory / Optional	Description
DesktopMonitor	Array	Mandatory	Array whose elements consist of one or more objects representing monitor information. You have to specify 1 to 8 objects for this array.
Name	string	Optional	This item is part of each object in the `DesktopMonitor` array. Specify the name of the monitor, which must be no more than 1,024 characters.

DiskDriveList object

Item name	Data type	Mandatory / Optional	Description
DiskDrive	Array	Mandatory	Array whose elements consist of one or more objects representing hard disk information. You have to specify 1 to 255 objects for this array.
DeviceID	string	Mandatory	This item is part of each object in the `DiskDrive` array. Specify the device ID of the hard disk, which must be no more than 1,024 characters.
InterfaceType	string	Optional	This item is part of each object in the `DiskDrive` array. Specify the interface type of the hard disk, which must be no more than 1,024 characters.
Model	string	Optional	This item is part of each object in the `DiskDrive` array. Specify the model name of the hard disk, which must be no more than 1,024 characters.
Size	unsignedLong	Optional	This item is part of each object in the `DiskDrive` array. Specify hard disk capacity in bytes.

KeyboardList object

Item name	Data type	Mandatory / Optional	Description
Keyboard	Array	Mandatory	Array whose elements consist of one or more objects representing keyboard information. You have to specify 1 to 8 objects for this array.
Description	string	Optional	This item is part of each object in the `Keyboard` array. Specify the name of the keyboard, which must be no more than 1,024 characters.

LogicalDiskList object

Item name	Data type	Mandatory / Optional	Description
LogicalDisk	Array	Mandatory	Array whose elements consist of one or more objects representing logical drive information. You have to specify 1 to 26 objects for this array.
DeviceID	string	Optional	This item is part of each object in the `LogicalDisk` array. Specify the drive letter, which must be no more than 1,024 characters.

Item name	Data type	Mandatory / Optional	Description
DriveType	string	Optional	This item is part of each object in the `LogicalDisk` array. Specify one of the following options as the drive type: • DriveTypeUnknown • DriveTypeRemovableDisk • DriveTypeLocalDisk • DriveTypeCompactDisc • DriveTypeRAMDisk
FileSystem	string	Optional	This item is part of each object in the `LogicalDisk` array. Specify the name of the file system, which must be no more than 1,024 characters.
FreeSpace	unsignedLong	Optional	This item is part of each object in the `LogicalDisk` array. Specify free drive space in bytes.
Size	unsignedLong	Optional	This item is part of each object in the `LogicalDisk` array. Specify drive capacity in bytes.

DiskDriveToLogicalDiskList object

Item name	Data type	Mandatory / Optional	Description
DiskDriveToLogicalDisk	Array	Mandatory	Array whose elements consist of one or more objects representing information that associates hard disk information with logical drive information. You have to specify 1 to 255 objects for this array.
DiskDriveDeviceID	string	Mandatory	This item is part of each object in the `DiskDriveToLogicalDisk` array. Specify the device ID of the hard disk, which must be no more than 1,024 characters.
LogicalDiskDeviceID	string	Mandatory	This item is part of each object in the `DiskDriveToLogicalDisk` array. Specify the drive letter, which must be no more than 1,024 characters.

Important

When a device ID of a nonexistent hard disk or a nonexistent drive letter is specified, the association is judged as being invalid.

BitLocker object

Item name	Data type	Mandatory / Optional	Description
DriveList	Object	Mandatory	Object that puts together BitLocker drive encryption information.
Drive	Array	Mandatory	Array whose elements consist of one or more objects representing drive information encrypted with BitLocker. You have to specify 1 to 255 objects for this array.
DriveLetter	string	Mandatory	This item is part of each object in the `Drive` array. Specify the drive letter of the drive encrypted with BitLocker, which must be no more than 1,024 characters.

Item name	Data type	Mandatory / Optional	Description
ProtectionStatus	int	Mandatory	This item is part of each object in the `Drive` array. Specify one of the following as the protection provided by BitLocker: • `0`: No encryption • `1`: Encrypted • `2`: Unknown
LockStatus	int	Mandatory	This item is part of each object in the `Drive` array. Specify one of the following as the lock status: • `0`: No lock • `1`: Locked (encrypted and locked)

NetworkAdapterList object

Item name	Data type	Mandatory / Optional	Description
NetworkAdapter	Array	Mandatory	Array whose elements consist of one or more objects representing network adapter information. You have to specify 1 to 255 objects for this array.
DeviceID	string	Mandatory	This item is part of each object in the `NetworkAdapter` array. Specify the device ID of the network adapter, which must be no more than 1,024 characters.
Name	string	Optional	This item is part of each object in the `NetworkAdapter` array. Specify the name of the network adapter, which must be no more than 1,024 characters.

NetworkAdapterConfigurationList object

Item name		Data type	Mandatory / Optional	Description
NetworkAdapterConfiguration		Array	Mandatory	Array whose elements consist of one or more objects representing network adapter configuration information. You have to specify 1 to 255 objects for this array.
DefaultIPGatewayList		Object	Optional	Object that puts together default gateway information.
DefaultIPGateway		Array	Mandatory	Array whose element consists of one object representing default gateway information. You have to specify 1 object for this array.
	_value	string	Mandatory	This item is part of an object in the `DefaultIPGateway` array. Specify the default gateway, which must be no more than 39 characters.
	@Index	int	Mandatory	This item is part of an object in the `DefaultIPGateway` array. Specify an index for the default gateway information. Specify a serial number starting with 1.
DHCPEnabled		string	Optional	Whether DHCP is enabled or disabled. Specify one of the following: • `0`: DHCP disabled • `1`: DHCP enabled
DHCPLeaseExpires		dateTime	Optional	Specify the date and time when the DHCP lease expires.
DHCPLeaseObtained		dateTime	Optional	Specify the date and time when the DHCP lease was obtained.

Item name		Data type	Mandatory / Optional	Description
DHCPServer		string	Optional	Specify the address of the DHCP server, which must be no more than 39 characters.
DNSServerSearchOrderList		Object	Optional	Object that puts together DNS server information.
DNSServerSearchOrder		Array	Mandatory	Array whose elements consist of one or more objects representing DNS server information. You have to specify 1 to 255 objects for this array.
	_value	string	Mandatory	This item is part of each object in the `DNSServerSearchOrder` array. Specify the address of the DNS server, which must be no more than 39 characters.
	@Index	int	Mandatory	This item is part of each object in the `DNSServerSearchOrder` array. Specify an index for the DNS server. Specify a serial number starting with 1.
Index		unsignedInt	Mandatory	Specify the setting ID of network adapter configuration information.
IPAddressList		Object	Optional	Object that puts together IP address information.
IPAddress		Array	Mandatory	Array whose elements consist of one or more objects representing IP address information. You have to specify 1 to 255 objects for this array.
	_value	string	Mandatory	This item is part of each object in the `IPAddress` array. Specify the IP address in IPv4 format, where the first element of the `IPAddress` array inside the first obeject of the `NetworkAdapterConfiguration` arrray.
	@Index	int	Mandatory	This item is part of each object in the `IPAddress` array. Specify an index for the IP address. Specify a serial number starting with 1.
IPSubnetList		Object	Optional	Object that puts together subnet mask information.
IPSubnet		Array	Mandatory	Array whose elements consist of one or more objects representing subnet mask information. You have to specify 1 to 255 objects for this array.
	_value	string	Mandatory	This item is part of each object in the `IPSubnet` array. Specify the subnet mask, which must be no more than 39 characters.
	@Index	int	Mandatory	This item is part of each object in the `IPSubnet` array. Specify an index for the subnet mask. Specify a serial number starting with 1.
MACAddress		string	Optional	Specify a 17-character long MAC address in the following format: *xx*:*xx*:*xx*:*xx*:*xx*:*xx* *x*: One of the characters in the range from 0 to 9 and a to f.
WINSPrimaryServer		string	Optional	Specify the address of the primary WINS server, which must be no more than 39 characters.
WINSSecondaryServer		string	Optional	Specify the address of the secondary WINS server, which must be no more than 39 characters.

NetworkAdapterToNetworkAdapterConfigurationList object

Item name	Data type	Mandatory / Optional	Description
NetworkAdapterToNetworkAdapterConfiguration	Array	Mandatory	Array whose elements consist of one or more objects representing information that associates network adapter information with network adapter configuration information. You have to specify 1 to 255 objects for this array.
NetworkAdapterDeviceID	string	Mandatory	This item is part of each object in the `NetworkAdapterToNetworkAdapterConfiguration` array. Specify the device ID of the network adapter, which must be no more than 1,024 characters.
NetworkAdapterConfigurationIndex	unsignedInt	Mandatory	This item is part of each object in the `NetworkAdapterToNetworkAdapterConfiguration` array. Specify the setting ID of the network adapter configuration corresponding to the device ID of the network adapter specified in NetworkAdapterDeviceID.

OperatingSystem object

Item name	Data type	Mandatory / Optional	Description
OSKind	int	Optional	OS type. Specify one of the following: • `0`: Unknown • `1`: Windows • `2`: Linux • `3`: UNIX • `4`: Mac OS • `5`: OS for smart devices • `6`: HP-UX • `7`: Solaris • `8`: AIX
Caption	string	Optional	Specify the name of the OS. See the *List of OS names*, and specify one of the names in the "OS" column.
KernelVersion	string	Optional	Specify the Linux kernel version, which must be no more than 64 characters.
CSDVersion	string	Optional	See the "Service pack or OS version" column in the *List of OS names*, and specify as follows: In the case of a service pack: Specify a service pack in the following format: `Service△Pack△N` (where *N* denotes the service pack number). △ denotes a single-byte space. Example: `Service Pack 3` In the case of an OS version: Specify an OS version. Example: `1803`
Description	string	Optional	Specify the description of the computer, which must be no more than 1,024 characters.
Locale	int	Optional	Specify a locale code. Specify one of the following: • 1 Arabic • 4 Chinese (Simplified) - China

Item name	Data type	Mandatory / Optional	Description
Locale	int	Optional	• 9 English • 1025 Arabic - Saudi Arabia • 1026 Bulgarian • 1027 Catalan • 1028 Chinese (Traditional) - Taiwan • 1029 Czech • 1030 Danish • 1031 German - Germany • 1032 Greek • 1033 English - United States • 1034 Spanish - Traditional Sort • 1035 Finnish 1036 French - France • 1037 Hebrew • 1038 Hungarian • 1039 Icelandic • 1040 Italian - Italy • 1041 Japanese • 1042 Korean • 1043 Dutch - Netherlands • 1044 Norwegian - Bokmal • 1045 Polish • 1046 Portuguese - Brazil • 1047 Rhaeto-Romanic • 1048 Romanian • 1049 Russian • 1050 Croatian • 1051 Slovak • 1052 Albanian • 1053 Swedish • 1054 Thai • 1055 Turkish • 1056 Urdu • 1057 Indonesian • 1058 Ukrainian • 1059 Belarusian • 1060 Slovenian • 1061 Estonian • 1062 Latvian • 1063 Lithuanian • 1065 Persian • 1066 Vietnamese • 1069 Basque • 1070 Serbian • 1071 Macedonian (F.Y.R.O. Macedonia) • 1072 Sutu • 1073 Tsonga • 1074 Tswana • 1076 Xhosa • 1077 Zulu • 1078 Afrikaans • 1080 Faeroese

Item name	Data type	Mandatory / Optional	Description
Locale	int	Optional	• 1081 Hindi • 1082 Maltese • 1084 Gaelic • 1085 Yiddish • 1086 Malay - Malaysia • 2049 Arabic - Iraq • 2052 Chinese (Simplified) - PRC • 2055 German - Switzerland • 2057 English - United Kingdom • 2058 Spanish - Mexico • 2060 French - Belgium • 2064 Italian - Switzerland • 2067 Dutch - Belgium • 2068 Norwegian - Nynorsk • 2070 Portuguese - Portugal • 2072 Romanian - Moldova • 2073 Russian - Moldova • 2074 Serbian - Latin • 2077 Swedish - Finland • 3073 Arabic - Egypt • 3076 Chinese (Traditional) - Hong Kong SAR • 3079 German - Austria • 3081 English - Australia • 3082 Spanish - International Sort • 3084 French - Canada • 3098 Serbian - Cyrillic • 4097 Arabic - Libya • 4100 Chinese (Simplified) - Singapore • 4103 German - Luxembourg • 4105 English - Canada • 4106 Spanish - Guatemala • 4108 French - Switzerland • 5121 Arabic - Algeria • 5127 German - Liechtenstein • 5129 English - New Zealand • 5130 Spanish - Costa Rica • 5132 French - Luxembourg • 6145 Arabic - Morocco • 6153 English - Ireland • 6154 Spanish - Panama • 7169 Arabic - Tunisia • 7177 English - South Africa • 7178 Spanish - Dominican Republic • 8193 Arabic - Oman • 8201 English - Jamaica • 8202 Spanish - Venezuela • 9217 Arabic - Yemen • 9226 Spanish - Colombia • 10241 Arabic - Syria • 10249 English - Belize • 10250 Spanish - Peru

Item name	Data type	Mandatory / Optional	Description
Locale	int	Optional	• 11265 Arabic - Jordan • 11273 English - Trinidad • 11274 Spanish - Argentina • 12289 Arabic - Lebanon • 12298 Spanish - Ecuador • 13313 Arabic - Kuwait • 13322 Spanish - Chile • 14337 Arabic - U.A.E. • 14346 Spanish - Uruguay • 15361 Arabic - Bahrain • 15370 Spanish - Paraguay • 16385 Arabic - Qatar • 16394 Spanish - Bolivia • 17418 Spanish - El Salvador • 18442 Spanish - Honduras • 19466 Spanish - Nicaragua • 20490 Spanish - Puerto Rico
Organization	string	Optional	Specify the company name, which must be no more than 1,024 characters.
OSCode	string	Optional	Specify an OS code. See the *List of OS names*, and specify one of the codes in the "OS code" column.
OSLanguage	int	Optional	Specify an OS language code. Specify one of the codes listed for *Locale* in the *Description* column.
RegisteredUser	string	Optional	Specify the owner name, which must be no more than 1,024 characters.
SerialNumber	string	Optional	Specify the serial number of the OS, which must be no more than 1,024 characters.
TotalVirtualMemorySize	unsignedLong	Optional	Specify the amount of virtual memory in bytes.

List of OS names

OS	CPU	OS code	Service pack or OS version
Microsoft Windows XP Home Edition	32bit	1.5.1.768.0.0.0	Service pack
Microsoft Windows XP Professional	32bit	1.5.1.256.0.0.0	Service pack
Microsoft(R) Windows(R) Server 2003, Enterprise Edition	32bit	1.5.2.274.1.0.0	Service pack
Microsoft(R) Windows(R) Server 2003, Standard Edition	32bit	1.5.2.272.1.0.0	Service pack
Microsoft(R) Windows(R) Server 2003, Enterprise x64 Edition	64bit	1.5.2.274.1.0.9	Service pack
Microsoft(R) Windows(R) Server 2003, Standard x64 Edition	64bit	1.5.2.272.1.0.9	Service pack
Microsoft(R) Windows Vista™ Business	32bit	1.6.0.6.0.0.0	Service pack
Microsoft(R) Windows Vista™ Enterprise	32bit	1.6.0.4.0.0.0	Service pack
Microsoft(R) Windows Vista™ Ultimate	32bit	1.6.0.1.0.0.0	Service pack

OS	CPU	OS code	Service pack or OS version
Microsoft(R) Windows Server(R) 2008 Standard	32bit	1.6.0.7.1.0.0	Service pack
Microsoft(R) Windows Server(R) 2008 Enterprise	32bit	1.6.0.10.1.0.0	Service pack
Microsoft(R) Windows(R) Server 2003 R2, Standard Edition	32bit	1.5.2.272.1.1.0	Service pack
Microsoft(R) Windows(R) Server 2003 R2, Enterprise Edition	32bit	1.5.2.274.1.1.0	Service pack
Microsoft(R) Windows(R) Server 2003 R2, Standard x64 Edition	64bit	1.5.2.272.1.1.9	Service pack
Microsoft(R) Windows(R) Server 2003 R2, Enterprise x64 Edition	64bit	1.5.2.274.1.1.9	Service pack
Microsoft(R) Windows Vista™ Home Basic	32bit	1.6.0.2.0.0.0	Service pack
Microsoft(R) Windows Vista™ Home Premium	32bit	1.6.0.3.0.0.0	Service pack
Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V	32bit	1.6.0.36.1.0.0	Service pack
Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V	32bit	1.6.0.38.1.0.0	Service pack
Microsoft Windows XP	--	1.5.1.-.0.-.-	Service pack
Microsoft(R) Windows(R) Server 2003	--	1.5.2.-.1.-.-	Service pack
Microsoft(R) Windows Vista™	--	1.6.0.-.0.-.-	Service pack
Microsoft(R) Windows Server(R) 2008	--	1.6.0.-.1.-.-	Service pack
Microsoft Windows	--	1.-.-.-.-.-.-	Service pack
Linux	--	2.-.-.-.-.-.-	Service pack
UNIX	--	3.-.-.-.-.-.-	Service pack
Mac OS	--	4.-.-.-.-.-.-	Service pack
Microsoft Windows 7 Starter	32bit	1.6.1.11.0.0.0	Service pack
Microsoft Windows 7 Home Premium	32bit	1.6.1.3.0.0.0	Service pack
Microsoft Windows 7 Professional	32bit	1.6.1.48.0.0.0	Service pack
Microsoft Windows 7 Enterprise	32bit	1.6.1.4.0.0.0	Service pack
Microsoft Windows 7 Ultimate	32bit	1.6.1.1.0.0.0	Service pack
Microsoft Windows 7 Edition / CPU unknown	--	1.6.1.-.0.-.-	Service pack
Microsoft Windows Server 2008 R2 Standard	64bit	1.6.1.7.1.0.9	Service pack
Microsoft Windows Server 2008 R2 Enterprise	64bit	1.6.1.10.1.0.9	Service pack
Microsoft Windows Server 2008 R2	64bit	1.6.1.-.1.-.-	Service pack
Microsoft(R) Windows Vista™ Home Basic	64bit	1.6.0.2.0.0.9	Service pack
Microsoft(R) Windows Vista™ Home Premium	64bit	1.6.0.3.0.0.9	Service pack
Microsoft(R) Windows Vista™ Business	64bit	1.6.0.6.0.0.9	Service pack
Microsoft(R) Windows Vista™ Enterprise	64bit	1.6.0.4.0.0.9	Service pack

OS	CPU	OS code	Service pack or OS version
Microsoft(R) Windows Vista™ Ultimate	64bit	1.6.0.1.0.0.9	Service pack
Microsoft(R) Windows Server(R) 2008 Standard	64bit	1.6.0.7.1.0.9	Service pack
Microsoft(R) Windows Server(R) 2008 Enterprise	64bit	1.6.0.10.1.0.9	Service pack
Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V	64bit	1.6.0.36.1.0.9	Service pack
Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V	64bit	1.6.0.38.1.0.9	Service pack
Microsoft Windows 7 Starter	64bit	1.6.1.11.0.0.9	Service pack
Microsoft Windows 7 Home Premium	64bit	1.6.1.3.0.0.9	Service pack
Microsoft Windows 7 Professional	64bit	1.6.1.48.0.0.9	Service pack
Microsoft Windows 7 Enterprise	64bit	1.6.1.4.0.0.9	Service pack
Microsoft Windows 7 Ultimate	64bit	1.6.1.1.0.0.9	Service pack
Microsoft(R) Windows Server(R) 2008 Datacenter	32bit	1.6.0.8.1.0.0	Service pack
Microsoft(R) Windows Server(R) 2008 Datacenter	64bit	1.6.0.8.1.0.9	Service pack
Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V	32bit	1.6.0.37.1.0.0	Service pack
Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V	64bit	1.6.0.37.1.0.9	Service pack
Microsoft Windows Server 2008 R2 Datacenter	64bit	1.6.1.8.1.0.9	Service pack
iOS	--	5.1.0.0.0.0.0	Service pack
Android	--	5.2.0.0.0.0.0	Service pack
Smart device	--	5.-.-.-.-.-.-	Service pack
Microsoft Windows 8	32bit	1.6.2.101.0.0.0	Service pack
Microsoft Windows 8	64bit	1.6.2.101.0.0.9	Service pack
Microsoft Windows 8 Pro	32bit	1.6.2.48.0.0.0	Service pack
Microsoft Windows 8 Pro	64bit	1.6.2.48.0.0.9	Service pack
Microsoft Windows 8 Enterprise	32bit	1.6.2.4.0.0.0	Service pack
Microsoft Windows 8 Enterprise	64bit	1.6.2.4.0.0.9	Service pack
Microsoft Windows 8 Edition / CPU unknown	--	1.6.2.-.0.-.-	Service pack
Microsoft Windows Server 2012 Standard	64bit	1.6.2.7.1.0.9	Service pack
Microsoft Windows Server 2012 Datacenter	64bit	1.6.2.8.1.0.9	Service pack
Microsoft Windows Server 2012 Edition unknown	--	1.6.2.-.1.-.-	Service pack
Microsoft Windows 7 Home Basic	32bit	1.6.1.2.0.0.0	Service pack
Microsoft Windows 7 Home Basic	64bit	1.6.1.2.0.0.9	Service pack
Microsoft Windows 8.1	32bit	1.6.3.101.0.0.0	Service pack
Microsoft Windows 8.1	64bit	1.6.3.101.0.0.9	Service pack

OS	CPU	OS code	Service pack or OS version
Microsoft Windows 8.1 Pro	32bit	1.6.3.48.0.0.0	Service pack
Microsoft Windows 8.1 Pro	64bit	1.6.3.48.0.0.9	Service pack
Microsoft Windows 8.1 Enterprise	32bit	1.6.3.4.0.0.0	Service pack
Microsoft Windows 8.1 Enterprise	64bit	1.6.3.4.0.0.9	Service pack
Microsoft Windows 8.1 Edition / CPU unknown	--	1.6.3.-.0.-.-	Service pack
Microsoft Windows Server 2012 R2 Standard	64bit	1.6.3.7.1.0.9	Service pack
Microsoft Windows Server 2012 R2 Datacenter	64bit	1.6.3.8.1.0.9	Service pack
Microsoft Windows Server 2012 R2 Edition unknown	--	1.6.3.-.1.-.-	Service pack
Microsoft Windows 10 Home	32bit	1.10.0.101.0.0.0	Service pack
Microsoft Windows 10 Home	64bit	1.10.0.101.0.0.9	Service pack
Microsoft Windows 10 Pro	32bit	1.10.0.48.0.0.0	Service pack
Microsoft Windows 10 Pro	64bit	1.10.0.48.0.0.9	Service pack
Microsoft Windows 10 Enterprise	32bit	1.10.0.4.0.0.0	Service pack
Microsoft Windows 10 Enterprise	64bit	1.10.0.4.0.0.9	Service pack
Microsoft Windows 10 Edition / CPU unknown	--	1.10.0.-.0.-.-	Service pack
HP-UX 11i V3 (IPF)	--	6.11.3.-.-.-.-	Service pack
HP-UX Version unknown	--	6.-.-.-.-.-.-	Service pack
Oracle Solaris 10 (SPARC)	--	7.10.-.-.-.-.-	Service pack
Oracle Solaris 11 (SPARC)	--	7.11.-.-.-.-.-	Service pack
Oracle Solaris (SPARC)	--	7.-.-.-.-.-.-	Service pack
AIX V6.1	--	8.6.1.-.-.-.-	Service pack
AIX V7.1	--	8.7.1.-.-.-.-	Service pack
AIX Version unknown	--	8.-.-.-.-.-.-	Service pack
Red Hat Enterprise Linux Server 6	--	2.6.-.1.-.-.-	Service pack
Red Hat Enterprise Linux Server 7	--	2.7.-.1.-.-.-	Service pack
Red Hat Enterprise Linux	--	2.-.-.1.-.-.-	Service pack
CentOS 6.1	--	2.6.-.2.-.-.-	Service pack
CentOS 7.1	--	2.7.-.2.-.-.-	Service pack
CentOS Version unknown	--	2.-.-.2.-.-.-	Service pack
Microsoft Windows 10 Enterprise LTSB	32bit	1.10.0.125.0.0.0	Service pack
AIX V7.2	--	8.7.2.-.-.-.-	Service pack
Microsoft Windows 10 Enterprise LTSB	64bit	1.10.0.125.0.0.9	Service pack
Microsoft Windows Server 2016 Standard	64bit	1.10.0.7.1.0.9	Service pack
Microsoft Windows Server 2016 Datacenter	64bit	1.10.0.8.1.0.9	Service pack
Microsoft Windows Server 2016	--	1.10.0.-.1.-.-	Service pack

OS	CPU	OS code	Service pack or OS version
OS X 10.10 Yosemite	--	4.10.10.-.-.-.-	Service pack
OS X 10.11 El Capitan	--	4.10.11.-.-.-.-	Service pack
macOS 10.12 Sierra	--	4.10.12.-.-.-.-	Service pack
Red Hat Enterprise Linux Server 5	--	2.5.-.1.-.-.-	Service pack
macOS High Sierra 10.13	--	4.10.13.-.-.-.-	Service pack
macOS Mojave 10.14	--	4.10.14.-.-.-.-	Service pack
Microsoft Windows 10 Pro for Workstations	32bit	1.10.0.161.0.0.0	OS version
Microsoft Windows 10 Pro for Workstations	64bit	1.10.0.161.0.0.9	OS version
Microsoft Windows Server 2019 Standard	64bit	1.10.17763.7.1.0.9	OS version
Microsoft Windows Server 2019 Datacenter	64bit	1.10.17763.8.1.0.9	OS version
Microsoft Windows Server 2019	--	1.10.17763.-.1.-.-	OS version
Microsoft Windows 10 Enterprise LTSC	32bit	1.10.0.125.0.0.0	OS version
Microsoft Windows 10 Pro N	32bit	1.10.0.49.0.0.0	OS version
Microsoft Windows 10 Pro N	64bit	1.10.0.49.0.0.9	OS version
Microsoft Windows 10 Enterprise N	32bit	1.10.0.27.0.0.0	OS version
Microsoft Windows 10 Enterprise N	64bit	1.10.0.27.0.0.9	OS version

Legend: --: Not applicable

PhysicalMemoryList object

Item name	Data type	Mandatory / Optional	Description
PhysicalMemory	Array	Mandatory	Array whose elements consist of one or more objects representing physical memory information. You have to specify 1 to 255 objects for this array.
Capacity	unsignedLong	Optional	This item is part of each object in the `PhysicalMemory` array. Specify the amount of physical memory inserted into the memory slot in bytes.

PointingDeviceList object

Item name	Data type	Mandatory / Optional	Description
PointingDevice	Array	Mandatory	Array whose elements consist of one or more objects representing mouse information. You have to specify 1 to 255 objects for this array.
Name	string	Optional	This item is part of each object in the `PointingDevice` array. Specify the name of the mouse, which must be no more than 1,024 characters.

PrinterList object

Item name	Data type	Mandatory / Optional	Description
Printer	Array	Mandatory	Array whose elements consist of one or more objects representing printer information. You have to specify 1 to 255 objects for this array.
Attributes	unsignedInt	Optional	This item is part of each object in the `Printer` array. Specify the attributes of the printer by using a combination of the following values: • 0x00000001: Queued • 0x00000002: Direct • 0x00000004: Default • 0x00000008: Shared • 0x00000010: Network • 0x00000020: Hidden • 0x00000040: Local • 0x00000080: EnableDevQ • 0x00000100: KeepPrintedJobs • 0x00000200: DoCompleteFirst • 0x00000400: WorkOffline • 0x00000800: EnableBIDI • 0x00001000: Allow only raw data type jobs to be spooled. • 0x00002000: Published
DriverName	string	Optional	This item is part of each object in the `Printer` array. Specify the driver name of the printer, which must be no more than 1,024 characters.
Name	string	Optional	This item is part of each object in the `Printer` array. Specify the printer name, which must be no more than 1,024 characters.
PortName	string	Optional	This item is part of each object in the `Printer` array. Specify the printer port, which must be no more than 1,024 characters.
ServerName	string	Optional	This item is part of each object in the `Printer` array. Specify the server name of the printer, which must be no more than 1,024 characters.
ShareName	string	Optional	This item is part of each object in the `Printer` array. Specify the share name of the printer, which must be no more than 1,024 characters.

ProcessorList object

Item name	Data type	Mandatory / Optional	Description
Processeor	Array	Mandatory	Array whose elements consist of one or more objects representing processor information. You have to specify 1 to 255 objects for this array.
Name	string	Optional	This item is part of each object in the `Processor` array. Specify the processor name, which must be no more than 1,024 characters.

SoundDeviceList object

Item name	Data type	Mandatory / Optional	Description
SoundDevice	Array	Mandatory	Array whose elements consist of one or more objects representing sound card information.

Item name	Data type	Mandatory / Optional	Description
SoundDevice	Array	Mandatory	You have to specify 1 to 255 objects for this array.
Manufacturer	string	Optional	This item is part of each object in the `SoundDevice` array. Specify the manufacturer of the sound card, which must be no more than 1,024 characters.
Name	string	Optional	This item is part of each object in the `SoundDevice` array. Specify the product name of the sound card, which must be no more than 1,024 characters.

UserAccount object

Item name	Data type	Mandatory / Optional	Description
Description	string	Optional	Specify user description, which must be no more than 1,024 characters.
FullName	string	Optional	Specify the full name of the user, which must be no more than 1,024 characters.

VideoControllerList object

Item name	Data type	Mandatory / Optional	Description
VideoController	Array	Mandatory	Array whose elements consist of one or more objects representing video controller information. You have to specify 1 to 255 objects for this array.
AdapterRAM	unsignedInt	Optional	This item is part of each object in the `VideoController` array. Specify the amount of video controller's VRAM in bytes.
Name	string	Optional	This item is part of each object in the `VideoController` array. Specify the video driver, which must be no more than 1,024 characters.
VideoProcessor	string	Optional	This item is part of each object in the `VideoController` array. Specify the video chip, which must be no more than 1,024 characters.

PowerManagement object

Item name	Data type	Mandatory / Optional	Description
VideoTimeoutAC	int	Optional	Specify Turn off monitor (AC) in seconds.
VideoTimeoutDC	int	Optional	Specify Turn off monitor (DC) in seconds.
SpindownTimeoutAC	int	Optional	Specify Turn off hard disks (AC) in seconds.
SpindownTimeoutDC	int	Optional	Specify Turn off hard disks (DC) in seconds.
StandbyTimeoutAC	int	Optional	Specify System standby (AC) in seconds.
StandbyTimeoutDC	int	Optional	Specify System standby (DC) in seconds.
HibernateTimeoutAC	int	Optional	Specify System hibernates (AC) in seconds.

Item name	Data type	Mandatory / Optional	Description
HibernateTimeoutDC	int	Optional	Specify System hibernates (DC) in seconds.
ThrottlePolicyAC	int	Optional	Specify Processor Throttle (AC) in seconds.
ThrottlePolicyDC	int	Optional	Specify Processor Throttle (DC) in seconds.

property array

Item name	Data type	Mandatory / Optional	Description
@category	string	Optional	This item is part of each object in the `property` array. Specify one of the following strings as the category name. For details, see *Combinations of generic inventories*. • prtMarker • prtMarkerSupplies • prtInput
@key	string	Optional	This item is part of each object in the `property` array. Specify one of the following as the key. For details, see *Combinations of generic inventories*. • prtMarkerMarkTech • prtMarkerProcessColorants • prtMarkerSuppliesType • prtMarkerSuppliesDescription • prtMarkerSuppliesLevel • prtInputType • prtInputName • prtInputCurrentLevel
@value	string	Optional	This item is part of each object in the `property` array. Specify a value corresponding to the key. For details, see *Combinations of generic inventories*.
@record	string	Optional	This item is part of each object in the `property` array. Specify a number that distinguishes the category. For details, see *Combinations of generic inventories*.

Combinations of generic inventories

@category	@key	Description of category / key	Data type of @value	Description of @value
prtMarker	prtMarkerMarkTech	Printing method - Method	int	Specify one of the followings: • other(1) Other • unknown(2) Unknown • electrophotographicLED(3) Laser printer • electrophotographicLaser(4) Laser printer • electrophotographicOther(5) Laser printer • impactMovingHeadDotMatrix9pin(6) Dot-matrix printer • impactMovingHeadDotMatrix24pin(7) Dot-matrix printer • impactMovingHeadDotMatrixOther(8) Dot-matrix printer

@category	@key	Description of category / key	Data type of @value	Description of @value
prtMarker	prtMarkerMarkTech	Printing method - Method	int	• impactMovingHeadFullyFormed(9) Dot-matrix printer • impactBand(10) Other • impactOther(11) Other • inkjetAqueous(12) Ink-jet printer • inkjetSolid(13) Ink-jet printer • inkjetOther(14) Ink-jet printer • pen(15) Pen • thermalTransfer(16) Thermal printer • thermalDiffusion(18) Thermal printer • thermalOther(19) Thermal printer • electroerosion(20) Other • electrostatic(21) Other • photographicMicrofiche(22) Other • photographicImagesetter(23) Other • photographicOther(24) Other • ionDeposition(25) Other • eBeam(26) Other • typesetter(27) Other
	prtMarkerProcessColorants	Printing method - Number of colors	int	Specify a value in the range from 0 to 65535.
prtMarkerSupplies	prtMarkerSuppliesType	Supplies - Type	int	Specify one of the following as the type of the consumable, package, or the like: • toner(3) • ink(5) • inkCartridge(6) • inkRibbon(7) • Other
	prtMarkerSuppliesDescription	Supplies - Description	string	Specify the description of the container or package of the consumable.
	prtMarkerSuppliesLevel	Supplies - State	int	Specify the current level when the consumable is a container, or the remaining space when the consumable is a package. Specify a value (%) in the range from 1 to 100. • 0 to 100: Current level or remaining space (%) • -1: Unknown • -2: Unknown • -3: This item is consumed to some extent, or there is some remaining space.
prtInput	prtInputType	Paper feed tray - Type	int	Specify one of the following values as the type of technology (which is mainly identified by the type of paper feed mechanism) adopted by a specific component: • sheetFeedAutoRemovableTray(3) • sheetFeedAutoNonRemovableTray(4) • sheetFeedManual(5) • continuousRoll(6) • continuousFanFold(7)
	prtInputName	Paper feed tray - Name	string	Specify the name of the paper feed tray.

@category	@key	Description of category / key	Data type of @value	Description of @value
prtInput	prtInputCurrentLevel	Paper feed tray - Capacity	int	The current capacity of the Input subunit, shown in capacity units of the Input subunit. Specify the remaining capacity (%) as the value to be displayed. • 0 to 100: Remaining capacity (%) • -1: Unknown • -2: Unknown • -3: At least 1 unit is remaining.

SmartDeviceInformation object

Item name		Data type	Mandatory / Optional	Description
UUID		string	Optional	Specify the device identifier, which must be no more than 256 characters.
IMEI		string	Optional	Specify the International Mobile Equipment Identifier (IMEI), which must be no more than 64 characters.
UDID		string	Optional	Specify the identifier of the iOS terminal, which must be no more than 128 characters.
ICCID		string	Optional	Specify the ICCID, which must be no more than 64 characters.
IMSI		string	Optional	Specify the International Mobile Subscriber Identity assigned to the SIM card inserted into the device, which must be no more than 64 characters.
PhoneNumber		string	Optional	Specify the mobile number, which must be no more than 256 characters.
mail		string	Optional	Specify the email address, which must be no more than 256 characters.
Carrier		string	Optional	Specify the carrier, which must be no more than 512 characters.
PasscodeSetting		string	Optional	Specify one of the following values as the passcode setting status: • true: Passcode set • false: Passcode not set
PhisicalMemory		Object	Optional	Object name of RAM information.
	Size	unsignedLong	Optional	Specify the amount of RAM in bytes.
	FreeSpace	unsignedLong	Optional	Specify the free RAM space in bytes.
Storage		Object	Optional	Object name of internal storage information.
	Size	unsignedLong	Optional	Specify the amount of internal storage in bytes.
	FreeSpace	unsignedLong	Optional	Specify the free internal storage space in bytes.
Media		Object	Optional	Object name of external media information.
	Size	unsignedLong	Optional	Specify the size of external media in bytes.
	FreeSpace	unsignedLong	Optional	Specify the free space on the external media in bytes.

InstalledSoftware object

Item name	Data type	Mandatory / Optional	Description
@ReportType	string	Mandatory	Always specify `ALL`.
@LastUpdateTime	dateTime	Mandatory	Specify the date and time when the `InstalledSoftware` object was generated.
SoftwareList	Object	Optional	Object that puts together software information. For details, see *SoftwareList object of the InstalledSoftware object*.

SoftwareList object of the InstalledSoftware object

Item name	Data type	Mandatory / Optional	Description
Software	Array	Mandatory	Array whose elements consist of one or more objects representing software information. Specify 1 to 500 objects for this array.
@Type	string	Optional	This item is part of each object in the `Software` array. Specify one of the following values as the software type: • InstalledSoftware: Installed software • UpdateProgram: Update If you omit this item, it is assumed that `InstalledSoftware` is specified.
SourceID	string	Mandatory	This item is part of each object in the `Software` array. Specify the ID that uniquely identifies the software, which must be no more than 512 characters. Specify the software name.
InstallPath	string	Optional	This item is part of each object in the `Software` array. Specify the path to the location to which to install the software, which must be no more than 512 characters.
Name	string	Mandatory	This item is part of each object in the `Software` array. Specify the software name, which must be no more than 512 characters.
Version	string	Optional	This item is part of each object in the `Software` array. Specify the software version, which must be no more than 128 characters.
Publisher	string	Optional	This item is part of each object in the `Software` array. Specify the publisher of the software, which must be no more than 128 characters.
InstallDate	dateTime	Optional	This item is part of each object in the `Software` array. Specify the date when the software was installed.
HelpLink	string	Optional	This item is part of each object in the `Software` array. Specify the URL of the support page for the software, which must be no more than 512 characters.
AppType	int	Optional	This item is part of each object in the `Software` array. Specify one of the following values as the application type of the software: • 0: Software other than Windows Store applications • 1: Windows store application If you omit this item, it is assumed that `0` is set.

Update object

Item name	Data type	Mandatory / Optional	Description
@ReportType	string	Mandatory	Always specify `ALL`.
@LastUpdateTime	dateTime	Mandatory	Specify the date and time when the `Update` object was generated.
SoftwareList	Object	Mandatory	Object that puts together update information. For details, see *SoftwareList object of the Update object*.

SoftwareList object of the Update object

Item name	Data type	Mandatory / Optional	Description
Software	Array	Mandatory	Array whose elements consist of one or more objects representing update information. Specify 1 to 500 objects for this array.
HotFixID	string	Mandatory	This item is part of each object in the `Software` array. Specify the knowledge base number (KB number) of the update. Specify the KB number in one of the following formats: • Uppercase `KB` + at least 6-digit sequential number (hotfix ID) • Uppercase `KB` + at least 6-digit sequential number (hotfix ID) + `-v` + at least 1-digit sequential number (update version)
Description	string	Optional	This item is part of each object in the `Software` array. Specify the description of the update, which must be no more than 512 characters.
InstallDate	dateTime	Optional	This item is part of each object in the `Software` array. Specify the date when the update was installed.
Type	string	Optional	This item is part of each object in the `Software` array. Specify one of the following values as the type of update: • Update: Regular update • Rollup: Rollup update When this item is omitted, it is assumed that `Update` is set.

SecurityInventory object

Item name	Data type	Mandatory / Optional	Description
@LastUpdateTime	dateTime	Mandatory	Specify the date and time when the `SecurityInventory` object was generated.
AccountList	Object	Optional	Object that puts together account information. For details, see *AccountList object*.
PowerOnPassword	string	Mandatory	Power-on password status. Specify one of the following: • `PowerOnPasswordDisabled`: Disabled • `PowerOnPasswordEnabled`: Enabled • `PowerOnPasswordNotImplemented`: Not implemented • `PowerOnPasswordUnknown`: Unknown
GuestAccount	string	Mandatory	Guest account status. Specify one of the following: • `GuestAccountNone`: None of guest account • `GuestAccountDisabled`: Guest account is disabled • `GuestAccountEnabled`: Guest account is enabled • `GuestAccountUnknown`: Unknown

Item name	Data type	Mandatory / Optional	Description
AutoLogon	string	Mandatory	Whether automatic logon is enabled. Specify one of the following: • `AutoLogonDisabled`: Disabled • `AutoLogonEnabled`: Enabled • `AutoLogonUnknown`: Unknown
SharedDirectory	string	Mandatory	Availability of shared folders. Specify one of the following: • `SharedDirectoryNotFound`: No shared folder • `SharedDirectoryFound`: Shared folders available • `SharedDirectoryUnknown`: Unknown
AutoShareServer	string	Mandatory	State of an administrative share. Specify one of the following: • `AutoShareServerFalse`: Automatic creation of a share is disabled. • `AutoShareServerTrue`: Automatic creation of a share is enabled. • `AutoShareServerUnknown`: Unknown
DCOM	string	Mandatory	DCOM status. Specify one of the following: • `DCOMDisabled`: Disabled • `DCOMEnabled`: Enabled • `DCOMUnknown`: Unknown
RestrictAnonymous	string	Mandatory	Whether the collection of information through anonymous connections is restricted. Specify one of the following: • `RestrictAnonymousDisabled`: Anonymous connections are not restricted. • `RestrictAnonymousEnabled`: Anonymous connections are restricted. • `RestrictAnonymousUnknown`: Unknown
WindowsFirewall	string	Mandatory	Whether Windows Firewall is enabled. Specify one of the following: • `WindowsFirewallDisabled`: Disabled • `WindowsFirewallEnabled`: Enabled • `WindowsFirewallNotImplemented`: Not implemented • `WindowsFirewallUnknown`: Unknown
WindowsUpdate	string	Mandatory	Whether Windows automatic update is enabled. Specify one of the following: • `WindowsUpdateDisabled`: Disabled • `WindowsUpdateEnabled`: Enabled • `WindowsUpdateUnknown`: Unknown
DenyTSConnections	string	Mandatory	State of Remote Desktop. Specify one of the following: • `DenyTSConnectionsFalse`: Allowed • `DenyTSConnectionsTrue`: Denied • `DenyTSConnectionsNotImplemented`: Not implemented • `DenyTSConnectionsUnknown`: Unknown

AccountList object

Item name	Data type	Mandatory / Optional	Description
Account	Array	Mandatory	Array whose elements consist of one or more objects representing account information.

Item name	Data type	Mandatory / Optional	Description
Account	Array	Mandatory	Specify 1 to 500 objects for this array.
Name	string	Mandatory	This item is part of each object in the `Account` array. Specify the account name, which must be no more than 1,024 characters.
LastPasswordModifiedDate	dateTime	Optional	This item is part of each object in the `Account` array. Specify the last date and time when the password was modified.
WeakPassword	string	Optional	This item is part of each object in the `Account` array. Specify one of the following values as the password vulnerability check result: • `WeakPasswordFalse`: The password is secure. • `WeakPasswordTrue`: The password is vulnerable. • `WeakPasswordUnknown`: Unknown
UnexpirePassword	string	Optional	This item is part of each object in the `Account` array. Specify one of the following values to enable or disable Unexpire Password: • `UnexpirePasswordFalse`: Unexpire Password is disabled. • `UnexpirePasswordTrue`: Unexpire Password is enabled. • `UnexpirePasswordUnknown`: Unknown
ScreenSaverEnabled	string	Optional	This item is part of each object in the `Account` array. Specify one of the following values to enable or disable the screen saver: • `ScreenSaverEnabledFalse`: Screen saver disabled • `ScreenSaverEnabledTrue`: Screen saver enabled • `ScreenSaverEnabledUnknown`: Unknown
ScreenSaverIsSecure	string	Optional	This item is part of each object in the `Account` array. Specify one of the following values to enable or disable the screen saver password: • `ScreenSaverIsSecureFalse`: Password protection disabled • `ScreenSaverIsSecureTrue`: Password protection enabled
ScreenSaverTimeout	int	Optional	This item is part of each object in the `Account` array. Specify the wait time to launch the screen saver in seconds. If the screen saver is disabled, specify `0`.

ExtendInventory object

Item name	Data type	Mandatory / Optional	Description
@LastUpdateTime	dateTime	Mandatory	Specify the date and time when the `ExtendInventory` object was generated.
ExtendInventoryList	Object	Optional	Object that puts together common management fields of asset information and device information, and additional management fields of hardware asset information. For details, see *ExtendInventoryList object*.

ExtendInventoryList object

Item name	Data type	Mandatory / Optional	Description
ExtendInventoryItem	Array	Mandatory	Array whose elements consist of one or more objects representing common management fields of asset information and device information, and additional management fields of hardware asset information.

Item name	Data type	Mandatory / Optional	Description
ExtendInventoryItem	Array	Mandatory	Specify 1 to 221 objects for this array.
@InformationType	string	Mandatory	This item is part of each object in the `ExtendInventoryItem` array. Specify the information type. Specify one of the following values that is appropriate to the items of the common management fields and the additional management fields: Common management field `Organization`: Organization `Location`: Location `UserName`: User name `Account`: Account `Mail`: email address `Phone`: Phone number Additional management field `other` If there are no items which checked **Entering item is mandatory** in the setting asset field or a value of the asset field item which checked **Entering item is mandatory** is empty, it becomes an error.
ItemName	string	Optional	This item is part of each object in the `ExtendInventoryItem` array. Specify this item only when `other` is specified as `@InformationType`. Specify the name of the asset field within 256 characters. When the multiple-language definition is set for the item of the additional management field, specify the item name in the default language. If you omit this item when `other` is specified as `@InformationType`, or if you specify a value that is not included in the definition, the value is judged as being in violation of restrictions.
Value	string	Optional	This item is part of each object in the `ExtendInventoryItem` array. Specify this item when **Type** is **Text**, **Number**, or **Date** in the setting asset field. When specify an empty value, use `""`. When common management fields are either text type or number type, specify the default display values for text-type input items. When common management fields are date type, just specify the date in local time. If the specified value is in violation of the restrictions on entered characters defined in the Asset Field Definitions view, the value is judged as being in violation of restrictions. The Information type is **Department** or **Location**, specify `"/"` as a hierarchy. The maximum of the hierarchy is 40. Do not specify `"/"` consecutively such as `"//"`.
ValueList	Object	Optional	This item is part of each object in the `ExtendInventoryItem` array. Specify this item when **Type** is **Enumeration** in the setting asset field. This object puts together the items whose entry is selected from a list.
Value	string	Mandatory	Specify the values of the item whose entry is selected item. When the multiple-language definition is set, specify the values in the default language.

Item name		Data type	Mandatory / Optional	Description
	Value	string	Mandatory	When you specify the value which is not defined at select values, works as follows: When the Information type is **Department** or **Location**: Registered as a select value. Except the above: The value is judged as being in violation of restrictions. When specify an empty value, use `""`. The Information type is **Department** or **Location**, specify `"/"` as a hierarchy. The maximum of the hierarchy is 40. Do not specify `"/"` consecutively such as `"//"`.
ValueTree		Object	Optional	This item is part of each object in the `ExtendInventoryItem` array. Specify this item when **Type** is **Hierarchy** in the setting asset field. This object puts together the items whose entry is selected from a tree.
	Value	Object	Mandatory	Object representing the item whose entry is selected from a tree. Specify the item value in the `Data` member of the object.
	Data	string	Mandatory	This item is part of the `Value` object. Specify the value of the item whose entry is selected from a tree, which must be no more than 256 characters. If you specify a value that is not present in the item hierarchy definition (department, installation location), that value is registered anyway. The maximum of the hierarchy is 40. Do not use `"/"` character. When specify an empty value, the value of the first level is `""`.
	Value	Object	Optional	This item is part of the `Value` object. To specify a child item in the tree, nest one `Value` object inside another Value object. For example, if there are three levels (`X/Y/Z`), specify as follows: `"ValueTree" : { "Value": { "Data": "X", "Value": { "Data": "Y", "Value": { "Data": "Z" } } } }` You can specify until 510 characters including the hierarchy separate character `"/"`.

Response format

Status line

Either a status code or its text is returned. For details, see the description of status codes in 20.2 Common API specifications.

Response header

For details, see the description of the response format in 20.2 Common API specifications.

Response message body

The response does not have a message body when the request has been successful. When an error occurs, error information is stored in JSON format. For details, see the description of the error information in 20.2 Common API specifications.

Example usage


```
{
  "Device-Inventory":[
    {
      "Report": {
        "@CreationDate":"2017-04-13T15:45:15.000Z",
        "@Version":"0250",
        "ID":"1234567890",
        "Agent": {
          "Type":"REST",
          "DeviceStatus":"0",
          "Status":"0",
          "DistributionStatus":"0",
          "DiscoveryProtocol":"7"
        },
        "Inventory": {
          "Equipment": {
            "Type":"EquipmentTypeComputer"
          },
          "SystemInventory": {
            "@LastUpdateTime":"2018-04-04T11:35:08.000Z",
            "BaseBoard": {
              "SerialNumber":"JPXXXXXXXX"
            },
            "BIOS": {
              "Manufacturer":"XXXXXXXX",
              "Name":"Default System BIOS",
              "ReleaseDate":"2009-10-22T00:00:00.000Z",
              "SerialNumber":"JPXXXXXXXX",
              "SMBIOSBIOSVersion":"786G7 v01.02",
              "Version":"HPQOEM - 20091022"
            },
            "CDROMDriveList": {
              "CDROMDrive": [
                {
                  "Name":"XXXXXXXX DVDRAM XXXXXXXX ATA Device"
                }
              ]
            },
            "ComputerSystem": {
              "CurrentTimeZone":"540",
              "Domain":"WORKGROUP",
              "DomainRole":"DomainRoleStandaloneWorkstation",
              "Manufacturer":"XXXXXXXX",
              "Model":"XXXXXXXX XXXXXXXX PC",
              "Name":"JSS53445",
              "NumberOfProcessors":"2",
              "TotalPhysicalMemory":"4294967296",
```

```
    "UserName":"JSS53445\\hitachi"
  },
  "ComputerSystemProduct": {
    "IdentifyingNumber":"XXXXXXXX",
    "UUID":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
  },
  "DesktopMonitorList": {
    "DesktopMonitor": [
      {
        "Name":"Monitor"
      }
    ]
  },
  "DiskDriveList": {
    "DiskDrive": [
      {
        "DeviceID":"\\\\.\\PHYSICALDRIVE0",
        "InterfaceType":"IDE",
        "Model":"XXXXXXXX XXXXXXXX ATA Device",
        "Size":"500105249280"
      }
    ]
  },
  "KeyboardList": {
    "Keyboard": [
      {
        "Description":"HID Keyboard Device"
      }
    ]
  },
  "LogicalDiskList": {
    "LogicalDisk": [
      {
        "DeviceID":"C:",
        "DriveType":"DriveTypeLocalDisk",
        "FileSystem":"NTFS",
        "FreeSpace":"15716945920",
        "Size":"42952409088"
      }
    ]
  },
  "DiskDriveToLogicalDiskList": {
    "DiskDriveToLogicalDisk": [
      {
        "DiskDriveDeviceID":"\\\\.\\PHYSICALDRIVE0",
        "LogicalDiskDeviceID":"C:"
      }
    ]
  },
  "BitLocker": {
    "DriveList": {
      "Drive": [
        {
          "DriveLetter":"C:",
          "ProtectionStatus":"0",
          "LockStatus":"0"
        }
      ]
```

```
    }
  },
  "NetworkAdapterList": {
    "NetworkAdapter": [
      {
        "DeviceID":"7",
        "Name":"XXXXXXXX Gigabit Network Connection"
      }
    ]
  },
  "NetworkAdapterConfigurationList": {
    "NetworkAdapterConfiguration": [
      {
        "DefaultIPGatewayList": {
          "DefaultIPGateway": [
            {
              "_value":"10.208.152.1",
              "@Index":"1"
            }
          ]
        },
        "DHCPEnabled":"0",
        "DNSServerSearchOrderList": {
          "DNSServerSearchOrder": [
            {
              "_value":"172.16.0.152",
              "@Index":"1"
            },
            {
              "_value":"172.16.228.126",
              "@Index":"2"
            }
          ]
        },
        "Index":"7",
        "IPAddressList": {
          "IPAddress": [
            {
              "_value":"10.208.152.21",
              "@Index":"1"
            }
          ]
        },
        "IPSubnetList": {
          "IPSubnet": [
            {
              "_value":"255.255.255.0",
              "@Index":"1"
            }
          ]
        },
        "MACAddress":"XX:XX:XX:XX:XX:XX"
      }
    ]
  },
  "NetworkAdapterToNetworkAdapterConfigurationList": {
    "NetworkAdapterToNetworkAdapterConfiguration": [
      {
```

```
        "NetworkAdapterDeviceID":"7",
        "NetworkAdapterConfigurationIndex":"7"
      }
    ]
  },
  "HostName":"JSS53445",
  "OperatingSystem": {
    "OSKind":"1",
    "Caption":"Microsoft Windows 7 Professional",
    "KernelVersion":"Kernel Version",
    "CSDVersion":"Service Pack 3",
    "Description":"Description of this computer",
    "Locale":"1041",
    "Organization":"Hitachi, Ltd.",
    "OSCode":"1.6.1.48.0.0.9",
    "OSLanguage":"1041",
    "RegisteredUser":"Bob Brown",
    "SerialNumber":"XXXXX-XXX-XXXXXXX-XXXXX",
    "TotalVirtualMemorySize":"8368304128"
  },
  "PhysicalMemoryList": {
    "PhysicalMemory": [
      {
        "Capacity":"2147483648"
      }
    ]
  },
  "PointingDeviceList": {
    "PointingDevice": [
      {
        "Name":"Name of mouse #1"
      }
    ]
  },
  "PrinterList": {
    "Printer": [
      {
        "Attributes":"580",
        "DriverName":"XXXXXXXX XXXXXXXX XXXXXXXX",
        "Name":"XXXXXXXX XXXXXXXX XXXXXXXX",
        "PortName":"XXXPort:",
        "ServerName":"Printer Server Name",
        "ShareName":"Shared Printer Name"
      }
    ]
  },
  "ProcessorList": {
    "Processor": [
      {
        "Name":"XXXXXXXX XXXXXXXX XXXXXXXX CPU @ 3.40GHz"
      },
      {
        "Name":"XXXXXXXX XXXXXXXX XXXXXXXX CPU @ 3.40GHz"
      }
    ]
  },
  "SoundDeviceList": {
    "SoundDevice": [
```

```
      {
        "Manufacturer":"XXXXXXXX",
        "Name":"High Definition Audio device"
      }
    ]
  },
  "UserAccount": {
    "Description":"Sample Description",
    "FullName":"Bob Brown"
  },
  "VideoControllerList": {
    "VideoController": [
      {
        "AdapterRAM":"1857681408",
        "Name":"XXXXXXXX XXXXXXXX XXXXXXXX (XXXXXXXX 1.1)",
        "VideoProcessor":"XXXXXXXX XXXXXXXX XXXXXXXX"
      }
    ]
  },
  "AMTFirmwareVersion":"1.0",
  "WindowsInstaller":"5.0.7600.16385",
  "WindowsUpdateAgent":"7.3.7600.16385",
  "OSLastStartupTime":"2009-10-22T00:00:00.000Z",
  "WindowsDirectory":"C:\\windows",
  "IEVersion":"8.0.7600.16385",
  "IEServicePack":"0",
  "PowerManagement": {
    "VideoTimeoutAC":"600",
    "VideoTimeoutDC":"300",
    "SpindownTimeoutAC":"1200",
    "SpindownTimeoutDC":"600",
    "StandbyTimeoutAC":"0",
    "StandbyTimeoutDC":"900",
    "HibernateTimeoutAC":"0",
    "HibernateTimeoutDC":"0",
    "ThrottlePolicyAC":"ThrottlePolicyAdaptive",
    "ThrottlePolicyDC":"ThrottlePolicyAdaptive"
  },
  "property": [
    {
      "@category":"Category Name",
      "@key":"Key Name",
      "@value":"1",
      "@type":"int",
      "@record":"1"
    }
  ],
  "SmartDeviceInformation": {
    "UUID":"1",
    "IMEI":"1",
    "UDID":"1",
    "ICCID":"1",
    "IMSI":"1",
    "PhoneNumber":"1",
    "mail":"foo@example.com",
    "Carrier":"XXXXXXXX",
    "PasscodeSetting":"true",
    "PhisicalMemory": {
```

```
        "Size":"100",
        "FreeSpace":"100"
      },
      "Storage": {
        "Size":"100",
        "FreeSpace":"100"
      },
      "Media": {
        "Size":"100",
        "FreeSpace":"100"
      }
    }
  },
  "InstalledSoftware": {
    "@LastUpdateTime":"2018-04-12T15:35:53.000Z",
    "@ReportType":"All",
    "SoftwareList": {
      "Software": [
        {
          "@Type":"InstalledSoftware",
          "SourceID":"XXXXXXXX 2013",
          "InstallPath":"C:\\Program Files\\XXXXXXXX\\",
          "Name":"XXXXXXXX 2013",
          "Version":"15.0.4569.1506",
          "Publisher":"XXXXXXXX",
          "InstallDate":"2016-10-03T00:00:00.000Z"
        }
      ]
    }
  },
  "Update": {
    "@ReportType":"All",
    "@LastUpdateTime":"2018-04-12T15:35:53.000Z",
    "SoftwareList": {
      "Software": [
        {
          "HotFixID":"KB00000",
          "Description":"Description",
          "InstallDate":"2016-10-03T00:00:00.000Z"
        }
      ]
    }
  },
  "SecurityInventory": {
    "@LastUpdateTime":"2018-04-13T12:00:00.000Z",
    "AccountList": {
      "Account": [
        {
          "Name":"TEST\\1",
          "LastPasswordModifiedDate":"2017-08-10T06:00:00.000Z",
          "WeakPassword":"WeakPasswordFalse",
          "UnexpirePassword":"UnexpirePasswordFalse",
          "ScreenSaverEnabled":"ScreenSaverEnabledFalse",
          "ScreenSaverIsSecure":"ScreenSaverIsSecureFalse",
          "ScreenSaverTimeout":"0"
        }
      ]
    },
```

```
            "PowerOnPassword":"PowerOnPasswordDisabled",
            "GuestAccount":"GuestAccountDisabled",
            "AutoLogon":"AutoLogonDisabled",
            "SharedDirectory":"SharedDirectoryFound",
            "AutoShareServer":"AutoShareServerTrue",
            "DCOM":"DCOMEnabled",
            "RestrictAnonymous":"RestrictAnonymousDisabled",
            "WindowsFirewall":"WindowsFirewallDisabled",
            "WindowsUpdate":"WindowsUpdateEnabled",
            "DenyTSConnections":"DenyTSConnectionsTrue"
          },
          "ExtendInventory": {
            "@LastUpdateTime":"2019-10-11T12:12:12.000Z",
            "ExtendInventoryList": {
              "ExtendInventoryItem": [
                {
                  "@InformationType":"Organization",
                  "ValueTree" : {
                    "Value" : {
                      "Data" : "X",
                      "Value" : {
                        "Data" : "Y",
                        "Value" : {
                          "Data" : "Z"
                        }
                      }
                    }
                  }
                },
                {
                  "@InformationType":"other",
                  "ItemName":"Gender",
                    "ValueList": {
                      "Value":"xx"
                    }
                },
                {
                  "@InformationType":"other",
                  "ItemName":"Name",
                  "Value":"Pedro Garcia"
                },
                {
                  "@InformationType":"other",
                  "ItemName":"Age",
                  "Value":"20"
                },
                {
                  "@InformationType":"other",
                  "ItemName":"Birthday",
                  "Value":"2000-11-11T00:00:00.000Z"
                }
              ]
            }
          }
        }
      }
    }
```

```
    ]
}
```

20.3.2 Device information list acquisition

This API acquires a device information list from the management server.

Execution permission

You need the following permission:

- API permission

API version

v1

Request format

Request line

```
GET /jp1itdm/api/v1/objects/devices_reference?filter HTTP/1.1
```

For *filter*, specify filter conditions for acquiring desired device information. For details, see *Filter conditions for acquiring device information*.

Request header

```
Host:host-name-or-IP-address-of-management-server:port-number-of-management-server
Accept-Language:language-code-in-the-message-of-response
Accept:application/json
Content-Type:application/json
X-ITDM-Authorization1:Base64-encoded-user-ID
X-ITDM-Authorization2:Base64-encoded-password
```

Request message body

None

Response format

Status line

Either a status code or its text is returned. For details, see the description of status codes in 20.2 Common API specifications.

Response header

For details, see the description of the response format in 20.2 Common API specifications.

Response message body

Under normal circumstances, the message body contains a device information list in JSON format. For details, see *Data format for device information*.

When an error occurs, error information is stored in JSON format. For details, see the description of the error information in 20.2 Common API specifications.

Filter conditions for acquiring device information

You can specify a filter condition for acquiring device information by inserting a query string in the request line. A query string to be used to specify filter conditions for acquiring device information should be in the following format:

```
count=number-of-records-to-acquire&offset=start-position-for-records&fields=
items-included-in-each-acquired-record&filters[1]=filter-condition-1&filter
s[2]=filter-condition-2...&filters[10]=filter-condition-10&sort=sort-conditi
on
```

Legend: ...: Repetitions of `&filters[n]=`*filter-condition-n* (*n* = 3 to 9)

Each item in the query string is described in detail below. All of these items are optional. When no query string is specified, a response returned will contain the maximum number of device information records that can be acquired.

count

Specify the number of device information records you want to acquire.

If you specify `0` or if you omit this parameter, it is assumed that the maximum number of device information records that can be acquired has been specified. Specifying a value that exceeds the maximum limit will result in an error.

Example: When you want to acquire 1,000 device information records, specify `count=1000`.

> **Note**
>
> The maximum number of device information records that can be acquired at one time by the device information list acquisition is 10,000.

offset

Specify the start position for the device information records to be acquired.

If you specify `0` or if you omit this parameter, device information records are acquired starting from the first record.

When you acquire device information records for the first time, execute this API with `0` set for this parameter. When the response has a `totalCount` value that is larger than the `responseCount` value, you can acquire the next set of device information records by executing this API with the sum of the `offset` value and `responseCount` value in the response specified for this parameter.

Example: When you want to acquire device information records starting from Record 1,001, specify `offset=1001`.

> **Note**
>
> Adding or deleting device information records during the acquisition of device information records can cause the start position to shift when you attempt to acquire the next set of device information records.
>
> If the records are shifted, some records may not be acquired (skipped) or duplicate records may be acquired.

fields

Specify the items you want included in each acquired device information record. For details about the specifiable items, see *Items that can be specified as filter conditions and the format of their values*. When you specify multiple items, use a comma (`,`) to separate them.

If you omit this parameter, each one of the acquired device information records will contain all items.

Example: If you want the acquired device information records to contain the host ID, host name, device type, and OS type of the individual devices, specify `fields=NodeID,HostName,EquipmentType,OsKind`.

filters[*n*]

Specify filter conditions for the device information records to be acquired. For details about filter conditions, see *Syntax for filter conditions*.

You can specify a maximum of 10 filter conditions. When there are 10 filter conditions, specify filter condition numbers from 1 to 10, in that order, by replacing each *n* with the corresponding number. Do not skip a filter condition number. For example, specifying the following filter conditions, in which filter condition number 3 is skipped, results in an error: `filters[1]=`*`filter-condition-1`*`&filters[2]=`*`filter-condition-2`*`&filters[4]=`*`filter-condition-4`*.

When you specify multiple filter conditions, only those device information records that satisfy all specified conditions are acquired.

sort

Specify items to be used to sort the acquired device information records. Select from the items listed under *Items that can be specified as filter conditions and the format of their values*. To sort the acquired device information records in the descending order of the values corresponding to a certain item, prefix the item name with a minus sign (−).

When you specify multiple item names, separate them with a comma (`,`). When multiple items are specified, the acquired device information records are first sorted according to the first item specified, and the resulting records are further sorted according to the second item specified, and so on.

If you omit this parameter, it is assumed that `sort=NodeID` is specified.

Example: To sort acquired device information records in ascending order of device type, and then sort the resulting records in descending order of last updated date and time, specify `sort=EquipmentType,-LastUpdateTime`.

> **Note**
>
> If you specify `sort` parameter, it is assumed that `,NodeID` is specified in end of the parameter.

> **Note**
>
> An error occurs if the total value for the `count` parameter and `offset` parameter exceeds 2,147,483,647. An error also occurs if the `count` parameter is not specified or `0` is specified for the `count` parameter, and the total value for the upper limit for the `count` parameter and the `offset` parameter exceeds 2,147,483,647.

> **Note**
>
> The following symbols cannot be used in the item names specified in the `fields` parameter, `filters[n]` parameter, or `sort` parameter.
>
> single quotation mark (`'`), double quotation mark (`"`), space, tab, left curly bracket (`{`), right curly bracket (`}`), left square bracket (`[`), right square bracket (`]`), left parenthesis (`(`), right parenthesis (`)`), backslash (`\`), colon (`:`), semicolon (`;`), asterisk (`*`), question mark (`?`), equal sign (=), hyphen (−), and vertical bar (`|`)

Syntax for filter conditions

Use the following syntax to specify a filter condition for `filters[n]`:

When an operator other than `in()` or `not in()` is to be used:

```
filters[n]=item-nameΔoperatorΔ'value'
```

When `in()` or `not in()` is to be used as an operator:

```
filters[n]=item-nameΔin('value-1','value-2'...)
filters[n]=item-nameΔnotΔin('value-1','value-2'...)
```

Legend:

...: Repetitions of `,'value-n'`

Δ: One space character

Important

Only one space should be written at Δ. If the space is used in not specified at Δ or if two or more spaces are written, an error occurs.

n

Specify a filter condition number. Filter conditions must be numbered serially from 1 to 10.

item-name

Specify a filter condition by selecting from the item names listed under *Items that can be specified as filter conditions and the format of their values*.

operator

Specify an operator for the filter condition. The following table shows specifiable operators.

Operator	Description	Example
=	Acquires device information records whose *value* corresponding to the specified *item-name* matches the specified value.	`filters[1]=HostName='host01'` Acquires device information records whose host name is `host01`.
!=	Acquires device information records whose *value* corresponding to the specified *item-name* does not match the specified value.	`filters[1]=HostName!='host01'` Acquires device information records whose host name is something other than `host01`.
>	Acquires device information records whose *value* corresponding to the specified *item-name* is larger than the specified value.	filters[1]=StandbyTimeoutAC>'60' Acquires device information records whose time to system standby (AC) is longer than 60 seconds. filters[1]=LastUpdateTime>'2020-04-01' Acquires device information records whose last updated date and time is after `2020-04-01T00:00:00.000Z`.
<	Acquires device information records whose *value* corresponding to the specified *item-name* is smaller than the specified value.	filters[1]=StandbyTimeoutAC<'60' Acquires device information records whose time to system standby (AC) is shorter than 60 seconds. filters[1]=LastUpdateTime<'2020-04-01' Acquires device information records whose last updated date and time is before `2020-04-01T00:00:00.000Z`.
>=	Acquires device information records whose *value* corresponding to the specified *item-name* is equal to or larger than the specified value.	filters[1]=StandbyTimeoutAC>='60' Acquires device information records whose time to system standby (AC) is equal to or longer than 60 seconds.

Operator	Description	Example
>=	Acquires device information records whose *value* corresponding to the specified *item-name* is equal to or larger than the specified value.	filters[1]=LastUpdateTime>='2020-04-01' Acquires device information records whose last updated date and time is `2020-04-01T00:00:00.000Z` or later.
<=	Acquires device information records whose *value* corresponding to the specified *item-name* is equal to or smaller than the specified value.	filters[1]=StandbyTimeoutAC<='60' Acquires device information records whose time to system standby (AC) is equal to or shorter than 60 seconds. filters[1]=LastUpdateTime<='2020-04-01' Acquires device information records whose last updated date and time is `2020-04-01T00:00:00.000Z` or earlier.
in()	Acquires device information records whose *value* corresponding to the specified *item-name* matches one of the values listed in parentheses. The listed values are individually enclosed in single quotation marks (`'`) and separated with a comma (`,`) in between. The maximum number of values that can be specified in the in() clause is 100.	`filters[1]=OsKind in('1','2','3')` Acquires device information records whose OS type is `1` (Windows), `2` (Linux), or `3` (UNIX).
not in()	Acquires device information records whose *value* corresponding to the specified *item-name* does not match any of the values listed in parentheses. The listed values are individually enclosed in single quotation marks (`'`) and separated with a comma (`,`) in between. The maximum number of values that can be specified in the not in() clause is 100.	`filters[1]=OsKind not in('1','2','3')` Acquires device information records whose OS type is something other than `1` (Windows), `2` (Linux), or `3` (UNIX).
like	Acquires device information records whose *value* corresponding to the specified *item-name* matches a string in the specified value. This operator distinguishes between uppercase and lowercase letters in a string contained in the *value*. You can use a wildcard (`%`) in a string contained in the specified *value*. % Represents a string of any length, including 0 length. When the specified value contains a string that contains a underscore (_), percent sign (`%`) or backslash (`\`), replace it with `\_`, `\%` or `\\`.	filters[1]=HostName like 'TestPC' Acquires device information records whose host name is `TestPC`. filters[1]=HostName like 'Test%' Acquires device information records whose host name starts with the string `Test`. filters[1]=HostName like '%Test%' Acquires device information records whose host name contains the string `Test`.
not like	Acquires device information records whose *value* corresponding to the specified *item-name* does not match a string in the specified value. This operator distinguishes between uppercase and lowercase letters in a string contained in the *value*. You can use a wildcard (`%`) in a string contained in the specified *value*. % Represents a string of any length, including 0 length.	filters[1]=HostName not like 'TestPC' Acquires device information records whose host name is something other than `TestPC`. filters[1]=HostName not like 'Test%' Acquires device information records whose host name does not start with the string `Test`. filters[1]=HostName not like '%Test%' Acquires device information records whose host name does not contain the string `Test`.

Operator	Description	Example
not like	When the specified value contains a string that contains a underscore (_), percent sign (%) or backslash (\), replace it with _, \% or \\.	filters[1]=HostName not like 'TestPC' Acquires device information records whose host name is something other than TestPC. filters[1]=HostName not like 'Test%' Acquires device information records whose host name does not start with the string Test. filters[1]=HostName not like '%Test%' Acquires device information records whose host name does not contain the string Test.

value

Specify a value for the filter condition.

For details about the data type of the item name to be specified, see *Items that can be specified as filter conditions and the format of their values*. For details about the coding format appropriate to each data type, see the information provided under Supported data types in 20.2 Common API specifications. Remember that you have to enclose a string in single quotation marks (') to specify a value.

Note

The format to be used to specify a value for the dateTime-type item names varies depending on the operator used.

When using = or != as the operator

Specify the value in the '*YYYY-MM-DD*T*HH*:*MM*:*SS*.*sss*Z' format.

When using >, >=, < or <= as the operator

The basic format being '*YYYY-MM-DD*T*HH*:*MM*:*SS*.*sss*Z', you only have to specify up to a desired point in this format.

For example, if you specify filters[1]=LastUpdateTime<'2020-04', device information records whose last updated date and time is earlier than 2020-04-01T00:00:00.000Z are acquired.

Note

If a string containing single quotation mark (') is specified as a *value*, it must be replaced with two single quotation marks ('').

Items that can be specified as filter conditions and the format of their values

The following table describes the items that can be specified as filter conditions and the format of their values:

Item name	Data type	Description
NodeID	string	Specify this item to filter device information records by host ID.
HostName	string	Specify this item to filter device information records by host name.
IPAddress	string	Specify this item to filter device information records by IP address. This value must be expressed as a string by using the IPv4 format *xxx*.*xxx*.*xxx*.*xxx* (where *xxx* represents a number in the range of 0-255). When using like or not like as the operator, remember to suffix the specified value with the wildcard character %.

Item name	Data type	Description
MACAddress	string	Specify this item to filter device information records by MAC address. This value must be in the *xx*:*xx*:*xx*:*xx*:*xx*:*xx* format or expressed as a string using the format *xx*-*xx*-*xx*-*xx*-*xx*-*xx* (where *x* represents a number in the range of 0-9 or a letter in the range of A-F or a-f). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`.
CreateTime	dateTime	Specify this item to filter device information records by created date and time.
LastUpdateTime	dateTime	Specify this item to filter device information records by last updated date and time.
LastAliveDate	dateTime	Specify this item to filter device information records by date and time when a computer-to-management server connection was last confirmed.
IPSubnet	string	Specify this item to filter device information records by subnet mask. This value must be expressed as a string by using the IPv4 format *xxx*.*xxx*.*xxx*.*xxx* (where *xxx* represents a number in the range of 0-255). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`.
EquipmentType	string	Specify this item to filter device information records by device type. You can specify one of the following values: • `EquipmentTypeComputer`: PC • `EquipmentTypeServer`: Server • `EquipmentTypeStorage`: Storage device • `EquipmentTypeNetworkDevice`: Network device • `EquipmentTypePrinter`: Printer device • `EquipmentTypePeripheralDevice`: Peripheral device • `EquipmentTypeUSBMemory`: USB memory • `EquipmentTypeDisplay`: Display • `EquipmentTypeSmartDevice`: Smart device • `EquipmentTypeOther`: Other device • `EquipmentTypeUnknown`: Unknown device • `EquipmentTypeUser`: Device type added by the administrator user
EquipmentUserType	string	Specify this item to filter device information records by name of user definition optionally added by the administrator user.
OsKind	int	Specify this item to filter device information records by OS type. You can specify one of the following values: • `0`: Unknown • `1`: Windows • `2`: Linux • `3`: UNIX • `4`: Mac OS • `5`: OS for smart devices • `6`: HP-UX • `7`: Solaris • `8`: AIX
AMTFirmwareVersion	string	Specify this item to filter device information records by AMT firmware version.
AgentType	int	Specify this item to filter device information records by management type. You can specify one of the following values: • `0`: Agent Management • `1`: Agentless Management

Item name	Data type	Description
AgentType	int	• 2: Agent Management(Network Access Control) • 4: Agent Management(Site Server) • 6: Agent Management(Site server)(Network Access Control) • 9: MDM Linkage Management • 16: Agent Management(Relaysystem) • 18: Agent Management(Relaysystem)(Network Access Control) • 32: Management Relay Server • 34: Management Relay Server(Network Access Control) • 65: API management
AgentVersion	string	Specify this item to filter device information records by agent version.
DistributionRegDate	dateTime	Specify this item to filter device information records by distribution date and time.
AgentDistributionStatus	int	Specify this item to filter device information records by agent distribution status. You can specify one of the following values: • 0: Not distributed yet (default value) • 1: Waiting to be distributed • 11: Currently being distributed • 51: Failed distribution attempt (distribution is being retried) • 52: Failed distribution attempt (with failed retry attempt) • 999: Agent installer started
AgentDistributionErrorType	int	Specify this item to filter device information records by error description provided after a failed agent distribution attempt. You can specify one of the following values: • 0: (Default) • 1: Authentication error • 2: Communication error • 3: Installation-in-progress error • 4: Waiting-for-PC-to-start error • 5: Other error • 101: An agent has not been registered. • 102: User authentication failed. • 103: Failed to access administrative shares. • 104: Failed to access the client. • 105: A communication error occurred. • 106: The MAC address is different from the registered one. • 107: An agent has already been installed. • 108: No notification of success has arrived from the agent. • 109: The client failed to resolve the manager's host name. • 110: Authentication information has not been specified. • 111: An error occurred during the creation of agent installation media. • 112: The agent installer is currently running. • 113: The agent installer did not finish. • 201: Failed decompression attempt • 202: Required-OS error • 203: User-permissions error • 204: Failed installation attempt
AgentStatus	int	Specify this item to filter device information records by device management status. You can specify one of the following values: • 0: Managed

Item name	Data type	Description
AgentStatus	int	• 1: Excluded • 2: Discovered
DiscoverTime	dateTime	Specify this item to filter device information records by discovered date and time.
AuthStatus	int	Specify this item to filter device information records by detailed device status. You can specify one of the following values: • 0: Running normally (default value) • 1: (Status of the discovered device) An authentication error occurred. • 2: (Status of the discovered device) The computer is not running. • 101: (Printer status) Needing attention of maintenance personnel • 102: (Printer status) Cover open • 103: (Printer status) Paper jam • 104: (Printer status) Paper feeding tray missing • 105: (Printer status) Paper receiving tray missing • 106: (Printer status) Consumable items lost • 107: (Printer status) Toner empty • 108: (Printer status) Paper receiving tray full • 109: (Printer status) Out of paper • 110: (Printer status) Paper feeding tray empty • 111: (Printer status) Toner low • 112: (Printer status) Paper low • 113: (Printer status) Paper receiving tray almost full • 114: (Printer status) A communication error occurred. • 115: (Printer status) Timing of preventive maintenance due to expiry • 999: Unknown • 1350: (Site server status) A fatal error occurred. • 1360: (Site server status) The database was blocked. • 3060: (Site server status) An attempt to install the site server failed. • 3070: (Site server status) An attempt to uninstall the site server failed. • 3160: (Network monitor status) The network monitor services stopped. • 3260: (Site server status) The site server services stopped. • 3365: (Site server status) No free space left in the folder storing the operation log database. • 3370: (Site server status) No free disk space left on the drive that contains the folder storing the operation log. • 3375: (Site server status) The folder storing the operation log database is low on free space. • 3380: (Site server status) The drive that contains the folder storing the operation log is low on disk space. • 3470: (Site server status) No disk space left on the drive that contains the data folder. • 3480: (Site server status) The drive that contains the data folder is low on disk space. • 3680: (Network monitor/site server status) The computer is not running. • 3850: (Smart device status) The smart device was initialized.
NetworkStatus	int	Specify this item to filter device information records by connection status. You can specify one of the following values: • 0: Allowed • 1: Blocked • 2: Forcibly blocked • 3: Outside the period of use • 999: Unknown

Item name	Data type	Description
AgentDeviceStatus	int	Specify this item to filter device information records by device status. You can specify one of the following values: • 0: Running • 1: Not running • 2: Warning • 3: Failure • 999: Unknown • 1100: Not applicable
DiscoveryProtocol	int	Specify this item to filter device information records by method used to collect device information from agentless devices. You can specify one of the following values: • 0: Administrative shares • 1: Remote WMI • 2: SNMP • 3: ICMP • 4: ARP • 5: Active Directory • 6: MDM • 999: Unknown
Caption	string	Specify this item to filter device information records by OS name.
AllMacAddress	string	Specify this item to filter device information records by all MAC addresses held by a device. This value must be in the *xx*:*xx*:*xx*:*xx*:*xx*:*xx* format or expressed as a string using the format *xx*-*xx*-*xx*-*xx*-*xx*-*xx* (where *x* represents a number in the range of 0-9 or a letter in the range of A-F or a-f). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`. If the specified value exceeds the maximum length allowed, only those specified MAC addresses that fit within the allowed length become valid.
InstallCompletionDate	dateTime	Specify this item to filter device information records by date and time when the distribution of the agent was completed.
CSDVersion	string	Specify this item to filter device information records by OS Service Pack.
IEVersion	string	Specify this item to filter device information records by Internet Explorer version.
UnnecessaryServicecnt	int	Specify this item to filter device information records by number of Windows services prohibited by security policies.
VideoTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to monitor shutdown (AC).
VideoTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to monitor shutdown (DC).
StandbyTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to entering system standby (AC).
StandbyTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to entering system standby (DC).
HibernateTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to entering system hibernation state (AC).
HibernateTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to entering system hibernation state (DC).

Item name	Data type	Description
SpindownTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to hard disk shutdown (AC).
SpindownTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to hard disk shutdown (DC).
OsLanguage	int	Specify this item to filter device information records by OS language. You can specify one of the following values: • 1 Arabic • 4 Chinese (Simplified)– China • 9 English • 1025 Arabic – Saudi Arabia • 1026 Bulgarian • 1027 Catalan • 1028 Chinese (Traditional) – Taiwan • 1029 Czech • 1030 Danish • 1031 German – Germany • 1032 Greek • 1033 English – United States • 1034 Spanish – Traditional Sort • 1035 Finnish 1036 French – France • 1037 Hebrew • 1038 Hungarian • 1039 Icelandic • 1040 Italian – Italy • 1041 Japanese • 1042 Korean • 1043 Dutch – Netherlands • 1044 Norwegian – Bokmal • 1045 Polish • 1046 Portuguese – Brazil • 1047 Rhaeto-Romanic • 1048 Romanian • 1049 Russian • 1050 Croatian • 1051 Slovak • 1052 Albanian • 1053 Swedish • 1054 Thai • 1055 Turkish • 1056 Urdu • 1057 Indonesian • 1058 Ukrainian • 1059 Belarusian • 1060 Slovenian • 1061 Estonian • 1062 Latvian • 1063 Lithuanian • 1065 Persian • 1066 Vietnamese • 1069 Basque • 1070 Serbian

Item name	Data type	Description
OsLanguage	int	• 1071 Macedonian (F.Y.R.O. Macedonia) • 1072 Sutu • 1073 Tsonga • 1074 Tswana • 1076 Xhosa • 1077 Zulu • 1078 Afrikaans • 1080 Faeroese • 1081 Hindi • 1082 Maltese • 1084 Gaelic • 1085 Yiddish • 1086 Malay – Malaysia • 2049 Arabic – Iraq • 2052 Chinese (Simplified) – PRC • 2055 German – Switzerland • 2057 English – United Kingdom • 2058 Spanish – Mexico • 2060 French – Belgium • 2064 Italian – Switzerland • 2067 Dutch – Belgium • 2068 Norwegian – Nynorsk • 2070 Portuguese – Portugal • 2072 Romanian – Moldova • 2073 Russian – Moldova • 2074 Serbian – Latin • 2077 Swedish – Finland • 3073 Arabic – Egypt • 3076 Chinese (Traditional) – Hong Kong SAR • 3079 German – Austria • 3081 English – Australia • 3082 Spanish – International Sort • 3084 French – Canada • 3098 Serbian – Cyrillic • 4097 Arabic – Libya • 4100 Chinese (Simplified) – Singapore • 4103 German – Luxembourg • 4105 English – Canada • 4106 Spanish – Guatemala • 4108 French – Switzerland • 5121 Arabic – Algeria • 5127 German – Liechtenstein • 5129 English – New Zealand • 5130 Spanish – Costa Rica • 5132 French – Luxembourg • 6145 Arabic – Morocco • 6153 English – Ireland • 6154 Spanish – Panama • 7169 Arabic – Tunisia • 7177 English – South Africa • 7178 Spanish – Dominican Republic • 8193 Arabic – Oman

Item name	Data type	Description
OsLanguage	int	• 8201 English – Jamaica • 8202 Spanish – Venezuela • 9217 Arabic – Yemen • 9226 Spanish – Colombia • 10241 Arabic – Syria • 10249 English – Belize • 10250 Spanish – Peru • 11265 Arabic – Jordan • 11273 English – Trinidad • 11274 Spanish – Argentina • 12289 Arabic – Lebanon • 12298 Spanish – Ecuador • 13313 Arabic – Kuwait • 13322 Spanish – Chile • 14337 Arabic – U.A.E. • 14346 Spanish – Uruguay • 15361 Arabic – Bahrain • 15370 Spanish – Paraguay • 16385 Arabic – Qatar • 16394 Spanish – Bolivia • 17418 Spanish – El Salvador • 18442 Spanish – Honduras • 19466 Spanish – Nicaragua • 20490 Spanish – Puerto Rico
ProductID	string	Specify this item to filter device information records by agent model.
PollingInterval	int	Specify this item to filter device information records by interval (units: seconds) at which an agent polls the management server.
MngStatusUpdateTime	dateTime	Specify this item to filter device information records by date and time when the management status of devices was updated.
AllIpAddress	string	Specify this item to filter device information records by all IP addresses held by the individual devices. This value must be expressed as a string by using the IPv4 format *xxx*`.`*xxx*`.`*xxx*`.`*xxx* (where *xxx* represents a number in the range of 0-255), or the IPv6 format *xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx* (*x*: one character from 0-9, A-F, or a-f). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`. If the specified value exceeds the maximum length allowed, only those specified IP addresses that fit within the allowed length become valid.
SnoozeDownloadStatus	int	Specify this item to filter device information records by package download delay status. You can specify one of the following values: • 0: Not delayed • 1: Delayed
Domain	string	Specify this item to filter device information records by domain or work group.
Manufacturer	string	Specify this item to filter device information records by device model or manufacturer.
NodeNameInt	int	Specify this item to filter device information records by numeric-type host ID.
UUID	string	Specify this item to filter device information records by UDID.

Item name	Data type	Description
PhoneNumber	string	Specify this item to filter device information records by contract phone number.
IMEI	string	Specify this item to filter device information records by IMEI.
RegistrationType	int	Specify this item to filter device information records by management type. You can specify one of the following values: • 0: Online management • 1: Offline management
OsLastStartUpdateTime	dateTime	Specify this item to filter device information records by date and time when the OS was last started.

Data format for device information

Device information has the following data format:

```
{
    "DeviceList": [
        {
        "Device": {
            "NodeID": "host-ID",
            "HostName": "host-name",
            "IPAddress": "IP-address",
            "MACAddress": "MAC-address",
            "CreateTime": "created-date-and-time",
            "LastUpdateTime": "last-updated-date-and-time",
            "LastAliveDate": "date-and-time-last-confirmed",
            "IPSubnet": "subnet-mask",
            "EquipmentType": "device-type",
            "EquipmentUserType": "device-type-name-added-by-the-administrato
r-user",
            "OsKind": "OS-type",
            "AMTFirmwareVersion": "AMT-firmware-version",
            "AgentType": "management-type",
            "AgentVersion": "agent-version",
            "DistributionRegDate": "distribution-date-and-time",
            "AgentDistributionStatus": "agent-distribution-status",
            "AgentDistributionErrorType": "error-description-provided-after-
failed-agent-distribution",
            "AgentStatus": "device-management-status",
            "DiscoverTime": "discovered-date-and-time",
            "AuthStatus": "detailed-device-status",
            "NetworkStatus": "connection-status",
            "AgentDeviceStatus": "device-status",
            "DiscoveryProtocol": "method-used-to-collect-device-information-
from-agentless-devices",
            "Caption": "OS-name",
            "AllMacAddress": "all-MAC-addresses-held-by-a-device",
            "InstallCompletionDate": "date-and-time-when-the-distribution-of
-the-agent-was-completed",
            "CSDVersion": "OS-Service-Pack",
            "IEVersion": "Internet Explorer version",
            "UnnecessaryServicecnt": "number-of-Windows-services-prohibited-
by-security-policies",
            "VideoTimeoutAC": "time-(units:seconds)-to-monitor-shutdown-(AC)
",
            "VideoTimeoutDC": "time-(units:seconds)-to-monitor-shutdown-(DC)
```

```
",
            "StandbyTimeoutAC": "time-(units:seconds)-to-entering-system-sta
ndby-(AC)",
            "StandbyTimeoutDC": "time-(units:seconds)-to-entering-system-sta
ndby-(DC)",
            "HibernateTimeoutAC": "time-(units:seconds)-to-entering-system-h
ibernation-state-(AC)",
            "HibernateTimeoutDC": "time-(units:seconds)-to-entering-system-h
ibernation-state-(DC)",
            "SpindownTimeoutAC": "time-(units:seconds)-to-hard-disk-shutdown
-(AC)",
            "SpindownTimeoutDC": "time-(units:seconds)-to-hard-disk-shutdown
-(DC)",
            "OsLanguage": "OS-language",
            "ProductID": "agent-model",
            "PollingInterval": "interval-(units:seconds)-at-agent-polls-mana
gement-server",
            "MngStatusUpdateTime": "updated-date-and-time-management-status"
,
            "AllIpAddress": "all-IP-addresses-held-by-a-device",
            "SnoozeDownloadStatus": "package-download-delay-status",
            "Domain": "domain-or-work-group",
            "Manufacturer": "device-model-or-manufacturer",
            "NodeNameInt": "numeric-type-host-ID",
            "UUID": "UDID",
            "PhoneNumber": "contract-phone-number",
            "IMEI": "IMEI",
            "RegistrationType": "management-type",
            "OsLastStartUpdateTime": "date-and-time-when-OS-last-started"
            }, ...
        }
    ],
    "offset": "start-position-of-the-device-information-records",
    "responseCount": "number-of-acquired-device-information-records",
    "totalCount": "total-number-of-device-information-records-matching-the-s
pecified-filters"}
```

Legend: ...: Iterations of the previous layer

DeviceList

Item name	Data type	Mandatory / Optional	Description
DeviceList	Array	Mandatory	Root name of device information. This item stores arrays of `Device` objects.
Device	Object	Mandatory	Object name of a device information record. For details, see *Device object*.
offset	int	Mandatory	This item stores the start position of the device information records included in the current response data.
responseCount	int	Mandatory	This item stores the number of acquired device information records included in the current response data. To request the next set of device information records, calculate the sum of the `offset` value and the `responseCount` value, which must not exceed the `totalCount` value, and specify it for `offset` in the query string of the request.

Item name	Data type	Mandatory / Optional	Description
totalCount	int	Mandatory	This item stores the total number of device information records matching the filters specified in the query string of the request.

Device object

All `Device` object items are optional.

Item name	Data type	Description
NodeID	string	This item stores a host ID.
HostName	string	This item stores a host name. When an empty character is stored, this item appears as follows: `"HostName": ""`
IPAddress	string	This item stores an IP (IPv4) address. When there are multiple IP addresses, the one that was used to send a notification to the management server is stored. When an empty character is stored, this item appears as follows: `"IPAddress": ""`
MACAddress	string	This item stores a MAC address. When an empty character is stored, this item appears as follows: `"MACAddress": ""`
CreateTime	dateTime	This item stores a created date and time. When an empty character is stored, this item appears as follows: `"CreateTime": ""`
LastUpdateTime	dateTime	This item stores a last updated date and time. When an empty character is stored, this item appears as follows: `"LastUpdateTime": ""`
LastAliveDate	dateTime	This item stores a date and time when a computer-to-management server connection was last confirmed. When an empty character is stored, this item appears as follows: `"LastAliveDate": ""`
IPSubnet	string	This item stores the subnet mask corresponding to the IP address stored in `IPAddress`. When an empty character is stored, this item appears as follows: `"IPSubnet": ""`
EquipmentType	string	This item stores a device type. Specifically, one of the following device types is stored: • `EquipmentTypeComputer`: PC • `EquipmentTypeServer`: Server • `EquipmentTypeStorage`: Storage device • `EquipmentTypeNetworkDevice`: Network device • `EquipmentTypePrinter`: Printer device • `EquipmentTypePeripheralDevice`: Peripheral device • `EquipmentTypeUSBMemory`: USB memory • `EquipmentTypeDisplay`: Display • `EquipmentTypeSmartDevice`: Smart device • `EquipmentTypeOther`: Other device • `EquipmentTypeUnknown`: Unknown device • `EquipmentTypeUser`: Device type added by the administrator user

Item name	Data type	Description
EquipmentUserType	string	This item stores the name of the user definition optionally added by the administrator user. When an empty character is stored, this item appears as follows: `"EquipmentUserType": ""`
OsKind	int	This item stores an OS type. Specifically, one of the following values is stored: • `0`: Unknown • `1`: Windows • `2`: Linux • `3`: UNIX • `4`: Mac OS • `5`: OS for smart devices • `6`: HP-UX • `7`: Solaris • `8`: AIX
AMTFirmwareVersion	string	This item stores an AMT firmware version. When an empty character is stored, this item appears as follows: `"AMTFirmwareVersion": ""`
AgentType	int	This item stores a management type. Specifically, one of the following values is stored: • `0`: Agent Management • `1`: Agentless Management • `2`: Agent Management(Network Access Control) • `4`: Agent Management(Site Server) • `6`: Agent Management(Site server)(Network Access Control) • `9`: MDM Linkage Management • `16`: Agent Management(Relaysystem) • `18`: Agent Management(Relaysystem)(Network Access Control) • `32`: Management Relay Server • `34`: Management Relay Server(Network Access Control) • `65`: API management
AgentVersion	string	This item stores an agent version. When an empty character is stored, this item appears as follows: `"AgentVersion": ""`
DistributionRegDate	dateTime	This item stores a distribution date and time. When an empty character is stored, this item appears as follows: `"DistributionRegDate": ""`
AgentDistributionStatus	int	This item stores an agent distribution status. Specifically, one of the following values is stored: • `0`: Not distributed yet (default value) • `1`: Waiting to be distributed • `11`: Currently being distributed • `51`: Failed distribution attempt (distribution is being retried) • `52`: Failed distribution attempt (with failed retry attempt) • `999`: Agent installer started
AgentDistributionErrorType	int	This item stores an error description provided after a failed agent distribution attempt. Specifically, one of the following values is stored: • `0`: (Default)

Item name	Data type	Description
AgentDistributionErrorType	int	• 1: Authentication error • 2: Communication error • 3: Installation-in-progress error • 4: Waiting-for-PC-to-start error • 5: Other error • 101: An agent has not been registered. • 102: User authentication failed. • 103: Failed to access administrative shares. • 104: Failed to access the client. • 105: A communication error occurred. • 106: The MAC address is different from the registered one. • 107: An agent has already been installed. • 108: No notification of success has arrived from the agent. • 109: The client failed to resolve the manager's host name. • 110: Authentication information has not been specified. • 111: An error occurred during the creation of agent installation media. • 112: The agent installer is currently running. • 113: The agent installer did not finish. • 201: Failed decompression attempt • 202: Required-OS error • 203: User-permissions error • 204: Failed installation attempt
AgentStatus	int	This item stores a device management status. Specifically, one of the following values is stored: • 0: Managed • 1: Excluded • 2: Discovered
DiscoverTime	dateTime	This item stores a discovered date and time. When an empty character is stored, this item appears as follows: `"DiscoverTime": ""`
AuthStatus	int	This item stores a detailed device status. Specifically, one of the following values is stored: • 0: Running normally (default value) • 1: (Status of the discovered device) An authentication error occurred. • 2: (Status of the discovered device) The computer is not running. • 101: (Printer status) Needing attention of maintenance personnel • 102: (Printer status) Cover open • 103: (Printer status) Paper jam • 104: (Printer status) Paper feeding tray missing • 105: (Printer status) Paper receiving tray missing • 106: (Printer status) Consumable items lost • 107: (Printer status) Toner empty • 108: (Printer status) Paper receiving tray full • 109: (Printer status) Out of paper • 110: (Printer status) Paper feeding tray empty • 111: (Printer status) Toner low • 112: (Printer status) Paper low • 113: (Printer status) Paper receiving tray almost full • 114: (Printer status) A communication error occurred.

Item name	Data type	Description
AuthStatus	int	• 115: (Printer status) Timing of preventive maintenance due to expiry • 999: Unknown • 1350: (Site server status) A fatal error occurred. • 1360: (Site server status) The database was blocked. • 3060: (Site server status) An attempt to install the site server failed. • 3070: (Site server status) An attempt to uninstall the site server failed. • 3160: (Network monitor status) The network monitor services stopped. • 3260: (Site server status) The site server services stopped. • 3365: (Site server status) No free space left in the folder storing the operation log database. • 3370: (Site server status) No free disk space left on the drive that contains the folder storing the operation log. • 3375: (Site server status) The folder storing the operation log database is low on free space. • 3380: (Site server status) The drive that contains the folder storing the operation log is low on disk space. • 3470: (Site server status) No disk space left on the drive that contains the data folder. • 3480: (Site server status) The drive that contains the data folder is low on disk space. • 3680: (Network monitor/site server status) The computer is not running. • 3850: (Smart device status) The smart device was initialized.
NetworkStatus	int	This item stores a connection status. Specifically, one of the following values is stored: • 0: Allowed • 1: Blocked • 2: Forcibly blocked • 3: Outside the period of use • 999: Unknown
AgentDeviceStatus	int	This item stores a device status. Specifically, one of the following values is stored: • 0: Running • 1: Not running • 2: Warning • 3: Failure • 999: Unknown • 1100: Not applicable
DiscoveryProtocol	int	This item stores a method used to collect device information from agentless devices. Specifically, one of the following values is stored: • 0: Administrative shares • 2: SNMP • 3: ICMP • 4: ARP • 5: Active Directory • 6: MDM • 999: Unknown
Caption	string	This item stores an OS name. When an empty character is stored, this item appears as follows: `"Caption": ""`
AllMacAddress	string	This item stores all MAC addresses held by a device. The MAC addresses that are stored are represented by the following rules:

Item name	Data type	Description
AllMacAddress	string	• The MAC address is expressed in hexadecimal, separated by a colon (:). • Each MAC address is separated by a comma (,). • If all MAC addresses are lined up and more than 512 characters are displayed, the output will be limited to 512 characters. When an empty character is stored, this item appears as follows: `"AllMacAddress": ""`
InstallCompletionDate	dateTime	This item stores a date and time when the distribution of the agent was completed. When an empty character is stored, this item appears as follows: `"InstallCompletionDate": ""`
CSDVersion	string	This item stores an OS Service Pack. When an empty character is stored, this item appears as follows: `"CSDVersion": ""`
IEVersion	string	This item stores an Internet Explorer version. When an empty character is stored, this item appears as follows: `"IEVersion": ""`
UnnecessaryServicecnt	int	This item stores a number of Windows services prohibited by security policies.
VideoTimeoutAC	int	This item stores a time (units: seconds) to monitor shutdown (AC).
VideoTimeoutDC	int	This item stores a time (units: seconds) to monitor shutdown (DC).
StandbyTimeoutAC	int	This item stores a time (units: seconds) to entering system standby (AC).
StandbyTimeoutDC	int	This item stores a time (units: seconds) to entering system standby (DC).
HibernateTimeoutAC	int	This item stores a time (units: seconds) to entering system hibernation state (AC).
HibernateTimeoutDC	int	This item stores a time (units: seconds) to entering system hibernation state (DC).
SpindownTimeoutAC	int	This item stores a time (units: seconds) to hard disk shutdown (AC).
SpindownTimeoutDC	int	This item stores a time (units: seconds) to hard disk shutdown (DC).
OsLanguage	int	This item stores an OS language. Specifically, one of the following values is stored: • 1 Arabic • 4 Chinese (Simplified)– China • 9 English • 1025 Arabic – Saudi Arabia • 1026 Bulgarian • 1027 Catalan • 1028 Chinese (Traditional) – Taiwan • 1029 Czech • 1030 Danish • 1031 German – Germany • 1032 Greek • 1033 English – United States • 1034 Spanish – Traditional Sort • 1035 Finnish 1036 French – France • 1037 Hebrew • 1038 Hungarian • 1039 Icelandic • 1040 Italian – Italy • 1041 Japanese • 1042 Korean

Item name	Data type	Description
OsLanguage	int	• 1043 Dutch – Netherlands • 1044 Norwegian – Bokmal • 1045 Polish • 1046 Portuguese – Brazil • 1047 Rhaeto-Romanic • 1048 Romanian • 1049 Russian • 1050 Croatian • 1051 Slovak • 1052 Albanian • 1053 Swedish • 1054 Thai • 1055 Turkish • 1056 Urdu • 1057 Indonesian • 1058 Ukrainian • 1059 Belarusian • 1060 Slovenian • 1061 Estonian • 1062 Latvian • 1063 Lithuanian • 1065 Persian • 1066 Vietnamese • 1069 Basque • 1070 Serbian • 1071 Macedonian (F.Y.R.O. Macedonia) • 1072 Sutu • 1073 Tsonga • 1074 Tswana • 1076 Xhosa • 1077 Zulu • 1078 Afrikaans • 1080 Faeroese • 1081 Hindi • 1082 Maltese • 1084 Gaelic • 1085 Yiddish • 1086 Malay – Malaysia • 2049 Arabic – Iraq • 2052 Chinese (Simplified) – PRC • 2055 German – Switzerland • 2057 English – United Kingdom • 2058 Spanish – Mexico • 2060 French – Belgium • 2064 Italian – Switzerland • 2067 Dutch – Belgium • 2068 Norwegian – Nynorsk • 2070 Portuguese – Portugal • 2072 Romanian – Moldova • 2073 Russian – Moldova • 2074 Serbian – Latin • 2077 Swedish – Finland

Item name	Data type	Description
OsLanguage	int	• 3073 Arabic – Egypt • 3076 Chinese (Traditional) – Hong Kong SAR • 3079 German – Austria • 3081 English – Australia • 3082 Spanish – International Sort • 3084 French – Canada • 3098 Serbian – Cyrillic • 4097 Arabic – Libya • 4100 Chinese (Simplified) – Singapore • 4103 German – Luxembourg • 4105 English – Canada • 4106 Spanish – Guatemala • 4108 French – Switzerland • 5121 Arabic – Algeria • 5127 German – Liechtenstein • 5129 English – New Zealand • 5130 Spanish – Costa Rica • 5132 French – Luxembourg • 6145 Arabic – Morocco • 6153 English – Ireland • 6154 Spanish – Panama • 7169 Arabic – Tunisia • 7177 English – South Africa • 7178 Spanish – Dominican Republic • 8193 Arabic – Oman • 8201 English – Jamaica • 8202 Spanish – Venezuela • 9217 Arabic – Yemen • 9226 Spanish – Colombia • 10241 Arabic – Syria • 10249 English – Belize • 10250 Spanish – Peru • 11265 Arabic – Jordan • 11273 English – Trinidad • 11274 Spanish – Argentina • 12289 Arabic – Lebanon • 12298 Spanish – Ecuador • 13313 Arabic – Kuwait • 13322 Spanish – Chile • 14337 Arabic – U.A.E. • 14346 Spanish – Uruguay • 15361 Arabic – Bahrain • 15370 Spanish – Paraguay • 16385 Arabic – Qatar • 16394 Spanish – Bolivia • 17418 Spanish – El Salvador • 18442 Spanish – Honduras • 19466 Spanish – Nicaragua • 20490 Spanish – Puerto Rico
ProductID	string	This item stores an agent model.

Item name	Data type	Description
ProductID	string	When an empty character is stored, this item appears as follows: `"ProductID": ""`
PollingInterval	int	This item stores an interval (units: seconds) at which an agent polls the management server.
MngStatusUpdateTime	dateTime	This item stores a date and time when the management status of devices was updated. When an empty character is stored, this item appears as follows: `"MngStatusUpdateTime": ""`
AllIpAddress	string	This item stores all IP addresses (IPv4 and IPv6) held by a device. The IP addresses that are stored are represented by the following rules: • The IPv4 address is represented in decimal numbers separated by a period (`.`). • The IPv6 address is represented in hex numbers separated by a colon (:). • Each IP address is separated by a comma (`,`). • If all IP addresses are lined up and more than 512 characters are displayed, the output will be limited to 512 characters. When an empty character is stored, this item appears as follows: `"AllIpAddress": ""`
SnoozeDownloadStatus	int	This item stores a package download delay status. Specifically, one of the following values is stored: • 0: Not delayed • 1: Delayed
Domain	string	This item stores a domain or work group. When an empty character is stored, this item appears as follows: `"Domain": ""`
Manufacturer	string	This item stores a device model or manufacturer. When an empty character is stored, this item appears as follows: `"Manufacturer": ""`
NodeNameInt	int	This item stores a numeric-type host ID.
UUID	string	This item stores a UDID. When an empty character is stored, this item appears as follows: `"UUID": ""`
PhoneNumber	string	This item stores a contract phone number. When an empty character is stored, this item appears as follows: `"PhoneNumber": ""`
IMEI	string	This item stores a IMEI. When an empty character is stored, this item appears as follows: `"IMEI": ""`
RegistrationType	int	This item stores a management type. Specifically, one of the following values is stored: • 0: Online management • 1: Offline management
OsLastStartUpdateTime	dateTime	This item stores a date and time when the OS was last started. When an empty character is stored, this item appears as follows: `"OsLastStartUpdateTime": ""`

20.3.3 Installed software information list acquisition

This API acquires an installed software information list (list that shows information regarding the software programs installed on devices) from the management server.

The unit for one record of installed software information is not device unit, but installed software information of the device (Software object) unit. To obtain all software information installed on the device, use the following method.

Acquisition method

Get a list of device information. Obtain the installed software information of the device from the acquired device information. Include `NodeNameInt` (numeric host identifier) in the filter condition when acquiring the installed software information of the device. If the filter condition does not include `NodeNameInt` (numeric host identifier), it will take more time to acquire the information.

Execution permission

You need the following permission:

- API permission

API version

v1

Request format

Request line

```
GET /jp1itdm/api/v1/objects/devices_reference/softwares?filter HTTP/1.1
```

For *filter*, specify filter conditions for acquiring desired installed software information. For details, see *Filter conditions for acquiring installed software information*.

Request header

```
Host:host-name-or-IP-address-of-management-server:port-number-of-management-server
Accept-Language:language-code-in-the-message-of-response
Accept:application/json
Content-Type:application/json
X-ITDM-Authorization1:Base64-encoded-user-ID
X-ITDM-Authorization2:Base64-encoded-password
```

Request message body

None

Response format

Status line

Either a status code or its text is returned. For details, see the description of status codes in 20.2 Common API specifications.

Response header

For details, see the description of the response format in 20.2 Common API specifications.

Response message body

Under normal circumstances, the message body contains a device information list in JSON format. For details, see *Data format for installed software information*.

When an error occurs, error information is stored in JSON format. For details, see the description of the error information in 20.2 Common API specifications.

Filter conditions for acquiring installed software information

You can specify a filter condition for acquiring installed software information by inserting a query string in the request line. A query string to be used to specify filter conditions for acquiring installed software information should be in the following format:

```
count=number-of-records-to-acquire&offset=start-position-for-records&fields=
items-included-in-each-acquired-record&filters[1]=filter-condition-1&filter
s[2]=filter-condition-2...&filters[10]=filter-condition-10&sort=sort-conditi
on
```

Legend: ...: Repetitions of `&filters[n]=`*filter-condition-n* (*n* = 3 to 9)

Each item in the query string is described in detail below. All of these items are optional. When no query string is specified, a response returned will contain the maximum number of installed software information records that can be acquired.

count

Specify the number of installed software (Software Object) you want to acquire.

If you specify `0` or if you omit this parameter, it is assumed that 10,000 has been specified. Specifying a value that exceeds 10,000 will result in an error.

Example: When you want to acquire 1,000 installed software (Software Object), specify `count=1000`.

> **Note**
>
> The maximum number of information that can be acquired at one time by the installed software information list acquisition is 10,000.

offset

Specify the start position for the record of software information installed on the device to be acquired.

If you specify `0` or if you omit this parameter, installed software information records are acquired starting from the first record.

Example: When you want to acquire installed software information records starting from Record 1,001, specify `offset=1000`.

> **Note**
>
> Adding or deleting installed software information records during the acquisition of installed software information records can cause the start position to shift when you attempt to acquire the next set of installed software information records.
>
> If the records are shifted, some records may not be acquired (skipped) or duplicate records may be acquired.

fields

Specify the items you want included in each acquired installed software information record. For details about the specifiable items, see *Items that can be specified as filter conditions and the format of their values*. When you specify multiple items, use a comma (`,`) to separate them.

If you omit this parameter, each one of the acquired installed software information records will contain all items.

Example: If you want the acquired installed software information records to contain the host ID, host name, device type, and OS type of the individual devices, specify `fields=NodeID,HostName,EquipmentType,OsKind`.

filters[*n*]

Specify filter conditions for the installed software information records to be acquired. For details about filter conditions, see *Syntax for filter conditions*.

You can specify a maximum of 10 filter conditions. When there are 10 filter conditions, specify filter condition numbers from 1 to 10, in that order, by replacing each *n* with the corresponding number. Do not skip a filter condition number. For example, specifying the following filter conditions, in which filter condition number 3 is skipped, results in an error: `filters[1]=`*`filter-condition-1`*`&filters[2]=`*`filter-condition-2`*`&filters[4]=`*`filter-condition-4`*.

When you specify multiple filter conditions, only those installed software information records that satisfy all specified conditions are acquired.

sort

Specify items to be used to sort the acquired installed software information records. Select from the items listed under *Items that can be specified as filter conditions and the format of their values*. To sort the acquired device information records in the descending order of the values corresponding to a certain item, prefix the item name with a minus sign (-).

When you specify multiple item names, separate them with a comma (`,`). When multiple items are specified, the acquired installed software information records are first sorted according to the first item specified, and the resulting records are further sorted according to the second item specified, and so on.

If you omit this parameter, it is assumed that `sort=NodeID,SoftwareName,SoftwareVersion,SoftwarePublisher` is specified.

Example: To sort acquired installed software information records in ascending order of device type, and then sort the resulting records in descending order of last updated date and time, specify `sort=EquipmentType,-LastUpdateTime`.

> **Note**
>
> If you specify `sort` parameter, it is assumed that `,NodeID,SoftwareName,SoftwareVersion,SoftwarePublisher` is specified in end of the parameter.

> **Note**
>
> An error occurs if the total value for the `count` parameter and `offset` parameter exceeds 2,147,483,647. An error also occurs if the `count` parameter is not specified or `0` is specified for the `count` parameter, and the total value for the upper limit for the `count` parameter and the `offset` parameter exceeds 2,147,483,647.

> **Note**
>
> The following symbols cannot be used in the item names specified in the `fields` parameter, `filters[n]` parameter, or `sort` parameter.
>
> single quotation mark (`'`), double quotation mark (`"`), space, tab, left curly bracket (`{`), right curly bracket (`}`), left square bracket (`[`), right square bracket (`]`), left parenthesis (`(`), right parenthesis (`)`), backslash (`\`), colon (`:`), semicolon (`;`), asterisk (`*`), question mark (`?`), equal sign (=), hyphen (-), and vertical bar (`|`)

Syntax for filter conditions

Use the following syntax to specify a filter condition for `filters[n]`:

When an operator other than `in()` or `not in()` is to be used:

```
filters[n]=item-nameΔoperatorΔ'value'
```

When `in()` or `not in()` is to be used as an operator:

```
filters[n]=item-nameΔin('value-1','value-2'...)
filters[n]=item-nameΔnotΔin('value-1','value-2'...)
```

Legend:

...: Repetitions of `,'value-n'`

Δ: One space character

Important

Only one space should be written at Δ. If the space is used in not specified at Δ or if two or more spaces are written, an error occurs.

n

Specify a filter condition number. Filter conditions must be numbered serially from 1 to 10.

item-name

Specify a filter condition by selecting from the item names listed under *Items that can be specified as filter conditions and the format of their values*.

operator

Specify an operator for the filter condition. The following table shows specifiable operators.

Operator	Description	Example
=	Acquires installed software information records whose *value* corresponding to the specified *item-name* matches the specified value.	`filters[1]=HostName = 'host01'` Acquires installed software information records whose host name is `host01`.
!=	Acquires installed software information records whose *value* corresponding to the specified *item-name* does not match the specified value.	`filters[1]=HostName != 'host01'` Acquires installed software information records whose host name is something other than `host01`.
>	Acquires installed software information records whose *value* corresponding to the specified *item-name* is larger than the specified value.	filters[1]=StandbyTimeoutAC > '60' Acquires installed software information records whose time to system standby (AC) is longer than 60 seconds. filters[1]=LastUpdateTime > '2020-04-01' Acquires installed software information records whose last updated date and time is after `2020-04-01T00:00:00.000Z`.
<	Acquires installed software information records whose *value* corresponding to the specified *item-name* is smaller than the specified value.	filters[1]=StandbyTimeoutAC < '60' Acquires installed software information records whose time to system standby (AC) is shorter than 60 seconds. filters[1]=LastUpdateTime < '2020-04-01' Acquires installed software information records whose last updated date and time is before `2020-04-01T00:00:00.000Z`.

Operator	Description	Example
>=	Acquires installed software information records whose *value* corresponding to the specified *itemname* is equal to or larger than the specified value.	filters[1]=StandbyTimeoutAC >= '60' Acquires installed software information records whose time to system standby (AC) is equal to or longer than 60 seconds. filters[1]=LastUpdateTime >= '2020-04-01' Acquires installed software information records whose last updated date and time is `2020-04-01T00:00:00.000Z` or later.
<=	Acquires installed software information records whose *value* corresponding to the specified *itemname* is equal to or smaller than the specified value.	filters[1]=StandbyTimeoutAC <= '60' Acquires installed software information records whose time to system standby (AC) is equal to or shorter than 60 seconds. filters[1]=LastUpdateTime <= '2020-04-01' Acquires installed software information records whose last updated date and time is `2020-04-01T00:00:00.000Z` or earlier.
in()	Acquires installed software information records whose *value* corresponding to the specified *itemname* matches one of the values listed in parentheses. The listed values are individually enclosed in single quotation marks (`'`) and separated with a comma (`,`) in between. The maximum number of values that can be specified in the in() clause is 100.	`filters[1]=OsKind in('1','2','3')` Acquires installed software information records whose OS type is `1` (Windows), `2` (Linux), or `3` (UNIX).
not in()	Acquires installed software information records whose *value* corresponding to the specified *itemname* does not match any of the values listed in parentheses. The listed values are individually enclosed in single quotation marks (`'`) and separated with a comma (`,`) in between. The maximum number of values that can be specified in the not in() clause is 100.	`filters[1]=OsKind not in('1','2','3')` Acquires installed software information records whose OS type is something other than `1` (Windows), `2` (Linux), or `3` (UNIX).
like	Acquires installed software information records whose *value* corresponding to the specified *itemname* matches a string in the specified value. This operator distinguishes between uppercase and lowercase letters in a string contained in the *value*. You can use a wildcard (`%`) in a string contained in the specified *value*. % Represents a string of any length, including 0 length. When the specified value contains a string that contains a underscore (_), percent sign (`%`) or backslash (\), replace it with `\_`, `\%` or `\\`.	filters[1]=HostName like 'TestPC' Acquires installed software information records whose host name is `TestPC`. filters[1]=HostName like 'Test%' Acquires installed software information records whose host name starts with the string `Test`. filters[1]=HostName like '%Test%' Acquires installed software information records whose host name contains the string `Test`.
not like	Acquires installed software information records whose *value* corresponding to the specified *itemname* does not match a string in the specified value.	filters[1]=HostName not like 'TestPC' Acquires installed software information records whose host name is something other than `TestPC`. filters[1]=HostName not like 'Test%'

Operator	Description	Example
not like	This operator distinguishes between uppercase and lowercase letters in a string contained in the *value*. You can use a wildcard (%) in a string contained in the specified *value*. % Represents a string of any length, including 0 length. When the specified value contains a string that contains a underscore (_), percent sign (%) or backslash (\), replace it with _, \% or \\.	Acquires installed software information records whose host name does not start with the string Test. filters[1]=HostName not like '%Test%' Acquires installed software information records whose host name does not contain the string Test.

value

Specify a value for the filter condition.

For details about the data type of the item name to be specified, see *Items that can be specified as filter conditions and the format of their values*. For details about the coding format appropriate to each data type, see the information provided under Supported data types in 20.2 Common API specifications. Remember that you have to enclose a string in single quotation marks (') to specify a value.

Note

The format to be used to specify a value for the dateTime-type item names varies depending on the operator used.

When using = or != as the operator

Specify the value in the '*YYYY-MM-DD*T*HH*:*MM*:*SS*.*sss*Z' format.

When using >, >=, < or <= as the operator

The basic format being '*YYYY-MM-DD*T*HH*:*MM*:*SS*.*sss*Z', you only have to specify up to a desired point in this format.

For example, if you specify filters[1]=LastUpdateTime<'2020-04', installed software information records whose last updated date and time is earlier than 2020-04-01T00:00:00.000Z are acquired.

Note

If a string containing single quotation mark (') is specified as a *value*, it must be replaced with two single quotation marks ('').

Items that can be specified as filter conditions and the format of their values

The following table describes the items that can be specified as filter conditions and the format of their values:

Item name	Data type	Description
NodeID	string	Specify this item to filter device information records by host ID.
HostName	string	Specify this item to filter device information records by host name.
IPAddress	string	Specify this item to filter device information records by IP address. This value must be expressed as a string by using the IPv4 format *xxx*.*xxx*.*xxx*.*xxx* (where *xxx* represents a number in the range of 0-255).

Item name	Data type	Description
IPAddress	string	When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`.
MACAddress	string	Specify this item to filter device information records by MAC address. This value must be in the *xx*`:`*xx*`:`*xx*`:`*xx*`:`*xx*`:`*xx* format or expressed as a string using the format *xx*`-`*xx*`-`*xx*`-`*xx*`-`*xx*`-`*xx* (where *x* represents a number in the range of 0-9 or a letter in the range of A-F or a-f). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`.
CreateTime	dateTime	Specify this item to filter device information records by created date and time.
LastUpdateTime	dateTime	Specify this item to filter device information records by last updated date and time.
LastAliveDate	dateTime	Specify this item to filter device information records by date and time when a computer-to-management server connection was last confirmed.
IPSubnet	string	Specify this item to filter device information records by subnet mask. This value must be expressed as a string by using the IPv4 format *xxx*`.`*xxx*`.`*xxx*`.`*xxx* (where *xxx* represents a number in the range of 0-255). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`.
EquipmentType	string	Specify this item to filter device information records by device type. You can specify one of the following values: • `EquipmentTypeComputer`: PC • `EquipmentTypeServer`: Server • `EquipmentTypeStorage`: Storage device • `EquipmentTypeNetworkDevice`: Network device • `EquipmentTypePrinter`: Printer device • `EquipmentTypePeripheralDevice`: Peripheral device • `EquipmentTypeUSBMemory`: USB memory • `EquipmentTypeDisplay`: Display • `EquipmentTypeSmartDevice`: Smart device • `EquipmentTypeOther`: Other device • `EquipmentTypeUnknown`: Unknown device • `EquipmentTypeUser`: Device type added by the administrator user
EquipmentUserType	string	Specify this item to filter device information records by name of user definition optionally added by the administrator user.
OsKind	int	Specify this item to filter device information records by OS type. You can specify one of the following values: • `0`: Unknown • `1`: Windows • `2`: Linux • `3`: UNIX • `4`: Mac OS • `5`: OS for smart devices • `6`: HP-UX • `7`: Solaris • `8`: AIX
AMTFirmwareVersion	string	Specify this item to filter device information records by AMT firmware version.
AgentType	int	Specify this item to filter device information records by management type. You can specify one of the following values:

Item name	Data type	Description
AgentType	int	• 0: Agent Management • 1: Agentless Management • 2: Agent Management(Network Access Control) • 4: Agent Management(Site Server) • 6: Agent Management(Site server)(Network Access Control) • 9: MDM Linkage Management • 16: Agent Management(Relaysystem) • 18: Agent Management(Relaysystem)(Network Access Control) • 32: Management Relay Server • 34: Management Relay Server(Network Access Control) • 65: API management
AgentVersion	string	Specify this item to filter device information records by agent version.
DistributionRegDate	dateTime	Specify this item to filter device information records by distribution date and time.
AgentDistributionStatus	int	Specify this item to filter device information records by agent distribution status. You can specify one of the following values: • 0: Not distributed yet (default value) • 1: Waiting to be distributed • 11: Currently being distributed • 51: Failed distribution attempt (distribution is being retried) • 52: Failed distribution attempt (with failed retry attempt) • 999: Agent installer started
AgentDistributionErrorType	int	Specify this item to filter device information records by error description provided after a failed agent distribution attempt. You can specify one of the following values: • 0: (Default) • 1: Authentication error • 2: Communication error • 3: Installation-in-progress error • 4: Waiting-for-PC-to-start error • 5: Other error • 101: An agent has not been registered. • 102: User authentication failed. • 103: Failed to access administrative shares. • 104: Failed to access the client. • 105: A communication error occurred. • 106: The MAC address is different from the registered one. • 107: An agent has already been installed. • 108: No notification of success has arrived from the agent. • 109: The client failed to resolve the manager's host name. • 110: Authentication information has not been specified. • 111: An error occurred during the creation of agent installation media. • 112: The agent installer is currently running. • 113: The agent installer did not finish. • 201: Failed decompression attempt • 202: Required-OS error • 203: User-permissions error • 204: Failed installation attempt
AgentStatus	int	Specify this item to filter device information records by device management status.

Item name	Data type	Description
AgentStatus	int	You can specify one of the following values: • 0: Managed • 1: Excluded • 2: Discovered
DiscoverTime	dateTime	Specify this item to filter device information records by discovered date and time.
AuthStatus	int	Specify this item to filter device information records by detailed device status. You can specify one of the following values: • 0: Running normally (default value) • 1: (Status of the discovered device) An authentication error occurred. • 2: (Status of the discovered device) The computer is not running. • 101: (Printer status) Needing attention of maintenance personnel • 102: (Printer status) Cover open • 103: (Printer status) Paper jam • 104: (Printer status) Paper feeding tray missing • 105: (Printer status) Paper receiving tray missing • 106: (Printer status) Consumable items lost • 107: (Printer status) Toner empty • 108: (Printer status) Paper receiving tray full • 109: (Printer status) Out of paper • 110: (Printer status) Paper feeding tray empty • 111: (Printer status) Toner low • 112: (Printer status) Paper low • 113: (Printer status) Paper receiving tray almost full • 114: (Printer status) A communication error occurred. • 115: (Printer status) Timing of preventive maintenance due to expiry • 999: Unknown • 1350: (Site server status) A fatal error occurred. • 1360: (Site server status) The database was blocked. • 3060: (Site server status) An attempt to install the site server failed. • 3070: (Site server status) An attempt to uninstall the site server failed. • 3160: (Network monitor status) The network monitor services stopped. • 3260: (Site server status) The site server services stopped. • 3365: (Site server status) No free space left in the folder storing the operation log database. • 3370: (Site server status) No free disk space left on the drive that contains the folder storing the operation log. • 3375: (Site server status) The folder storing the operation log database is low on free space. • 3380: (Site server status) The drive that contains the folder storing the operation log is low on disk space. • 3470: (Site server status) No disk space left on the drive that contains the data folder. • 3480: (Site server status) The drive that contains the data folder is low on disk space. • 3680: (Network monitor/site server status) The computer is not running. • 3850: (Smart device status) The smart device was initialized.
NetworkStatus	int	Specify this item to filter device information records by connection status. You can specify one of the following values: • 0: Allowed • 1: Blocked • 2: Forcibly blocked

Item name	Data type	Description
NetworkStatus	int	• 3: Outside the period of use • 999: Unknown
AgentDeviceStatus	int	Specify this item to filter device information records by device status. You can specify one of the following values: • 0: Running • 1: Not running • 2: Warning • 3: Failure • 999: Unknown • 1100: Not applicable
DiscoveryProtocol	int	Specify this item to filter device information records by method used to collect device information from agentless devices. You can specify one of the following values: • 0: Administrative shares • 1: Remote WMI • 2: SNMP • 3: ICMP • 4: ARP • 5: Active Directory • 6: MDM • 999: Unknown
Caption	string	Specify this item to filter device information records by OS name.
AllMacAddress	string	Specify this item to filter device information records by all MAC addresses held by a device. This value must be in the *xx*:*xx*:*xx*:*xx*:*xx*:*xx* format or expressed as a string using the format *xx*-*xx*-*xx*-*xx*-*xx*-*xx* (where *x* represents a number in the range of 0-9 or a letter in the range of A-F or a-f). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`. If the specified value exceeds the maximum length allowed, only those specified MAC addresses that fit within the allowed length become valid.
InstallCompletionDate	dateTime	Specify this item to filter device information records by date and time when the distribution of the agent was completed.
CSDVersion	string	Specify this item to filter device information records by OS Service Pack.
IEVersion	string	Specify this item to filter device information records by Internet Explorer version.
UnnecessaryServicecnt	int	Specify this item to filter device information records by number of Windows services prohibited by security policies.
VideoTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to monitor shutdown (AC).
VideoTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to monitor shutdown (DC).
StandbyTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to entering system standby (AC).
StandbyTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to entering system standby (DC).
HibernateTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to entering system hibernation state (AC).

Item name	Data type	Description
HibernateTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to entering system hibernation state (DC).
SpindownTimeoutAC	int	Specify this item to filter device information records by time (units: seconds) to hard disk shutdown (AC).
SpindownTimeoutDC	int	Specify this item to filter device information records by time (units: seconds) to hard disk shutdown (DC).
OsLanguage	int	Specify this item to filter device information records by OS language. You can specify one of the following values: • 1 Arabic • 4 Chinese (Simplified)– China • 9 English • 1025 Arabic – Saudi Arabia • 1026 Bulgarian • 1027 Catalan • 1028 Chinese (Traditional) – Taiwan • 1029 Czech • 1030 Danish • 1031 German – Germany • 1032 Greek • 1033 English – United States • 1034 Spanish – Traditional Sort • 1035 Finnish 1036 French – France • 1037 Hebrew • 1038 Hungarian • 1039 Icelandic • 1040 Italian – Italy • 1041 Japanese • 1042 Korean • 1043 Dutch – Netherlands • 1044 Norwegian – Bokmal • 1045 Polish • 1046 Portuguese – Brazil • 1047 Rhaeto-Romanic • 1048 Romanian • 1049 Russian • 1050 Croatian • 1051 Slovak • 1052 Albanian • 1053 Swedish • 1054 Thai • 1055 Turkish • 1056 Urdu • 1057 Indonesian • 1058 Ukrainian • 1059 Belarusian • 1060 Slovenian • 1061 Estonian • 1062 Latvian • 1063 Lithuanian • 1065 Persian • 1066 Vietnamese

Item name	Data type	Description
OsLanguage	int	• 1069 Basque • 1070 Serbian • 1071 Macedonian (F.Y.R.O. Macedonia) • 1072 Sutu • 1073 Tsonga • 1074 Tswana • 1076 Xhosa • 1077 Zulu • 1078 Afrikaans • 1080 Faeroese • 1081 Hindi • 1082 Maltese • 1084 Gaelic • 1085 Yiddish • 1086 Malay – Malaysia • 2049 Arabic – Iraq • 2052 Chinese (Simplified) – PRC • 2055 German – Switzerland • 2057 English – United Kingdom • 2058 Spanish – Mexico • 2060 French – Belgium • 2064 Italian – Switzerland • 2067 Dutch – Belgium • 2068 Norwegian – Nynorsk • 2070 Portuguese – Portugal • 2072 Romanian – Moldova • 2073 Russian – Moldova • 2074 Serbian – Latin • 2077 Swedish – Finland • 3073 Arabic – Egypt • 3076 Chinese (Traditional) – Hong Kong SAR • 3079 German – Austria • 3081 English – Australia • 3082 Spanish – International Sort • 3084 French – Canada • 3098 Serbian – Cyrillic • 4097 Arabic – Libya • 4100 Chinese (Simplified) – Singapore • 4103 German – Luxembourg • 4105 English – Canada • 4106 Spanish – Guatemala • 4108 French – Switzerland • 5121 Arabic – Algeria • 5127 German – Liechtenstein • 5129 English – New Zealand • 5130 Spanish – Costa Rica • 5132 French – Luxembourg • 6145 Arabic – Morocco • 6153 English – Ireland • 6154 Spanish – Panama • 7169 Arabic – Tunisia • 7177 English – South Africa

Item name	Data type	Description
OsLanguage	int	• 7178 Spanish – Dominican Republic • 8193 Arabic – Oman • 8201 English – Jamaica • 8202 Spanish – Venezuela • 9217 Arabic – Yemen • 9226 Spanish – Colombia • 10241 Arabic – Syria • 10249 English – Belize • 10250 Spanish – Peru • 11265 Arabic – Jordan • 11273 English – Trinidad • 11274 Spanish – Argentina • 12289 Arabic – Lebanon • 12298 Spanish – Ecuador • 13313 Arabic – Kuwait • 13322 Spanish – Chile • 14337 Arabic – U.A.E. • 14346 Spanish – Uruguay • 15361 Arabic – Bahrain • 15370 Spanish – Paraguay • 16385 Arabic – Qatar • 16394 Spanish – Bolivia • 17418 Spanish – El Salvador • 18442 Spanish – Honduras • 19466 Spanish – Nicaragua • 20490 Spanish – Puerto Rico
ProductID	string	Specify this item to filter device information records by agent model.
PollingInterval	int	Specify this item to filter device information records by interval (units: seconds) at which an agent polls the management server.
MngStatusUpdateTime	dateTime	Specify this item to filter device information records by date and time when the management status of devices was updated.
AllIpAddress	string	Specify this item to filter device information records by all IP addresses held by the individual devices. This value must be expressed as a string by using the IPv4 format *xxx*`.`*xxx*`.`*xxx*`.`*xxx* (where *xxx* represents a number in the range of 0-255), or the IPv6 format *xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx*`:`*xxxx* (*x*: one character from 0-9, A-F, or a-f). When using `like` or `not like` as the operator, remember to suffix the specified value with the wildcard character `%`. If the specified value exceeds the maximum length allowed, only those specified IP addresses that fit within the allowed length become valid.
SnoozeDownloadStatus	int	Specify this item to filter device information records by package download delay status. You can specify one of the following values: • 0: Not delayed • 1: Delayed
Domain	string	Specify this item to filter device information records by domain or work group.
Manufacturer	string	Specify this item to filter device information records by device model or manufacturer.

Item name	Data type	Description
NodeNameInt	int	Specify this item to filter device information records by numeric-type host ID.
UUID	string	Specify this item to filter device information records by UDID.
PhoneNumber	string	Specify this item to filter device information records by contract phone number.
IMEI	string	Specify this item to filter device information records by IMEI.
RegistrationType	int	Specify this item to filter device information records by management type. You can specify one of the following values: • 0: Online management • 1: Offline management
OsLastStartUpdateTime	dateTime	Specify this item to filter device information records by date and time when the OS was last started.
InstallDate	dateTime	Specify this item to filter installed software information records by installation date.
SourceKind	int	Specify this item to filter installed software information records by method used to collect software information. You can specify one of the following values: • 1: Added to **Programs and Features** • 2: **Software Search List**
InstallPath	string	Specify this item to filter installed software information records by installation folder.
BgStatus	int	Specify this item to filter installed software information records by status that shows how software information is being processed internally. You can specify one of the following values: • 0: Processing completed. • 1: Addition processing is in progress. • 2: Deletion processing is in progress.
SoftwareProductID	string	Specify this item to filter installed software information records by product ID.
GUID	int	Specify this item to filter installed software information records by GUID.
SoftwareName	string	Specify this item to filter installed software information records by software name.
SoftwareVersion	string	Specify this item to filter installed software information records by version.
SoftwarePublisher	string	Specify this item to filter installed software information records by manufacturer.
SoftwareType	int	Specify this item to filter installed software information records by software information type. You can specify one of the following values: • 1: Added to **Programs and Features** • 2: **Software Search List** • 3: Program updates
RegistrationDate	dateTime	Specify this item to filter installed software information records by registration date and time.
HelpLink	string	Specify this item to filter installed software information records by support information (URL).
SoftwareCheck	int	Specify this item to filter installed software information records by check status. You can specify one of the following values: • 0: Not checked • 1: Checked
ImportantSoft	int	Specify this item to filter installed software information records by whether the software in question is a Microsoft Office product.

Item name	Data type	Description
ImportantSoft	int	You can specify one of the following values: • 0: The software is not a Microsoft Office product. • 1: The software is a Microsoft Office product.
AppType	int	Specify this item to filter installed software information records by application type. You can specify one of the following values: • 0: Software other than Windows Store apps • 1: Windows Store app
MSProductType	int	Specify this item to filter installed software information records by purchasing status of Microsoft Office products. You can specify one of the following values: • 0: Volume license version • 1: Full-product version
MSProductId	string	Specify this item to filter installed software information records by Microsoft Office product ID.

Data format for installed software information

Installed software information has the following data format:

```
{
    "DeviceSoftwareList": [
    {
        "DeviceSoftware": {
            "NodeID": "host-ID",
            "HostName": "host-name",
            "IPAddress": "IP-address",
            "MACAddress": "MAC-address",
            "CreateTime": "created-date-and-time",
            "LastUpdateTime": "last-updated-date-and-time",
            "LastAliveDate": "date-and-time-last-confirmed",
            "IPSubnet": "subnet-mask",
            "EquipmentType": "device-type",
            "EquipmentUserType": "device-type-name-added-by-the-administrato
r-user",
            "OsKind": "OS-type",
            "AMTFirmwareVersion": "AMT-firmware-version",
            "AgentType": "management-type",
            "AgentVertsion": "agent-version",
            "DistributionRegDate": "distribution-date-and-time",
            "AgentDistributionStatus": "agent-distribution-status",
            "AgentDistributionErrorType": "error-description-provided-after-
failed-agent-distribution",
            "AgentStatus": "device-management-status",
            "DiscoverTime": "discovered-date-and-time",
            "AuthStatus": "detailed-device-status",
            "NetworkStatus": "connection-status",
            "AgentDeviceStatus": "device-status",
            "DiscoveryProtocol": "method-used-to-collect-device-information-
from-agentless-devices",
            "Caption": "OS-name",
            "AllMacAddress": "all-MAC-addresses-held-by-a-device",
            "InstallCompletionDate": "date-and-time-when-the-distribution-of
-the-agent-was-completed",
            "CSDVersion": "OS-Service-Pack",
```

```
            "IEVersion": "Internet Explorer version",
            "UnnecessaryServicecnt": "number-of-Windows-services-prohibited-
by-security-policies",
            "VideoTimeoutAC": "time-(units:seconds)-to-monitor-shutdown-(AC)
",
            "VideoTimeoutDC": "time-(units:seconds)-to-monitor-shutdown-(DC)
",
            "StandbyTimeoutAC": "time-(units:seconds)-to-entering-system-sta
ndby-(AC)",
            "StandbyTimeoutDC": "time-(units:seconds)-to-entering-system-sta
ndby-(DC)",
            "HibernateTimeoutAC": "time-(units:seconds)-to-entering-system-h
ibernation-state-(AC)",
            "HibernateTimeoutDC": "time-(units:seconds)-to-entering-system-h
ibernation-state-(DC)",
            "SpindownTimeoutAC": "time-(units:seconds)-to-hard-disk-shutdown
-(AC)",
            "SpindownTimeoutDC": "time-(units:seconds)-to-hard-disk-shutdown
-(DC)",
            "OsLanguage": "OS-language",
            "ProductID": "agent-model",
            "PollingInterval": "interval-(units:seconds)-at-agent-polls-mana
gement-server",
            "MngStatusUpdateTime": "updated-date-and-time-management-status"
,
            "AllIpAddress": "all-IP-addresses-held-by-a-device",
            "SnoozeDownloadStatus": "package-download-delay-status",
            "Domain": "domain-or-work-group",
            "Manufacturer": "device-model-or-manufacturer",
            "NodeNameInt": "numeric-type-host-ID",
            "UUID": "UDID",
            "PhoneNumber": "contract-phone-number",
            "IMEI": "IMEI",
            "RegistrationType": "management-type",
            "OsLastStartUpdateTime": "date-and-time-when-OS-last-started",
            "SoftwareList": [
            {
                "Software": {
                    "InstallDate": "installation-date",
                    "SourceKind": "method-used-to-collect-software-informati
on",
                    "InstallPath": "installation-folder",
                    "BgStatus": "status-of-internally-processed-software-inf
ormation",
                    "SoftwareProductID": "product-ID",
                    "GUID": "GUID",
                    "SoftwareName": "software-name",
                    "SoftwareVersion": "version",
                    "SoftwarePublisher": "manufacturer",
                    "SoftwareType": "software-information-type",
                    "RegistrationDate": "registration-date-and-time",
                    "HelpLink": "support-information-(URL)",
                    "SoftwareCheck": "check-status",
                    "ImportantSoft": "whether-the-software-is-a-Microsoft-Of
fice-product",
                    "AppType": "application-type",
                    "MSProductType": "purchasing-type-of-Microsoft-Office-pr
oduct",
```

```
                    "MSProductId": "Microsoft-Office-product-ID"
                }, ...
            }
            ]
        }, ...
    }
    ],
    "offset": "start-position-of-the-installed-software-information-records"
,
    "responseCount": "number-of-acquired-installed-software-information-reco
rds",
    "totalCount": "total-number-of-installed-software-information-records-ma
tching-the-specified-filters"}
}
```

Legend: ...: Iterations of the previous layer

DeviceSoftwareList

Item name	Data type	Mandatory / Optional	Description
DeviceSoftwareList	Array	Mandatory	Root name of installed software information. This item stores arrays of `DeviceSoftware` objects.
DeviceSoftware	Object	Mandatory	Object name of an installed software information record. For details, see *DeviceSoftware object*.
offset	int	Mandatory	This item stores the start position of the device information records included in the current response data.
responseCount	int	Mandatory	This item stores the number of acquired device information records included in the current response data. To request the next set of device information records, calculate the sum of the `offset` value and the `responseCount` value, which must not exceed the `totalCount` value, and specify it for `offset` in the query string of the request.
totalCount	int	Mandatory	This item stores the total number of device information records matching the filters specified in the query string of the request.

DeviceSoftware object

Although the `SoftwareList` array and the `Software` object are mandatory, all the other `DeviceSoftware` object items are optional.

Item name	Data type	Description
NodeID	string	This item stores a host ID.
HostName	string	This item stores a host name. When an empty character is stored, this item appears as follows: `"HostName": ""`
IPAddress	string	This item stores an IP (IPv4) address. When there are multiple IP addresses, the one that was used to send a notification to the management server is stored. When an empty character is stored, this item appears as follows: `"IPAddress": ""`
MACAddress	string	This item stores a MAC address.

Item name	Data type	Description
MACAddress	string	When an empty character is stored, this item appears as follows: `"MACAddress": ""`
CreateTime	dateTime	This item stores a created date and time. When an empty character is stored, this item appears as follows: `"CreateTime": ""`
LastUpdateTime	dateTime	This item stores a last updated date and time. When an empty character is stored, this item appears as follows: `"LastUpdateTime": ""`
LastAliveDate	dateTime	This item stores a date and time when a computer-to-management server connection was last confirmed. When an empty character is stored, this item appears as follows: `"LastAliveDate": ""`
IPSubnet	string	This item stores the subnet mask corresponding to the IP address stored in `IPAddress`. When an empty character is stored, this item appears as follows: `"IPSubnet": ""`
EquipmentType	string	This item stores a device type. Specifically, one of the following device types is stored: • `EquipmentTypeComputer`: PC • `EquipmentTypeServer`: Server • `EquipmentTypeStorage`: Storage device • `EquipmentTypeNetworkDevice`: Network device • `EquipmentTypePrinter`: Printer device • `EquipmentTypePeripheralDevice`: Peripheral device • `EquipmentTypeUSBMemory`: USB memory • `EquipmentTypeDisplay`: Display • `EquipmentTypeSmartDevice`: Smart device • `EquipmentTypeOther`: Other device • `EquipmentTypeUnknown`: Unknown device • `EquipmentTypeUser`: Device type added by the administrator user
EquipmentUserType	string	This item stores the name of the user definition optionally added by the administrator user. When an empty character is stored, this item appears as follows: `"EquipmentUserType": ""`
OsKind	int	This item stores an OS type. Specifically, one of the following values is stored: • `0`: Unknown • `1`: Windows • `2`: Linux • `3`: UNIX • `4`: Mac OS • `5`: OS for smart devices • `6`: HP-UX • `7`: Solaris • `8`: AIX
AMTFirmwareVersion	string	This item stores an AMT firmware version. When an empty character is stored, this item appears as follows: `"AMTFirmwareVersion": ""`

Item name	Data type	Description
AgentType	int	This item stores a management type. Specifically, one of the following values is stored: • 0: Agent Management • 1: Agentless Management • 2: Agent Management(Network Access Control) • 4: Agent Management(Site Server) • 6: Agent Management(Site server)(Network Access Control) • 9: MDM Linkage Management • 16: Agent Management(Relaysystem) • 18: Agent Management(Relaysystem)(Network Access Control) • 32: Management Relay Server • 34: Management Relay Server(Network Access Control) • 65: API management
AgentVersion	string	This item stores an agent version. When an empty character is stored, this item appears as follows: "AgentVersion": ""
DistributionRegDate	dateTime	This item stores a distribution date and time. When an empty character is stored, this item appears as follows: "DistributionRegDate": ""
AgentDistributionStatus	int	This item stores an agent distribution status. Specifically, one of the following values is stored: • 0: Not distributed yet (default value) • 1: Waiting to be distributed • 11: Currently being distributed • 51: Failed distribution attempt (distribution is being retried) • 52: Failed distribution attempt (with failed retry attempt) • 999: Agent installer started
AgentDistributionErrorType	int	This item stores an error description provided after a failed agent distribution attempt. Specifically, one of the following values is stored: • 0: (Default) • 1: Authentication error • 2: Communication error • 3: Installation-in-progress error • 4: Waiting-for-PC-to-start error • 5: Other error • 101: An agent has not been registered. • 102: User authentication failed. • 103: Failed to access administrative shares. • 104: Failed to access the client. • 105: A communication error occurred. • 106: The MAC address is different from the registered one. • 107: An agent has already been installed. • 108: No notification of success has arrived from the agent. • 109: The client failed to resolve the manager's host name. • 110: Authentication information has not been specified. • 111: An error occurred during the creation of agent installation media. • 112: The agent installer is currently running. • 113: The agent installer did not finish.

Item name	Data type	Description
AgentDistributionErrorType	int	• `201`: Failed decompression attempt • `202`: Required-OS error • `203`: User-permissions error • `204`: Failed installation attempt
AgentStatus	int	This item stores a device management status. Specifically, one of the following values is stored: • `0`: Managed • `1`: Excluded • `2`: Discovered
DiscoverTime	dateTime	This item stores a discovered date and time. When an empty character is stored, this item appears as follows: `"DiscoverTime": ""`
AuthStatus	int	This item stores a detailed device status. Specifically, one of the following values is stored: • 0: Running normally (default value) • 1: (Status of the discovered device) An authentication error occurred. • 2: (Status of the discovered device) The computer is not running. • 101: (Printer status) Needing attention of maintenance personnel • 102: (Printer status) Cover open • 103: (Printer status) Paper jam • 104: (Printer status) Paper feeding tray missing • 105: (Printer status) Paper receiving tray missing • 106: (Printer status) Consumable items lost • 107: (Printer status) Toner empty • 108: (Printer status) Paper receiving tray full • 109: (Printer status) Out of paper • 110: (Printer status) Paper feeding tray empty • 111: (Printer status) Toner low • 112: (Printer status) Paper low • 113: (Printer status) Paper receiving tray almost full • 114: (Printer status) A communication error occurred. • 115: (Printer status) Timing of preventive maintenance due to expiry • 999: Unknown • 1350: (Site server status) A fatal error occurred. • 1360: (Site server status) The database was blocked. • 3060: (Site server status) An attempt to install the site server failed. • 3070: (Site server status) An attempt to uninstall the site server failed. • 3160: (Network monitor status) The network monitor services stopped. • 3260: (Site server status) The site server services stopped. • 3365: (Site server status) No free space left in the folder storing the operation log database. • 3370: (Site server status) No free disk space left on the drive that contains the folder storing the operation log. • 3375: (Site server status) The folder storing the operation log database is low on free space. • 3380: (Site server status) The drive that contains the folder storing the operation log is low on disk space. • 3470: (Site server status) No disk space left on the drive that contains the data folder. • 3480: (Site server status) The drive that contains the data folder is low on disk space.

Item name	Data type	Description
AuthStatus	int	• 3680: (Network monitor/site server status) The computer is not running. • 3850: (Smart device status) The smart device was initialized.
NetworkStatus	int	This item stores a connection status. Specifically, one of the following values is stored: • 0: Allowed • 1: Blocked • 2: Forcibly blocked • 3: Outside the period of use • 999: Unknown
AgentDeviceStatus	int	This item stores a device status. Specifically, one of the following values is stored: • 0: Running • 1: Not running • 2: Warning • 3: Failure • 999: Unknown • 1100: Not applicable
DiscoveryProtocol	int	This item stores a method used to collect device information from agentless devices. Specifically, one of the following values is stored: • 0: Administrative shares • 2: SNMP • 3: ICMP • 4: ARP • 5: Active Directory • 6: MDM • 999: Unknown
Caption	string	This item stores an OS name. When an empty character is stored, this item appears as follows: `"Caption": ""`
AllMacAddress	string	This item stores all MAC addresses held by a device. The MAC addresses that are stored are represented by the following rules: • The MAC address is expressed in hexadecimal, separated by a colon (`:`). • Each MAC address is separated by a comma (`,`). • If all MAC addresses are lined up and more than 512 characters are displayed, the output will be limited to 512 characters. When an empty character is stored, this item appears as follows: `"AllMacAddress": ""`
InstallCompletionDate	dateTime	This item stores a date and time when the distribution of the agent was completed. When an empty character is stored, this item appears as follows: `"InstallCompletionDate": ""`
CSDVersion	string	This item stores an OS Service Pack. When an empty character is stored, this item appears as follows: `"CSDVersion": ""`
IEVersion	string	This item stores an Internet Explorer version. When an empty character is stored, this item appears as follows: `"IEVersion": ""`
UnnecessaryServicecnt	int	This item stores a number of Windows services prohibited by security policies.
VideoTimeoutAC	int	This item stores a time (units: seconds) to monitor shutdown (AC).

Item name	Data type	Description
VideoTimeoutDC	int	This item stores a time (units: seconds) to monitor shutdown (DC).
StandbyTimeoutAC	int	This item stores a time (units: seconds) to entering system standby (AC).
StandbyTimeoutDC	int	This item stores a time (units: seconds) to entering system standby (DC).
HibernateTimeoutAC	int	This item stores a time (units: seconds) to entering system hibernation state (AC).
HibernateTimeoutDC	int	This item stores a time (units: seconds) to entering system hibernation state (DC).
SpindownTimeoutAC	int	This item stores a time (units: seconds) to hard disk shutdown (AC).
SpindownTimeoutDC	int	This item stores a time (units: seconds) to hard disk shutdown (DC).
OsLanguage	int	This item stores an OS language. Specifically, one of the following values is stored: • 1 Arabic • 4 Chinese (Simplified)– China • 9 English • 1025 Arabic – Saudi Arabia • 1026 Bulgarian • 1027 Catalan • 1028 Chinese (Traditional) – Taiwan • 1029 Czech • 1030 Danish • 1031 German – Germany • 1032 Greek • 1033 English – United States • 1034 Spanish – Traditional Sort • 1035 Finnish 1036 French – France • 1037 Hebrew • 1038 Hungarian • 1039 Icelandic • 1040 Italian – Italy • 1041 Japanese • 1042 Korean • 1043 Dutch – Netherlands • 1044 Norwegian – Bokmal • 1045 Polish • 1046 Portuguese – Brazil • 1047 Rhaeto-Romanic • 1048 Romanian • 1049 Russian • 1050 Croatian • 1051 Slovak • 1052 Albanian • 1053 Swedish • 1054 Thai • 1055 Turkish • 1056 Urdu • 1057 Indonesian • 1058 Ukrainian • 1059 Belarusian • 1060 Slovenian • 1061 Estonian

Item name	Data type	Description
OsLanguage	int	• 1062 Latvian • 1063 Lithuanian • 1065 Persian • 1066 Vietnamese • 1069 Basque • 1070 Serbian • 1071 Macedonian (F.Y.R.O. Macedonia) • 1072 Sutu • 1073 Tsonga • 1074 Tswana • 1076 Xhosa • 1077 Zulu • 1078 Afrikaans • 1080 Faeroese • 1081 Hindi • 1082 Maltese • 1084 Gaelic • 1085 Yiddish • 1086 Malay – Malaysia • 2049 Arabic – Iraq • 2052 Chinese (Simplified) – PRC • 2055 German – Switzerland • 2057 English – United Kingdom • 2058 Spanish – Mexico • 2060 French – Belgium • 2064 Italian – Switzerland • 2067 Dutch – Belgium • 2068 Norwegian – Nynorsk • 2070 Portuguese – Portugal • 2072 Romanian – Moldova • 2073 Russian – Moldova • 2074 Serbian – Latin • 2077 Swedish – Finland • 3073 Arabic – Egypt • 3076 Chinese (Traditional) – Hong Kong SAR • 3079 German – Austria • 3081 English – Australia • 3082 Spanish – International Sort • 3084 French – Canada • 3098 Serbian – Cyrillic • 4097 Arabic – Libya • 4100 Chinese (Simplified) – Singapore • 4103 German – Luxembourg • 4105 English – Canada • 4106 Spanish – Guatemala • 4108 French – Switzerland • 5121 Arabic – Algeria • 5127 German – Liechtenstein • 5129 English – New Zealand • 5130 Spanish – Costa Rica • 5132 French – Luxembourg • 6145 Arabic – Morocco

Item name	Data type	Description
OsLanguage	int	• 6153 English – Ireland • 6154 Spanish – Panama • 7169 Arabic – Tunisia • 7177 English – South Africa • 7178 Spanish – Dominican Republic • 8193 Arabic – Oman • 8201 English – Jamaica • 8202 Spanish – Venezuela • 9217 Arabic – Yemen • 9226 Spanish – Colombia • 10241 Arabic – Syria • 10249 English – Belize • 10250 Spanish – Peru • 11265 Arabic – Jordan • 11273 English – Trinidad • 11274 Spanish – Argentina • 12289 Arabic – Lebanon • 12298 Spanish – Ecuador • 13313 Arabic – Kuwait • 13322 Spanish – Chile • 14337 Arabic – U.A.E. • 14346 Spanish – Uruguay • 15361 Arabic – Bahrain • 15370 Spanish – Paraguay • 16385 Arabic – Qatar • 16394 Spanish – Bolivia • 17418 Spanish – El Salvador • 18442 Spanish – Honduras • 19466 Spanish – Nicaragua • 20490 Spanish – Puerto Rico
ProductID	string	This item stores an agent model. When an empty character is stored, this item appears as follows: `"ProductID": ""`
PollingInterval	int	This item stores an interval (units: seconds) at which an agent polls the management server.
MngStatusUpdateTime	dateTime	This item stores a date and time when the management status of devices was updated. When an empty character is stored, this item appears as follows: `"MngStatusUpdateTime": ""`
AllIpAddress	string	This item stores all IP addresses (IPv4 and IPv6) held by a device. The IP addresses that are stored are represented by the following rules: • The IPv4 address is represented in decimal numbers separated by a period (`.`). • The IPv6 address is represented in hex numbers separated by a colon (:). • Each IP address is separated by a comma (`,`). • If all IP addresses are lined up and more than 512 characters are displayed, the output will be limited to 512 characters. When an empty character is stored, this item appears as follows: `"AllIpAddress": ""`
SnoozeDownloadStatus	int	This item stores a package download delay status. Specifically, one of the following values is stored: • 0: Not delayed

Item name	Data type	Description
SnoozeDownloadStatus	int	• 1: Delayed
Domain	string	This item stores a domain or work group. When an empty character is stored, this item appears as follows: `"Domain": ""`
Manufacturer	string	This item stores a device model or manufacturer. When an empty character is stored, this item appears as follows: `"Manufacturer": ""`
NodeNameInt	int	This item stores a numeric-type host ID.
UUID	string	This item stores a UDID. When an empty character is stored, this item appears as follows: `"UUID": ""`
PhoneNumber	string	This item stores a contract phone number. When an empty character is stored, this item appears as follows: `"PhoneNumber": ""`
IMEI	string	This item stores a IMEI. When an empty character is stored, this item appears as follows: `"IMEI": ""`
RegistrationType	int	This item stores a management type. Specifically, one of the following values is stored: • 0: Online management • 1: Offline management
OsLastStartUpdateTime	dateTime	This item stores a date and time when the OS was last started. When an empty character is stored, this item appears as follows: `"OsLastStartUpdateTime": ""`
SoftwareList	Array	This item stores arrays of `Software` objects that represent the individual installed software information records. This item is mandatory.
Software	Object	This item stores an object name of each installed software information record. For details, see `Software` object. This item is mandatory.

Software object

All Software object items are optional.

Item name	Data type	Description
InstallDate	dateTime	This item stores an installation date. When an empty character is stored, this item appears as follows: `"InstallDate": ""`
SourceKind	int	This item stores the method used to collect software information. Specifically, one of the following values is stored: • 1: Added to **Programs and Features** • 2: **Software Search List**
InstallPath	string	This item stores an installation folder. When an empty character is stored, this item appears as follows: `"InstallPath": ""`
BgStatus	int	This item stores the status that shows how software information is being processed internally. Specifically, one of the following values is stored:

Item name	Data type	Description
BgStatus	int	• 0: Processing completed. • 1: Addition processing is in progress. • 2: Deletion processing is in progress.[#]
SoftwareProductID	string	This item stores a product ID. When an empty character is stored, this item appears as follows: `"SoftwareProductID": ""`
GUID	int	This item stores a GUID.
SoftwareName	string	This item stores a software name.
SoftwareVersion	string	This item stores a version. When an empty character is stored, this item appears as follows: `"SoftwareVersion": ""`
SoftwarePublisher	string	This item stores a manufacturer. When an empty character is stored, this item appears as follows: `"SoftwarePublisher": ""`
SoftwareType	int	This item stores a software information type. Specifically, one of the following values is stored: • 1: Added to **Programs and Features** • 2: **Software Search List** • 3: Program updates
RegistrationDate	dateTime	This item stores a registration date and time.
HelpLink	string	This item stores support information (URL).
SoftwareCheck	int	This item stores s check status. Specifically, one of the following values is stored: • 0: Not checked • 1: Checked
ImportantSoft	int	This item stores information regarding whether the software in question is a Microsoft Office product. Specifically, one of the following values is stored: • 0: The software is not a Microsoft Office product. • 1: The software is a Microsoft Office product.
AppType	int	This item stores an application type. Specifically, one of the following values is stored: • 0: Software other than Windows Store apps • 1: Windows Store app
MSProductType	int	This item stores the purchasing status of Microsoft Office products. `"-1"` is stored if no value is specified. Specifically, one of the following values is stored: • 0: Volume license version • 1: Boxed version • empty character: Other When an empty character is stored, this item appears as follows: `"MSProductType": ""`
MSProductId	string	This item stores the product ID of the Microsoft Office product. Specifically, the product ID of the volume license version is stored, with the last five digits of the ID masked with asterisks (`*`).

Item name	Data type	Description
MSProductId	string	When no product ID exists, or when the purchasing status is something other than the volume license version, an empty character is stored. When an empty character is stored, this item appears as follows: `"MSProductId": ""`

#: The software in this status is regarded as deleted software and does not show up in the management window.

Appendix

A. Miscellaneous Information

This appendix provides miscellaneous information about using JP1/IT Desktop Management 2.

A.1 Port number list

This section describes the port numbers used by JP1/IT Desktop Management 2.

If not otherwise specified, "management server" includes "primary management server" and "management relay server".

> **Tip**
>
> All port numbers used by JP1/IT Desktop Management 2 - Manager are the same as those used by JP1/IT Desktop Management 2 - Operations Director.

JP1/IT Desktop Management 2 - Manager port number list

Management server

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
Ephemeral	→	The JP1/Base authentication server [20240]	TCP	Used for communication from a management server to the authentication server when authenticating JP1 users.
31080	←	Administrator's computer [ephemeral]	TCP	Used for communication from an administrator's computer to a management server when the operation window is referenced or used. This port number is also used for communication from Remote Install Manager or Packager, or network control command installed on the administrator's computer to a management server.
31000	←	Agent, relay system or internet gateway [ephemeral]	TCP	Used for communication from an agent, relay system or an internet gateway to a management server
31002	←	Remote Install Manager or management server [ephemeral]	TCP	Used for communication from a remote Install Manager to a management server.
Ephemeral	→	Management relay server, agent or relay system [31001]	TCP	Used for communication from a management server to a management relay server, agent or relay system during distribution using Remote Install Manager
31006 to 31009, 31011, 31012	← →	Management server [ephemeral]	TCP	Used for communication for internal processing within a management server.
31010	←	• Remote Install Manager [ephemeral] • Asset Console (jamTakeITDM2Info.exe) [ephemeral]	TCP	Used for communication from Remote Install Manager or Asset Console to a management server, or internal processing

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
ephemeral	→	Management relay server, agent, or relay system [31001]	UDP	Used for controlling the power source by using Wake on LAN.
Ephemeral	→	Agent or relay system [31014]	UDP	Used for communication from a management server to an agent or relay system to distribute jobs by multicasting
31015	←	Agent or relay system [ephemeral]	UDP	Used for communication from an agent or relay system to a management server for requesting retransmission during multicast distribution
31021	←	• Remote Install Manager [ephemeral] • Agent [ephemeral] • Relay system [ephemeral] • Packager [ephemeral] • Management relay server [ephemeral] • Management server [ephemeral] • Internet gateway [ephemeral]	TCP	Used for communication from Remote Install Manager, agent, relay system, Packager, management relay server, management server and internet gateway to a management server during distribution using Remote Install Manager
31023	← →	Management server or management relay server [ephemeral]	TCP	Used for communication between a management server and a management relay server.
31026 to 31029	← →	Management server [ephemeral]	TCP	Used for communication of internal processing performed on the management server when the API is used.
31030	←	External system [ephemeral]	TCP	Used for communication between the external system and the management server via the API.
Ephemeral	→	Management relay server, agent, or relay system [16992]	TCP	Used for controlling the power source of a computer that uses AMT

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, in the setup, change them to port numbers that are not used.

If a management server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Also, specify firewall settings to enable ports used for communication in internal processing. Note that if you install JP1/IT Desktop Management 2 - Manager in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Administrator's computer (Remote Install Manager)

Port number for administrator's computer	Connection direction	Connected to [port number]	Protocol	Use
Ephemeral	→	Management server [31002, 31010, 31021, 31080]	TCP	Used for communication from Remote Install Manager to a management server during distribution using Remote Install Manager
Ephemeral#	← →	Management server [ephemeral#]	TCP	Used for Remote Install Manager internal processing

Port number for administrator's computer	Connection direction	Connected to [port number]	Protocol	Use
Ephemeral	→	Relay system [31021]	TCP	Used when deleting a package on a relay system using Remote Install Manager.

#: The following describes how to fix the port numbers used for connecting the database to the agent.

To fix the port number of the management server (connection destination):

1. Execute the `stopservice` command to stop the services on the management server.
2. Use a text editor to open the `pdsys` file stored in *JP1/IT Desktop Management 2 - Manager-installation-folder*\mgr\db\CONF.
3. Add `set pd_service_port =` *port-number*. For *port-number*, specify the port number you want to use.

   Example: To specify 10000 as the port number, enter as follows:

   ```
   set pd_service_port = 10000
   ```

4. Execute the `startservice` command to restart the services on the management server.

To fix the port numbers of Remote Install Manager (connection destination):

For receiving ports, the OS automatically assigns port numbers by default. Ten or more receiving ports are used.

1. Stop Remote Install Manager and other applications for JP1/IT Desktop Management 2.
2. Use a text editor to open the `HiRDB.ini` file stored in *Remote-Install-Manager-installation-folder*\mgr\dbclt.

   If Remote Install Manager and the management server are installed in the same computer, `HiRDB.ini` is stored in *JP1/IT Desktop Management 2-Manager-installation-folder*\mgr\dbclt.
3. For `PDCLTRCVPORT=`, specify the range of port numbers you want to use in the *port-number-port-number* format. Note that the range of port numbers is not set if you do not specify anything or specify `0` after `PDCLTRCVPORT=`, By default, the range of port numbers is not set.

   Example: To specify 10000-10500 as the range of port numbers, enter as follows:

   ```
   PDCLTRCVPORT=10000-10500
   ```

4. Start Remote Install Manager and other applications for JP1/IT Desktop Management 2.

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, in the setup, change them to unused port numbers.

If the administrator's server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if you install Remote Install Manager in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Port number list for a relay system

Port number for relay system	Connection direction	Connected to [port number]	Protocol	Use
16992	←	Management server [ephemeral]	TCP	Used for controlling the power source of a computer that uses AMT
31001	←	Management server [ephemeral]	TCP	Used for communication from a management server to a relay system during distribution using Remote Install Manager

Port number for relay system	Connection direction	Connected to [port number]	Protocol	Use
31001	←	Management server [ephemeral]	UDP	Used for controlling the power source by using Wake on LAN.
31002	←	• Agent [ephemeral] • Internet Gateway [ephemeral]	TCP	Used for communication from an agent and internet gateway to a relay system during distribution using Remote Install Manager
31014	←	Management server [ephemeral]	UDP	Used for communication from a management server to a relay system to distribute jobs by multicasting
31015	←	Agent [ephemeral]	UDP	Used for communication from an agent to a relay system for requesting retransmission during multicast distribution
31021	←	Remote Install Manager [ephemeral]	TCP	Used when deleting a package on a relay system using Remote Install Manager.
ephemeral	→	Management server [31015]	UDP	Used for communication from a relay system to a management server for requesting retransmission during multicast distribution.
Ephemeral	→	Management server [31021]	TCP	Used for communication from a relay system to a management server during distribution using Remote Install Manager
Ephemeral	→	Agent [16992]	TCP	Used for controlling the power source of a computer that uses AMT
ephemeral	→	Agent [31001]	UDP	Used for controlling the power source by using Wake on LAN.
ephemeral	→	Agent [31014]	UDP	Used for communication from a relay system to an agent during multicast distribution.

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
controller [ephemeral]	→	RFB connection target device [5900]	TCP	Used for remote control by means of RFB connection.
controller [ephemeral]	→	Remote control agent[16992]	TCP	Used for controlling the power source of a computer that uses AMT

Controller or remote control agent [port number]	Connection direction	Connected server [port number]	Protocol	Use
Controller [ephemeral]	→	Remote control agent [31016]	UDP	Used for controlling the power source by using Wake on LAN.

If a computer with a controller installed or a computer that is remotely controlled controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if a controller and remote control agent are installed in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, follow the steps below to change them to port numbers that are not used.

- Port number for a controller
  Specify port numbers in the **Options** dialog box of the controller.
- Port number for a remote controller agent
  Specify port numbers in the **Remote control settings** view used for agent configuration.
- Port number for the chat functionality
  In the **Chat** window, select **Options**, and in the displayed dialog box, in the **Connect** tab, specify the port numbers.

JP1/IT Desktop Management 2 - Agent port number list

Agent port number	Connection direction	Connected server [port number]	Protocol	Use
31001	←	Management server [ephemeral]	TCP	Used for communication from a management server to the agent
31001	←	Management server or relay system [ephemeral]	UDP	Used for controlling the power source by using Wake on LAN.
16992	←	Management server [ephemeral]	TCP	Used for controlling the power source of a computer that uses AMT
Ephemeral	→	Relay system [31002]	TCP	Used for communication from an agent to a relay system during distribution using Remote Install Manager
31014	←	Management server or relay system [ephemeral]	UDP	Used for communication from a management server or relay system to an agent to distribute jobs by multicasting
Ephemeral	→	Management server or relay system [31015]	UDP	Used for communication from an agent to a management server or relay system for requesting retransmission during multicast distribution
Ephemeral	→	Management server [31021]	TCP	Used for communication from an agent to a management server system during distribution using Remote Install Manager
31024	←	Agent [ephemeral]	TCP	Used for communication within an agent when an agent that communicates with a higher system via the Internet gateway communicates with the Internet gateway.
31025	←	Agent [ephemeral]	TCP	Used for communication within an agent when an agent that communicates with a

Agent port number	Connection direction	Connected server [port number]	Protocol	Use
31025	←	Agent [ephemeral]	TCP	higher system via the Internet gateway communicates with the Internet gateway.
Ephemeral	→	Internet gateway [443]	TCP	Used for communication via the Internet gateway.

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, when setting up a management server, change them to port numbers that are not used.

If a computer with an agent installed controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if an agent is installed in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

If networks between JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Agent control ports by using Windows Firewall, specify firewall settings to enable the ports in the above table.

Port numbers for agentless devices

For agentless devices, the port numbers for Windows administrative shares or SNMP are used depending on the authentication status of the devices.

Port number list for an Internet gateway

Port number for Internet gateway	Connection direction	Connected to [port number]	Protocol	Use
443	←	Agent [ephemeral]	TCP	Used for communication via the Internet gateway.

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.) • When the agent is stopped, such as when a PC is turned off (The information about stopping is sent.)

Category	Major actions that trigger communication
Application or change of agent configurations 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

A.3 Format of a user settings file excluded from security status judgment

Specify the file name as follows: jdn_except_users.dat.

After creating the file, place it in *JP1/IT-Desktop-Management-2- Manager-installation-folder*`\mgr\conf`.

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.

Leading and trailing single-byte spaces in user account names are ignored.

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.4 Output format of exported operation logs

The following table shows the output format of a CSV file that is output by using the `ioutils exportoplog` command or by periodically exporting an operation log.

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 (Agent)	The date and time are output in the following format: YYYY/MM/DD hh:mm:ss[#2]	19
Operation Date/Time (UTC)	The date and time are output in the following format: YYYY/MM/DD hh:mm:ss[#2]	19
Time Zone	The time zone of the computer where the operation was carried out. It also displays the difference from the UTC time. Example: `GMT+09:00`	9
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 • Device operation Entry of the HIBUN access log or extended operation log, starting with `[HIBUN]`[#4]	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)	244

Output item	Output format	Maximum number of bytes of the output character string[#1]
Operation Type (Detail)	• 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 • Web Access • Change active window • Device connection • Device disconnection • Suppressing device connection • Permitting device connection Entry of the HIBUN access log, event log, or extended operation log, starting with `[HIBUN]`[#4]	244
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	40

Output item	Output format	Maximum number of bytes of the output character string[#1]
Source File Drive Type	• 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
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
Drive type	One of the following is output: • Local Disk • Network Drive • Removable Disk • CD-ROM • RAM Disk • Other	40
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
Device type	A character string of 1,024 or fewer characters is output.	4,096
Device name	A character string of 1,024 or fewer characters is output.	4,096
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
Host ID	A character string of 64 or fewer characters is output.	64

Output item	Output format	Maximum number of bytes of the output character string[#1]
Device category	One of the following is output: • USB device • Built-in CD or DVD drive • Internal floppy disk drive • IEEE1394 device • Built-in SD card • Bluetooth device • Imaging device • Windows portable device • Unknown • Removable media[#4] • External hard disk[#4] • CD or DVD drive[#4] • Infrared device[#4] • Wireless LAN[#4] • Modem[#4] • Windows Mobile device[#4] • Palm handheld device[#4] • BlackBerry device[#4] • Serial or parallel port[#4] • Other controlled device[#4] • Wired LAN (USB connections)[#4] • Wired LAN (non-USB connections)[#4]	64
HIBUN log entry[#4]	The following entries of the HIBUN log are output: • [HIBUN]Header • [HIBUN]Version • [HIBUN]Date • [HIBUN]Time • [HIBUN]HIBUN User • [HIBUN]Windows User • [HIBUN]SID • [HIBUN]Computer • [HIBUN]IP Address • [HIBUN]Function Type • [HIBUN]Status • [HIBUN]Log Type • [HIBUN]Operation • [HIBUN]Process • [HIBUN]File Name • [HIBUN]Event Target • [HIBUN]APP Data Version • [HIBUN]Message 1 • [HIBUN]Message 2 • [HIBUN]Message 3	It depends on the specifications of HIBUN.

#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.

#4: They are output when HIBUN logs are imported. For details about the HIBUN logs, see *Importing HIBUN logs into the management server* in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

Note

The following item names that are output in a CSV file when operation logs are exported by using the `ioutils exportoplog` command have been updated. If you have specified these item names in an operation log analysis tool or such, change the names.

- <Before> External Drive Type, <After> Drive Type
- <Before> External Drive Name, <After> Drive Name
- <Before> External Device Type, <After> Device Type
- <Before> External Device Name, <After> Device Name
- <Before> External Device Instance ID, <After> Device Instance ID

Related Topics:

- 15.3.3 Periodically exporting operation logs
- 17.20 ioutils exportoplog (exporting operation logs)

A.5 Format of the updated program list (patch information CSV file)

The following table describes the format of input and output files for the import and export commands of the updated program list:

Item	Format#	Maximum length of the character string (in bytes)
Update Name	A character string of 256 or fewer characters	1,024
Security Bulletin Number	A character string of 8 or fewer characters, composed of single-byte alphanumeric characters and hyphens (-)	8
Detail URL	A character string of 2,083 or fewer characters	8,332
Article ID	A character string of 10 or fewer characters, composed of ASCII characters (excluding control characters)	10
Severity	Critical or Important	9
Support OS	One of the following character strings: • XP_32 Windows XP 32-bit • WS2003_32 Windows Server 2003 32-bit and Windows Server 2003 R2 32-bit • WS2003_64 Windows Server 2003 64-bit and Windows Server 2003 R2 64-bit • WS2008R2	11

Item	Format#	Maximum length of the character string (in bytes)
Support OS	Windows Server 2008 R2 64-bit • Vista_32 Windows Vista 32-bit • Vista_64 Windows Vista 64-bit • WS2008_32 Windows Server 2008 32-bit • WS2008_64 Windows Server 2008 64-bit • 7_32 Windows 7 32-bit • 7_64 Windows 7 64-bit • 8_32 Windows 8 32-bit • 8_64 Windows 8 64-bit • WS2012_64 Windows Server 2012 64-bit • 8.1_32 Windows 8.1 32-bit • 8.1_64 Windows 8.1 64-bit • WS2012R2_64 Windows Server 2012 R2 64-bit • 10_32 Windows 10 32-bit • 10_64 Windows 10 64-bit • WS2016_64 Windows Server 2016 64-bit • WS2019_64 Windows Server 2019 64-bit	11
Service Pack or Version	One of the following character strings: • None No service pack • SP1 Service Pack 1 • SP2 Service Pack 2 • SP3 Service Pack 3 • (For Windows 10, Windows Server 2019, or Windows Server 2016) A number of 1000 to 32767. The version of Windows 10, Windows Server 2019, or Windows Server 2016	5
Update Target	Windows (for Windows OS), or Software (for other software program)	8
Software name (under Update Target)	IE (for Microsoft Internet Explorer)	2

Item	Format#	Maximum length of the character string (in bytes)
Version (under Update Target)	A positive integer from 6 to 11	2
Service Pack (under Update Target)	One of the following character strings: • None No service pack • SP1 Service Pack 1 • SP2 Service Pack 2 • SP3 Service Pack 3	4
Description	A character string of 2,048 or fewer characters	8,192
Release Date	A date in the format YYYY/MM/DD (where YYYY indicates the year, MM indicates the month, and DD indicates the day)	10
Language Type	"ja" (Japanese), "en" (English), or "zh" (Chinese)	2

#: The first line is a header line and the subsequent lines are data lines. Enclose each value with double quotation marks ("). When a value contains a literal double quotation mark ("), the double quotation mark must be preceded by another double quotation mark.

Related Topics:

- 17.18 ioutils exportupdatelist (exporting the updated program list)
- 17.19 ioutils importupdatelist (importing the updated program list)

A.6 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	--	--

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 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.

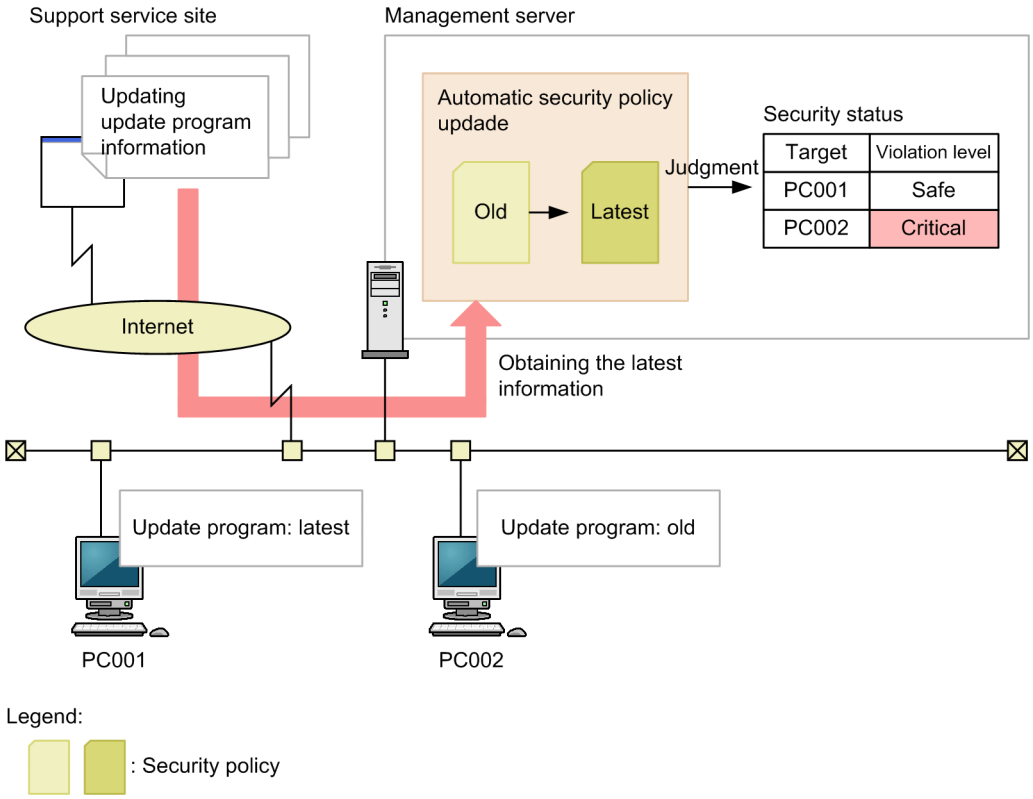
#4: If you omit a value for the default language, a null character is set. If you omit a value for a language other than the default language, the same value as the default language is set for that language.

A.7 Obtaining information from the support service

If you have a contract with the support service, you can obtain updated program information, anti-virus product information, and SAMAC software dictionary information. The functionality provided by JP1/IT Desktop Management 2 enables automatic acquisition of updated program information and anti-virus product information.

(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

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 or if you want to update the information in the SAMAC software dictionary, an administrator uses an externally connected computer to download the latest information from the support service site. 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 Inventory module.

Updating offline by executing a command

Execute the `updatesupportinfo` command to update. For details, see 17.24 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	Whether the information can be obtainable automatically
Support information file	Update program information	Update program name	The name of an update program	Y
		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 or version	An OS service pack or version 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	
	Anti-virus product information	Product list	List of anti-virus products supported by JP1/IT Desktop Management 2	
		Scripts obtained	Scripts that the Agent executes when you obtain anti-virus product information	
SAMAC software dictionary file for offline updates		Software type	Software type based on the information in the SAMAC software dictionary. A type of software information managed by JP1/IT Desktop Management 2.	N

Legend: Y: Obtainable automatically N: Not obtainable automatically

(4) Confirmation of the acquisition situation of the information from the support service

When you obtain the information from the support service, following events or audit logs are output.

Update program information

Evnet: 63

Audit log: KDEX5371-I

Anti-virus product information

Evnet: 1007

Audit log: KDEX5373-I

SAMAC dictionary file information

Evnet: 1124

Audit log: KDEX5437-I

Confirm these events or audit logs whether you have been able to obtain the information from the support service normally.

A.8 Cases in which settings are applied after a restart

You sometimes need to restart a computer to apply settings for JP1/IT Desktop Management 2. A restart is required in the following cases:

- When a security policy is edited or assigned
- When security measures are manually performed

When a security policy is edited

If you edit any of the following items, restart the computer to which the edited security policy is assigned. The items inside the parentheses indicate the relevant security configuration items. After the computer is restarted, the edited security policy is applied to that computer.

- Auto enforce of Enable Automatic Update (Windows Update)
- Auto enforce of Disable Administrative Share (OS Security)
- Auto enforce of Disable Anonymous Access (OS Security)
- Auto enforce of Enable Firewall (OS Security)
  The following OSs do not require a restart: Windows Server 2003 and Windows XP
- Auto enforce of Disable DCOM (OS Security)
- Auto enforce of Disable Remote Desktop (OS Security)
- Suppression of Device Usage (Other Access Restrictions)#
- Enable or disable Acquisition of Operation Logs (including acquisition of Suspicious Operations To Be Reported) (Operation Logs)#

The settings of Suppression of Device Usage and Acquisition of Operation Logs are applied when a security policy is assigned. However, we recommend that you restart your computer, because some of settings related to the suppression of device usage or to operation logs take effect only after a restart.

The settings that take effect after a restart are as follows.

Classification		Setting Item
operation logs	operation logs	• Copy file • Move file • Rename file • Create file • Delete file • Web Access (Upload) • Web Access (Download) • FTP (Send File) • FTP (Receive File) • Send Mail (Attachment File) • Receive Mail (Attachment File) • Save Attached File • Copy folder

Classification		Setting Item
operation logs	operation logs	• Move folder • Rename folder • Create folder • Delete folder
	Suspicious operations	• Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device
Other Access Restrictions	Suppression of write operation	• Removable disks • CD/DVD drives • FD drives

When a security policy is assigned

Restart the computer to which the security policy is assigned. After the computer is restarted, the assigned security policy is applied to that computer.

The settings of Suppression of Device Usage and Acquisition of Operation Logs are applied when a security policy is assigned. However, some settings of Suppression of Device Usage and Operation Logs might take effect after a restart.

When security measures are manually performed

If you specify any of the following configuration items, restart the computer for which the items have been specified. The items inside the parentheses indicate the relevant security configuration items. After the computer is restarted, the security measures are executed on the computer.

- Enable Automatic Update (Windows Update)
- Disable Administrative Share (OS Security)
- Disable Anonymous Access (OS Security)
- Enable Firewall (OS Security)
  The following OSs do not require a restart: Windows Server 2003 and Windows XP
- Disable DCOM (OS Security)
- Disable Remote Desktop (OS Security)

A.9 Displayed date and time

The date and time displayed in JP1/IT Desktop Management 2 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

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	on the management server. This date and time is not updated.
	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. In a multi-server configuration, the information about Last Alive Confirmation Date/Time is not sent to the higher management servers. Therefore, a hyphen (-) is displayed for devices other than those immediately under the local server.
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	Y	N	A search is performed 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	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 **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

While JP1/IT Desktop Management 2 is running, do not revert the date and time on any of the computers that make up a JP1/IT Desktop Management 2 system. Changing the date and time might cause a failure in functions that work according to the set date and time.

A.10 Outputting audit logs

Audit logs in JP1/IT Desktop Management 2 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 2 is stored in the audit logs. This topic explains audit logs that are output from management servers. For details about audit logs of the distribution function using Remote Install Manager, see the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

Tip

Audit logs are output not only from JP1/IT Desktop Management 2, but also from other JP1 products and OS (Windows event log). By using JP1/Audit Management - Manager[#1] to collect and manage audit logs, you can use audit logs for evaluation and audit of the internal control. You can link with JP1/Audit Management - Manager only when the OS language for the management server is Japanese or English[#2].

#1: JP1/Audit Management - Manager is a program that collects and manages audit logs to support evaluation and audit of the internal control for the whole system. In version 9 or earlier, this product was called *JP1/NETM/Audit - Manager*.

#2: If the language set in the OS of the management server is English, audit logs are output in UTF-8. Therefore, characters in audit logs might not be displayed properly in JP1/Audit Management - Manager.

(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 2 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 2 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 2 - Manager service • Startup failure of the JP1/IT Desktop Management 2 - Manager service • Abnormal end of the JP1/IT Desktop Management 2 - Manager service
Authentication	This event type indicates that this is an audit log related to the authentication results of a JP1/IT Desktop Management 2 - Manager user.	• Success or failure in login to JP1/IT Desktop Management 2 - Manager • Logout from JP1/IT Desktop Management 2 - 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 2 - Manager • Normal or abnormal end during agent setup • Normal or abnormal end in license information registration • 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

Event type	Description	When JP1/IT Desktop Management 2 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 the JP1/NETM/NM - Manager linkage • Success or failure in changing the operation log settings • Success or failure in changing the range of targets subject to automatic updates of the network filter list • Success or failure in executing the distributelicense command • Success or failure in setting a component of an agent to be distributed • Success or failure in setting the asset status of hardware assets associated with deleted devices • Success or failure in changing the device maintenance settings
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 • Success or failure in updating information in the SAMAC software dictionary • 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 removing operation logs • Normal or abnormal termination of an import of the network control list • Normal or abnormal termination of an export of the network control list
Maintenance	This event type indicates that this is an audit log related to database operation.	• Success or failure in backing up databases

Event type	Description	When JP1/IT Desktop Management 2 outputs audit logs
Maintenance	This event type indicates that this is an audit log related to database operation.	• 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) • *TZD*: time zone
Program name	progid	JP1/ITDM2	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	The name of the component in which an event occurred

Output item		Value	Description
Item name	Output attribute name		
Component name	compid	• AgentControl • Agent • RelayManagerService (relay service of management server)	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 2 - 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 2 - Manager action definition file) • Agent • AssetInfo (asset information) • SecurityInfo (operation log) • NetCtrlInfo (network control)	Information about the object that caused an event to occur
Action information	op	One of the following is output: • Start • Stop • Login • Logout	Action information about the user who caused an event to occur

Output item		Value	Description
Item name	Output attribute name		
Action information	op	• Add • Update • Delete • Request • Response • Import • Export • 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 2 • 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.11 Conditions where the tools must be re-executed on an offline-managed computer

After you modify a configuration of an offline-managed computer in the operation window, you need to re-execute a tool. The following table lists and describes which configuration tool must be re-executed depending on which configuration item is modified.

Configuration item		Condition	Configuration tool		
			Installation set	`getinv.vbs` (to collect offline management information)	`setsecpolicy.vbs` (to apply the security policy to the offline-managed computer and collect device information)
Agent configuration		• If a configuration of the agent to be applied is modified • If an agent configuration that was applied to the offline-managed computer is updated	R	--	--
System policy	Extended inventory	- If one of the following configurations is modified: • Start Date for Entry of User Information • Field Order of Custom Fields on the User Input Window - If one of the following configuration items is added or updated when the data source is End User or Registry: • Common Fields (Assets and Device Inventory) • Custom fields of hardware asset	--	R	R

Configuration item			Condition	Configuration tool		
				Installation set	`getinv.vbs` (to collect offline management information)	`setsecpolicy.vbs` (to apply the security policy to the offline-managed computer and collect device information)
System policy	Extended inventory		informati on	--	R	R
	Software search condition		If a condition is added or modified	--	R	R
License information			If the software is changed from the evaluation version to the product version	--	R	R
Script to collect anti-virus product information			If the script to collect anti-virus product information is updated	--	R	R
Security policy	Security configuration item	Updates	If the Auto Enforce configuration in Automatic Windows Update is updated	--	--	R
		Prohibited software	If the Restriction Setting for startup in Auto Enforce is updated	--	--	R
		Anti-virus product	--	--	--	--
		Mandatory software	--	--	--	--
		User-Defined Security Settings	--	--	--	--
		Unauthorized Windows Service	If a prohibited service is added or removed or the Auto Enforce configuration is updated	--	--	R
		OS Security	If the Auto Enforce configuration is updated	--	--	R
	Suppress item	Start of software	If a configuration is modified	--	--	R

Configuration item			Condition	Configuration tool		
				Installation set	`getinv.vbs` (to collect offline management information)	`setsecpolicy.vbs` (to apply the security policy to the offline-managed computer and collect device information)
Security policy	Suppress item	Print	If a configuration is modified	--	--	R
		Device Attach	If a configuration is modified	--	--	R
		USB device list	If a registered USB device is changed	--	--	R

Legend: R: Re-execution is required, --: Not applicable

Tip

The configuration items for Security Policies, the Operations Logs, Common settings for prohibited operations and operation logs, Collect List of USB Device Files, and Action Items cannot be configured for the offline-managed computer.

A.12 Amendments for each version

(1) Changes in 12-60

(a) Changes in the manual (3021-3-E14-30(E))

- The **All Assets Cost** report, which totals the cost values of hardware assets, software license, and other, was added to **Asset Detail Reports**.
- Maximum of 300,000 devices can be managed.
- Software information can now be searched for at any time with the `softwaresearch` command.
- **Operation Date/Time (UTC)** was added to the information items to be collected in the operation log.

(2) Changes in 12-50

(a) Changes in the manual (3021-3-E14-20(E))

- A new network monitor setting can allow events to be issued whenever unauthorized devices access the network.
- The `ioutils importasset` command can now be used to import not only hardware asset information but also software license information, managed software information, contract information, and a contract vendor list.
- The `ioutils exportasset` command can now be used to export not only hardware asset information but also software license information, managed software information, contract information, and a contract vendor list.

- Asset association information can now be imported. Information regarding the `ioutils importassetassoc` command was added.
- Asset association information can now be exported. Information regarding the `ioutils exportassetassoc` command was added.
- The following events were changed:
  1087, 1164
- The following events were added:
  1174 to 1182
- The following information can now be acquired via an API:
  - List of device information
  - List of information about software installed on devices

(3) Changes in 12-10

(a) Changes in the manual (3021-3-E14-10(E))

- Windows Server 2019 was added as an applicable operating system for the following products:
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console
  - JP1/IT Desktop Management 2 - Internet Gateway
  - Remote Install Manager
- Windows updates and a feature update to Windows 10 can now be packaged for distribution by using Remote Install Manager.
- Devices can now be managed from an external system via the API.
- The **Hardware Assets Cost** report and the **Software License Cost** report can now display the total cost calculated based on the contract information valid at the time the report is displayed.
- A description of the upldoplog (uploading operation logs) command was added.
- A description of the prepagt.bat (generalizing an agent) command was added.
- Notes on managing shared VDI-based virtual computers were added to the description of `resetnid.vbs` (resetting the host ID).
- The following events were added:
  1168 to 1173

(4) Changes in 12-00

(a) Changes in the manual (3021-3-E14(E))

- Windows Server 2008 R2 was removed from applicable OSs for the following products:
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console

    - Remote Install Manager
- Improvements were made to the security judgment for cumulative updates and Security Monthly Quality Rollup for Windows.
- Computers can now be managed via the Internet.
- A description of the deletelicense (delete licenses) command was added.

(5) Changes in 11-51

(a) Changes in the manual (3021-3-B54-40(E))

- A security policy can now be set for offline-managed devices.
- The file information stored in all the registered USB devices can now be collected.
- A file larger than 2 gigabytes can now be distributed.
- The VPN connection configurations for PCs for use outside the company were added.
- HIBUN logs can now be imported into JP1/IT Desktop Management 2 operation logs.
- When hardware asset information is imported, the user can now select whether to register the information as new hardware asset information if it is not associated.
- The `ioutils importexlog` command was added to the commands that cannot be executed simultaneously.
- The following events were added:
  1164, 1165, 1166, 1167
- In event 1079, the MAC address and the IP address are now set for the issued host name item.

(6) Changes in 11-50

(a) Changes in the manual (3021-3-B54-30(E))

- For agents for Mac, the distribution of software and files (remote installation) is now enabled. Additionally, these agents are judged for security status based on security policies.
- You can now use a command to control network access of devices.
- The setting that suppresses the use of USB devices is now available to limit assets that can use USB devices.
- The managed software information now includes information on which operating system the software program is installed on. This enables the licenses of a software program to be managed for each operating system.
- You can now install an agent on the server on which Citrix XenApp and Microsoft RDS have been installed and manage it with JP1/IT Desktop Management 2.
- A list of update programs registered with a management server can now be exported to a CSV file. Additionally, the exported CSV file containing patch information can now be imported to the source management server or other management servers.
- The ioutils exportupdatelist command and the ioutils importupdatelist command are now included as part of the commands that cannot be simultaneously executed.
- The following events were added:
  1159 to 1163

(7) Changes in version 11-10

(a) Changes in the manual (3021-3-B54-20(E))

- Windows Server 2016 was added as an applicable operating system for the following products:
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - Asset Console
  - Remote Install Manager
- An agent can now be managed after being installed on a computer running Mac OS.
  Provided functionality
  - Acquisition of system information and software information
  - Remote control via RFB connections (already provided for agentless management)
  - Network control (enabling or disabling network access on demand)

  Unavailable functionality (including functionality in development)
  - Software and file distribution (remote installation)
  - Collection of files (remote collection)
  - Agent settings and agent deployment
  - Security management (security judgments, automated countermeasures)
  - Operation logs
  - Device control
- By linking with JP1/Base, you can now log in to JP1/IT Desktop Management 2 by using JP1 authentication.
- As files that are to be executed automatically during installation, ZIP files for installers of related products, such as Hibun, can now be set.
- Information about Windows Store apps can now be collected as installed software information.

(8) Changes in version 11-01

(a) Changes in the manual (3021-3-B54-10(E))

- JP1/IT Desktop Management 2 - Operations Director was added as a relevant program product.
- Windows 10 was added as an applicable operating system for JP1/IT Desktop Management 2 - Network Monitor.
- Smart device software can now be managed.
- You can now use the file for connection destinations (`itdmhost.conf`) to specify the connection destination of an agent.
- You can now perform device maintenance in which you can specify judgement conditions for duplicate or idle devices in order to detect devices suggested for deletion, and then delete them automatically or manually.
- The description of the remote control function for UNIX agents was removed.
- The description of the systems on which the `itdm2nodecount` (counting the number of managed devices) command can be executed was amended.

- The return values 4 and 85 were added to the `itdm2nodecount` (counting the number of managed devices) command.
- The procedure for executing the `deletenwgroup` command for the first time was added.
- When a device is deleted, the asset status of the hardware assets associated with the deleted device can now be automatically changed.
- Events with the following event numbers were added:
  1154 to 1158
- JP1 event attributes for event number 1157 were added.
- A description of the port numbers used on the administrator's computer (Remote Install Manager) and relay systems was added.
- Information about the Windows OS version can now be obtained.
- A trigger for JP1/IT Desktop Management 2 to output audit logs was added.

(9) Changes in version 11-00

(a) Changes in the manual (3021-3-B54(E))

- Operating JP1/IT Desktop Management 2 in a multi-server configuration can now enable both location-by-location management and integrated management.
- The setting procedure for obtaining revision history of devices was changed.
- Windows 10 was added as the applicable OS for the following products.
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - RC Manager
  - Remote Install Manager
- Windows Server 2003 and Windows Server 2008 (excluding Windows Server 2008 R2) were excluded from the applicable OS for the following products.
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - RC Manager
- You can now import and export network connection information.
- With the end of the support of the JP1 smart device management service, the JP1 smart device management service was deleted from the MDM systems that can be linked.
- You can now use JP1/Audit Management - Manager to collect and manage audit logs of JP1/IT Desktop Management 2 if the language set for the management server OS is Japanese or English.
- As an argument for the resetnid.vbs (resetting host identifiers) command, /s was added.
- A description of the distributelicense (distributing licenses) command was added. In addition, the deletenwgroup (deleting network groups) command was added in the description that the distributelicense command cannot be executed simultaneously with some commands.
- A description of the deletenwgroup (deleting network groups) command was added. In addition, the distributelicense (distributing licenses) command was added in the description that the deletenwgroup command cannot be executed simultaneously with some command.
- A description of the itdm2nodecount (counting the number of managed devices) command was added.

- Event numbers 1145, 1146, 1148, 1149, 1150, 1151, and 1152 were added in the event list.
- Port number 31023 was added in the port number list.
- The procedure for changing the display order of user information was added.
- You can now install and manage an agent on a computer whose OS is UNIX.
- Anti-virus product information can now be acquired from the support service site.
- In the description about the browsers that can display the operation windows, Internet Explorer 11 was added.
- (Changes from only this manual (3021-3-370(E))) The software, purchasing status, product ID, GUID, and software type for some software can now be managed.

(10) Changes in version 10-50

(a) Changes in the manuals (3021-3-276 and 3021-3-370(E))

- For the `resetnid.vbs` (resetting the host ID) command, how to display return codes was added, and the example was corrected.
- Functions of a site server configuration system were deleted, and a relay system was added as the system necessary for using Remote Installation Manager for distribution,
- The distribution function using Remote Installation Manager now allows you to perform distribution by specifying detailed conditions of managed computers and operations to be performed on the computers.
- You can now manage hardware information, software information, and contract information including network devices by using a database.
- You can now collect files stored in managed computers in a single operation.
- You can now suppress the use of the following devices:
  - Bluetooth device
  - Imaging device
  - Windows portable device

  In addition, you can now suppress the use of the following types of devices, which were suppressed as removable disks in Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista:
  - USB device
  - IEEE1394 device
  - Internal SD card
- You can now select to obtain a list of files stored in a USB device permitted for use.
- You can now specify whether to display, on a user's computer, a message indicating that the use of devices is suppressed.
- The **Getting Started** wizard can now install an agent as a method of managing devices.
- Functions of a multi-server configuration system were deleted, and you can now manage a maximum of 30,000 devices on a management server.
- You can now specify the conditions to acquire operation logs relating to the following operations:
  - File Operation
  - Process/Program Operation
  - Window Operation
- You can now acquire an operation log for permitting device connection.

- You can now set intervals for reporting prohibited-operation suppression events and operation logs to the higher-level system, and the maximum period for holding such events and operation logs on a user's computer.
- You can now specify the number of consecutive login failures before an account is locked, and the password expiration period.
- Settings for installation, setup, and agent configuration were changed according to changes in product configuration.
- Windows 8.1 and Windows Server 2012 R2 were added as applicable OSs for the following products:
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
- Windows 8 and Windows 7 were removed from the applicable OSs for the following product:
  - JP1/IT Desktop Management 2 - Manager
- Windows 2000 was removed from the applicable OSs for the following product:
  - JP1/IT Desktop Management 2 - Agent
- Supported Internet Explorer versions were changed.
- Some port numbers were changed.
- The following events were added:
  1011, 1138, 1139, and 1140
- The following events were changed:
  1032, 1033, 1034, and 1076
- The following events were deleted:
  1010 and 1121
- You can no longer acquire print operation logs or suppress printing for shared network printers.
- For connection mode in the remote control agent configuration, the description of control mode was replaced with that of the monitoring mode. Accordingly, the description of how to determine the connection mode was changed.
- Information output in audit logs was changed.
- The following items were added to actions to be taken after a failover during command execution:
  - ioutils exportdevice (to export device information)
  - ioutils exportdevicedetail (to export device information details)
  - ioassetsfieldutil export (to export the definitions of common management fields and additional management fields)
- Description about handling of values when a CSV file is imported by the `ioutils importasset` command was added.

(11) Changes in version 10-10

(a) Changes in the manual (3021-3-154-30)

- The following note was added: If you want to specify a period of time to intensively search for devices connected to the network, you must specify settings so that the number of IP addresses contained in the IP address range is 50,000 or lower.
- In the Security module and Device module, you can now create groups to which managed computers are automatically assigned according to certain conditions.

- You can now select whether to display, in the user computer, the balloon hint for the JP1/IT Desktop Management icon in the task tray and the End User Form view.
- For automatic update of the network filter list, you can now specify whether to enable all automatic updates or automatic updates only for add operations.
- You can now link with JP1/NM - Manager to allow JP1/IT Desktop Management to control network connections monitored by appliance products with JP1/NM installed.
- Descriptions of how to import a server certificate to the management server, and then change the server certificate of the MDM system, were added. The descriptions of the Internet Explorer version were deleted from the procedure for setting information required to link with an MDM system. In addition, settings required for linking with the JP1 smart device management service were added.
- Descriptions about permissions required to execute commands were collected in 17.1 Executing commands. In addition, a description about what to do if User Account Control (UAC) for the OS is enabled when executing a command other than the `getinv.vbs` command was added.
- Notes on command execution were added.
- Return value 1 was added to `ioutils importfield` command.
- The CSV file output format when an operation log is exported by using the `ioutils exportoplog` command was added.
- The `/i` option was added to the `resetnid.vbs` command so that a dialog box prompting the user to select whether to execute the command, and a dialog box showing the execution results, appear on the user computer.
- The following event was added as an event that requires corrective actions:
  1059
- The following messages were added:
  KDEX1598-E, KDEX3319-I, KDEX3320-E, KDEX3321-I, KDEX3322-E, KDEX4126-W, KDEX5305-I, KDEX5306-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 message was deleted:
  KDEX6321-E
- The following events were added:
  1134, 1135, 1136, and 1137
- The following event was changed:
  19
- The JP1 event attributes of the following events were added:
  1135, 1136, and 1137
- The JP1 event attribute of the following event was changed:
  1118
- The description about ports was corrected. Also, a description about the network between JP1/IT Desktop Management - Remote Site Server and agentless computers was added.
- Descriptions about the registration date and time, and the management start date and time displayed in the device list, were added.

(b) Changes in the manual (3021-3-339-10(E))

- The following note was added: If you want to specify a period of time to intensively search for devices connected to the network, you must specify settings so that the number of IP addresses contained in the IP address range is 50,000 or lower.
- You can now make security judgment on any judgment conditions you like by adding any desired policy about computer security settings to the list of security policies.
- You can now obtain change histories of device information.
- You can now manage the use status of software licenses for each management software in the **Software License Status** window.
- A description was added about the flow of changing the definition of a department when the organizational structure of the department is changed.
- You can now collectively delete departments and locations that are deleted from the department definitions, from the groups displayed in the menu area.
- In the Security module and Device module, you can now create groups to which managed computers are automatically assigned according to certain conditions.
- You can now select whether to display, in the user computer, the balloon hint for the Job Management Partner 1/IT Desktop Management icon in the task tray and the window for entering user information.
- A system administrator can now set (in the Settings module) the date and time when the user can start entering user information.
- For automatic update of the network control list, you can now specify whether to enable all automatic updates or automatic updates for add operations only.
- You can now link with JP1/NETM/Network Monitor - Manager to allow Job Management Partner 1/IT Desktop Management to control network connections (monitored by appliance products with JP1/NETM/Network Monitor installed).
- You can now restrict the display range of software licenses and contracts according to the jurisdiction range specified in the user account.
- Descriptions of how to import a server certificate to the management server, and then change the server certificate of the MDM system, were added. The descriptions of the Internet Explorer version were deleted from the procedure for setting information required to link with an MDM system.
- Descriptions about permissions required to execute commands were collected in 17.1 Executing commands. In addition, a description about what to do if User Account Control (UAC) for the OS is enabled when executing a command other than the getinv.vbs command was added.
- A procedure of executing commands on a computer with an agent installed was added.
- Notes on command execution were added.

  You can now export and import definitions of asset management items in CSV format.
- Return value 1 was added to the ioutils importfield command.
- A note on specifying the -filter option for the `ioutils exportoplog` command was added.
- The CSV file output format when an operation log is exported by using the ioutils exportoplog command was added.
- A description was added about the characters that can be used for folder names specified in the following commands:
  - exportdb command
  - importdb command
  - reorgdb command
  - getlogs command

  - getinstlogs command
- The /i option was added to the resetnid.vbs command so that a dialog box to select whether to let the user's computer execute the command and a dialog box to show execution results are displayed.
- The following event was added as an event that requires action when a failure occurs:
  1059
- 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
- 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
- JP1 event attributes for the following events were added:
  1132, 1133, 1135, 1136, and 1137
- JP1 event attributes for the following events were changed:
  1079, 1082, and 1118
- The explanation of port settings was changed. Also, an explanation about a network between Job Management Partner 1/IT Desktop Management - Remote Site Server and an agentless computer was added.
- An explanation was added regarding the registration date and time and the management start date and time displayed in the device list.

(12) Changes in version 10-02

(a) Changes in the manual (3021-3-154-20)

- You can now make security judgment on any judgment conditions, by adding any desired policy about computer security settings to the list of security policies.
- You can now obtain change histories of device information.
- You can now manage the use status of software licenses for each management software in the **Software License Status** window.
- A description was added about the flow of changing the definition of a department when the organizational structure of the department is changed.

- You can now collectively delete departments (and locations that are deleted from the department definitions) from the groups displayed in the menu area.
- A system administrator can now set the date and time when the user can start entering user information, in the Settings module.
- You can now restrict the display range of software licenses and contracts according to the jurisdiction range specified in the user account.
- Windows 8 and Windows Server 2012 were added as applicable OSs for the following programs:
  - JP1/IT Desktop Management - Manager
  - JP1/IT Desktop Management - Remote Site Server
  - JP1/IT Desktop Management - Network Monitor
- A procedure of executing commands on a computer with an agent installed was added.
- You can now export and import definitions of asset management items in CSV format.
- A note on specifying the -filter option for the `ioutils exportoplog` command was added.
- A description was added about the characters that can be used for folder names specified in the following commands:
  - `exportdb` command
  - `importdb` command
  - `reorgdb` command
  - `getlogs` command
  - `getinstlogs` command
- A procedure of resetting a host ID on a computer in which a site server is installed was added.
- The following note was added: Do not execute the resetnid.vbs command on a device on which the network monitor is installed.
- The following messages were added:
  KDEX1597-E, 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, KDEX5460-I, KDEX5461-I, KDEX5462-E, and KDEX5463-E
- The following messages were deleted:
  KDEX1543-E and KDEX4065-E
- The following events were added:
  1127, 1128, 1129, 1130, 1131, 1132, and 1133
- The following events were deleted:
  50, 51, and 52
- The following events were changed:
  1079 and 1082

(13) Changes in version 10-01

(a) Changes in the manual (3021-3-154-10)

- 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 on the `recreatelogdb` command were corrected.
- Notes on 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, including anti-virus product 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. In addition, you can now update the information in JP1/IT Desktop Management by obtaining support service information including the SAMAC software dictionary file for offline update to manage software types.
- Notes on error message KDEX4041-E which is output when executing the `getlogs` command were 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, KDEX1543-E, KDEX1594-E, KDEX3029-E, KDEX3030-I, KDEX4203-E, KDEX4270-I, KDEX4287-E, KDEX5401-E, KDEX5437-I, KDEX5438-E, KDEX5440-E, KDEX5450-E, KDEX5451-E, KDEX5452-E, KDEX5453-E, KDEX5454-E, KDEX5455-E, and KDEX5456-E
- The following messages were changed:

  KDEX4023-E, KDEX4073-I, KDEX4204-E, KDEX4220-E, KDEX4295-E, KDEX4378-Q, 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, KDEX5396-I, KDEX5397-E, KDEX5407-E, KDEX5414-E, KDEX5415-E, KDEX5423-E, KDEX5426-E, KDEX5427-E, KDEX5428-E, KDEX5430-E, KDEX5431-I, KDEX5432-I, KDEX5435-E, KDEX6112-E, KDEX6113-E, KDEX6115-E, KDEX6132-E, KDEX6151-E, KDEX6152-E, KDEX8006-E, KDEX8019-E, KDEX8022-W, KDEX8024-W, and KDEX8028-E
- The following events were added:

  1117, 1118, 1123, and 1124
- The following events were added:

  1107 and 1108
- IDs that are displayed in JP1/IM as JP1 events when linked with JP1/IM were added.
- Event 1118 can now be output to JP1/IM as a JP1 event when linked with JP1/IM.
- A description of attributes for JP1 events was 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 or prohibited operations suppression events are being sent to a higher-level system, the operation logs or prohibited operations suppression events are sent to the higher-level system after the computer is turned on.
- The name of the program that collects and manages audit logs to support evaluation and audit of the integral control for the whole system was changed to JP1/Audit Management - Manager.
- "Success or failure in updating the SAMA software dictionary information" was added as the timing when ContentAccess audit logs are output.

(b) Changes in the manual (3021-3-339(E))

- The following information was combined into the Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 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, for example, kilobyte (KB)
  - 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 on the `recreatelogdb` command were corrected.
- Notes on 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.
- The 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 on error message KDEX4041-E which is output when executing the `getlogs` command was added.
- The 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 to 1118, and 1120 to 1123
- IDs that are displayed in JP1/IM as JP1 events when linked with JP1/IM were added.
- Event 1118 can now be output to JP1/IM as a JP1 event when linked with JP1/IM.
- A description of attributes for JP1 events was 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 or prohibited operations suppression events are being sent to a higher-level system, the operation logs or prohibited operations suppression events are sent to the higher-level system 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.
- You can now suppress only writing to FD drives and removable disks.
- 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 description was added about the method of removing 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 Configuration** window, 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 **OK** in the JP1/IT Desktop Management dialog box for 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: Of 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.
- The description of actions that trigger communication between a management server and an agent was 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 (anti-virus product 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 to 1116 were added to the events for which action needs to be taken.

(14) Changes in version 10-00

(a) Changes in the manual (3021-3-154)

- 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 division of work responsibilities specified for user accounts.
- You can now suppress only writing to FD drives and removable disks as well.
- You can now link with the MDM service to manage smart devices.
- 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 description was added about the method of removing 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.
- A description of the targets of the network monitoring functionality was added.
- The following description was added: If you install an agent in Windows 2000, Windows XP, or Windows Server 2003, in the **Agent Configuration** window, 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 **OK** in the JP1/IT Desktop Management dialog box for 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: Of 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.
- The following messages were added:

  KDEX1077-E, KDEX1078-W, KDEX1581-E, KDEX1582-W, KDEX1583-W, KDEX1584-E, KDEX1587-Q, KDEX1588-Q, KDEX1589-Q, KDEX1590-E, KDEX1591-W, KDEX1592-E, KDEX1593-E, KDEX4074-E, KDEX4075-E, KDEX4076-E, KDEX4202-E, KDEX4215-Q, KDEX4216-Q, KDEX4233-E, KDEX5399-E, KDEX5400-E, KDEX5435-E, KDEX5436-E, KDEX6119-E, KDEX6151-E, KDEX6152-E, and KDEX6511-E
- The following messages were changed:

  KDEX1505-E, KDEX1506-E, KDEX4020-E, KDEX4023-E, KDEX4085-I, KDEX4100-E, KDEX4221-E, KDEX5071-W, KDEX5407-E, KDEX5415-E, KDEX5423-E, KDEX5426-E, KDEX5427-E, KDEX5428-E, KDEX5430-E, KDEX5431-I, KDEX5432-I, KDEX8003-I, KDEX8022-W, and KDEX8030-E
- Events (event numbers 1120, 1121, and 1122) were added.
- Events (event numbers 1107 and 1108) were changed.
- Port numbers of the controller and remote control agent were modified.
- The description of actions that trigger communication between a management server and an agent was 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 (updated program information)
  - AntivirusInfo (anti-virus product information)
  - ActionDefinition (JP1/ITDesktop 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.
- The following information was combined into the JP1 Version 10 JP1/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, for example, kilobyte (KB)
  - Glossary

(15) Changes in version 09-51

(a) Changes in the manual (3020-3-S95-10)

- 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 from the site server 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 to 1116 were added to the events for which action needs to be taken.
- The following messages were added:

  KDEX3299-I, KDEX3300-E, KDEX3301-I, KDEX3302-E, KDEX3303-I, KDEX3304-E, KDEX5104-I, KDEX5396-I, KDEX5397-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, KDEX8031-I, KDEX8032-W, KDEX8033-E, KDEX8034-E, KDEX8035-W, KDEX8036-E, KDEX8037-E, KDEX8038-E, and KDEX8039-E
- The following messages were changed:

  KDEX5000-I and KDEX5010-W
- Events (event numbers 1105 to 1116) were added.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Hitachi, Ltd.
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan