HITACHI
Inspire the Next

JP1 Version 13

JP1/IT Desktop Management 2 Configuration Guide

3021-3-L73-10(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-2A42-78DL JP1/IT Desktop Management 2 - Manager 13-01

The above product includes the following:

• P-CC2A42-7ADL JP1/IT Desktop Management 2 - Manager (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

• P-CC2A42-7BDL JP1/IT Desktop Management 2 - Agent (for Windows Server 2022, Windows 11, Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

• P-CC2A42-7CDL JP1/IT Desktop Management 2 - Network Monitor (for Windows Server 2022, Windows 11, 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-CC2A42-7DDL JP1/IT Desktop Management 2 - Asset Console (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

• P-CC2A42-7PDL JP1/IT Desktop Management 2 - Internet Gateway (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-2A42-7KDL JP1/IT Desktop Management 2 - Operations Director 13-01

The above product includes the following:

• P-CC2A42-7ADL JP1/IT Desktop Management 2 - Manager (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

• P-CC2A42-7BDL JP1/IT Desktop Management 2 - Agent (for Windows Server 2022, Windows 11, Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

• P-CC2A42-7CDL JP1/IT Desktop Management 2 - Network Monitor (for Windows Server 2022, Windows 11, 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-CC2A42-7PDL JP1/IT Desktop Management 2 - Internet Gateway (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

■ Trademarks

Microsoft, Active Directory are trademarks of the Microsoft group of companies.

Microsoft, Internet Explorer are trademarks of the Microsoft group of companies.

Microsoft, Windows are trademarks of the Microsoft group of companies.

Microsoft, Windows Server are trademarks of the Microsoft group of companies.

Microsoft, Windows Vista are trademarks of the Microsoft group of companies.

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

UNIX is a trademark of The Open Group.

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

Dec. 2023: 3021-3-L73-10(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-L73-10(E)) and product changes related to this manual.

Changes	Location
The flow rate control can be performed with relay system.	3.12
Added Microsoft Intune to MDM system to work with.	4.5.1

Legend: --: Not applicable

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

Preface

This manual describes how to build JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Operations Director systems. Hereinafter, the term JP1/IT Desktop Management 2 is used to refer to both JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Operations Director.

Some functions of JP1/IT Desktop Management 2 - Operations Director are restricted compared to JP1/IT Desktop Management 2 - Manager. For details about these restrictions, see 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 those who:

- Want to build a JP1/IT Desktop Management 2 system.
- Want to learn about how to build JP1/IT Desktop Management 2, how to perform overwrite installations, how to uninstall the product, or how to migrate an environment.

■ Organization of this manual

This manual is organized into the following chapters and an appendix:

1. Building management servers and agents

   This chapter describes how to build management servers and agents.

2. Building system configurations

   This chapter describes how to build each system configuration.

3. Changing settings

   This chapter describes how to change the settings you specified when setting up a management server.

4. Customizing the settings specified when building a system

   This chapter describes the items you can customize when specifying settings during the building of a system.

5. Overwrite-installing the product and updating the components

   This chapter describes overwrite installation of JP1/IT Desktop Management 2 - Manager, and how to update the various components (agents, relay systems, and network monitor agents).

6. Uninstalling products

   This chapter describes how to uninstall JP1/IT Desktop Management 2 programs.

7. Migrating environments

   This chapter describes how to migrate an environment in JP1/IT Desktop Management 2.

8. Commands used for building-related operations

This chapter describes the JP1/IT Desktop Management 2 commands you can use to build a system, change settings, and replace devices.

9. Troubleshooting

This chapter describes the actions you can take if problems occur while building JP1/IT Desktop Management 2.

A. Miscellaneous Information

This appendix provides miscellaneous information for users of JP1/IT Desktop Management 2.

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

Contents

Index 318

1 Building Management Servers and Agents

This chapter describes how to build management servers and agents. First, you build management servers and agents to prepare a base system. For the base system, you can select one of the following configurations: the minimal configuration, basic configuration, or multi-server configuration.

After building a base system, change the settings or add system components to tailor the system according to your administrative objectives. If you intend to build a system that is not a base system, see 2. Building system configurations first.

1.1 Building a base system

1.1.1 Overview of building a minimal configuration system

Building a minimal configuration system involves building a management server, and then installing the agent software on the computers that the management server will manage.

1. Build the management server.
2. Register the JP1/IT Desktop Management 2 product license.
3. Log in to the operation window and set user account information.
4. Have a good understanding of the devices in the organization, and decide which computers to install the agent on and the installation method.
5. Install an agent on the computers that will be managed by JP1/IT Desktop Management 2.

This completes the process of building a minimal configuration system.

Related Topics:

- 1.2 Creating a management server environment
- 1.3 Registering a Product License
- 1.4 Logging in to the Operation Window
- 1.5 Identifying all devices used in your organization
- 1.6 Manually installing agents on computers
- 1.7 Automatically installing agents on computers

1.1.2 Overview of building a basic configuration system

To build a basic configuration system, first build the management server environment, and then build the relay systems.

1. Build the management server environment.
2. Register the product license of JP1/IT Desktop Management 2.
3. Log in to the operation window, and then set the user account information.
4. Install and set up the relay system program on the computers that will serve as relay systems.
5. Understand the devices in your organization beforehand, and plan on which computers and in what way you will install the agent software.
6. Install the agent software on the computers to be managed by JP1/IT Desktop Management 2.

This completes the process of building a basic configuration system.

Tip

You can also install Remote Install Manager on its own on a different computer from the management server.

Related Topics:

- 1.2 Creating a management server environment
- 1.8 Building the environment of a relay system
- 1.3 Registering a Product License
- 1.4 Logging in to the Operation Window
- 1.6 Manually installing agents on computers
- 1.7 Automatically installing agents on computers
- 1.9.1 Procedure for installing Remote Install Manager only

1.1.3 Overview of building a multi-server system

To build a multi-server system, build the primary management server, and then build management relay servers.

1. Build the primary management server environment.
2. Build the management relay server environments.
3. On the primary management server, register the product license for JP1/IT Desktop Management 2.
4. To manage the number of used product licenses and number of available product licenses for JP1/IT Desktop Management 2 on individual management servers, execute the `distributelicense` command to give license registration permission to each management relay server. Alternatively, use the command to distribute the JP1/IT Desktop Management 2 product license to each management relay server.

   On the management relay servers on which product licenses can now be registered, register the product license.
5. Log in to the operation window of each management server, and then set the user account information.
6. Be aware of the state of all devices in the organization, and make an agent deployment plan, including the determination of the target computers and method of deployment.
7. Deploy an agent on each computer to be managed by JP1/IT Desktop Management 2.

You can build a multi-server system using the above procedure.

Related Topics:

- 1.2 Creating a management server environment
- 1.3 Registering a Product License
- 1.4 Logging in to the Operation Window
- 1.6 Manually installing agents on computers
- 1.7 Automatically installing agents on computers
- 8.11 distributelicense (distributing licenses)

1.2 Creating a management server environment

To build a management server, install and set up JP1/IT Desktop Management 2 - Manager.

After you decide on an installation type (installation in a single-server configuration or multi-server configuration), perform installation by referring to the relevant section.

Building an environment with a single-server configuration

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration

Building an environment with a multi-server configuration

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration
- 1.2.3 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management relay server)
- 1.2.5 Procedure for setting up a management relay server

1.2.1 Types of JP1/IT Desktop Management 2 - Manager installation

The following are the JP1/IT Desktop Management 2 - Manager installation types. During installation, select the appropriate type for your needs.

Quick installation

Use this type of installation to set up the product with a minimum number of operations. Default values are used for the settings and setup. We recommend this method when no special settings are required.

Custom installation

Install the product by specifying each setting. You must perform setup after installation to create a database. We recommend this method if you want to use special values for installation and setup. When you build a multi-server configuration system or install a server with the large-scale management option enabled, you must select this type.

1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)

To install JP1/IT Desktop Management 2 - Manager, you must log on to the OS as a user with administrator permissions.

Important

If you install the product on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the user permission level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the program might not operate correctly even if you install it again later.

Important

On a computer running Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders during installation:

- Folders under *system-drive*`:\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

Important

Before installation, make sure that all Windows applications have been closed. If you perform installation without terminating JP1/IT Desktop Management 2 - Manager, restart the OS regardless of whether installation was successful. If the service JP1_ITDM2_Service does not start or JP1/IT Desktop Management 2 - Manager does not run when the OS is restarted, use the following procedure to perform installation again:

1. Close all Windows applications.
2. Stop the service (`JP1_ITDM2_Service`).
3. Perform overwrite installation again. (The service you stopped will start.)

Important

Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

To install JP1/IT Desktop Management 2 - Manager:

1. Insert the media supplied with the product in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Manager**, and then click the **Install** button.
3. In the dialog box indicating the start of the installation, click the **Next** button.
4. In the **License Agreement** dialog box, check the displayed information, select **I accept the terms in the license agreement**, and then click the **Next** button.
5. In the **Installation type** dialog box, select the installation type, and then click the **Next** button.
   If you choose quick installation, go to step 7.
   Do not select quick installation if the installation-target server is to be used as the primary management server in a multi-server configuration. In this case, select *custom installation*.
6. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.

7. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.

   When you choose quick installation, specify the folder in which you want to create the database.

8. In the **Database Settings** dialog box, specify the user ID and password required to use the database, and then click the **Next** button.

   This step is required if you selected **Quick installation**. If you selected **Custom installation**, you can enter settings related to the database during the setup process.

   > **Tip**
   >
   > Specify the user ID using a maximum of 8 single-byte alphanumeric characters. The first character must be an alphabetic character. The default is `itdm2m`. The password can be a maximum of 28 single-byte alphanumeric characters, of which the first character is an alphabetic character. Take care to remember this user ID and password, which will be required when using JP1/IT Desktop Management 2 - Asset Console.

   > **Important**
   >
   > Do not specify `root`, `ALL`, `MASTER`, `netmdm`, or `PUBLIC` for the user ID (case-insensitive).

9. In the dialog box where you select the component to install, select Manager, specify the installation method, and then click the **Next** button.

   This step is required when performing a custom installation.

   > **Tip**
   >
   > When installing JP1/IT Desktop Management 2 - Manager, you also need to install Remote Install Manager. You cannot install JP1/IT Desktop Management 2 - Manager if you select **This feature will not be available.** from the pull-down menu for Remote Install Manager.
   >
   > You can select the installation method from the pull-down menu that appears when you click the icon to the left of the label.

10. In the **Type of Manager to Install** dialog box, select **The management server in a single-server configuration, or the primary management server in a multi-server configuration**, and then click the **Next** button.

    If you operate 50,000 devices or more in a large-scale environment, select the **For large-scale management** check box.

    This step is required when performing a custom installation.

11. In the confirmation dialog box for the installation, make sure the information you selected for the installation is correct, and then click the **Install** button.

    Installation starts. If you notice a problem during the installation, click the **Back** button and make the necessary correction.

12. When the installation finishes, click the **Completed** button.

Installation of JP1/IT Desktop Management 2 - Manager is complete. If a message asking you to restart the computer appears, restart it.

For a quick installation, setup is performed automatically during installation allowing you to log in to JP1/IT Desktop Management 2 and start using it as soon as installation is complete.

In a custom installation, you must perform setup after installation to create a database. If you select **Setup** when installation is complete, setup will start automatically.

Tip

When installation is complete, a shortcut for logging in to the operation window is created on the desktop. In a custom installation, the shortcut cannot be used until setup is complete.

Important

After installing JP1/IT Desktop Management 2 - Manager, even though the following messages might be output to the event log (system), these messages do not affect the operation of the product.

- The JP1_ITDM2_Agent Remote Control service is marked as an interactive service.
  However, the system is configured to not allow interactive services.
  This service may not function properly.
- The JP1_ITDM2_Agent Service service is marked as an interactive service.
  However, the system is configured to not allow interactive services.
  This service may not function properly.
- The JP1_ITDM2_Agent Monitor Control service is marked as an interactive service.
  However, the system is configured to not allow interactive services.
  This service may not function properly.

1.2.3 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management relay server)

Before you install JP1/IT Desktop Management 2 - Manager, log on to the OS as a user with administrator permissions.

Important

You cannot install a management relay server on a computer on which JP1/IT Desktop Management 2 - Agent is installed.

Important

If the installation target is a Windows computer that supports User Account Control (UAC), a dialog box that prompts you to elevate your permission level might appear. If this dialog box appears, elevate your permission level.

Important

Do not shut down the OS while installation is in progress. If you do so, re-installation later might not be successful.

Important

On a computer that runs Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders during installation:

- Folders in the *system-drive*:\program files\WindowsApps folder
- Folders in storage areas created by virtual provisioning

Important

Before you start installation, terminate all Windows applications. If you perform installation while the JP1/IT Desktop Management 2 - Manager program is running, after installation, restart the OS regardless of whether installation was successful. If the necessary services do not start or the JP1/IT Desktop Management 2 - Manager program does not run after restarting the OS, use the following procedure to re-install the program:

1. Terminate all Windows applications.
2. Stop the JP1_ITDM2_Service.
3. Re-perform an overwrite installation. The service will restart.

Important

Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

To install JP1/IT Desktop Management 2 - Manager on the computer to be used as a management relay server:

1. Set the distribution media on the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that appears, select **JP1/IT Desktop Management 2 - Manager**, and then click the **Install** button.
3. In the dialog box that appears, click the **Next** button.
4. In the **License Agreement** dialog box, read the agreement, select **I accept the terms in the license agreement**, and then click the **Next** button.
5. In the **Installation type** dialog box, select **Custom installation**, and then click the **Next** button.
6. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.
7. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.
8. In the component selection dialog box that appears, select *Manager* as the component to be installed, specify the installation method, and then click the **Next** button.

> **Tip**
>
> If you install Manager, you must also install Remote Install Manager. Note that Remote Install Manager is not installed if **This feature will not be available** is selected as the installation mode.
>
> You can select the installation mode from the context menu that is displayed by clicking the icon on the left of the character string (*Manager* or *Remote Install Manager*).

9. In the **Type of Manager to Install** dialog box, select **Management relay server**, and then click the **Next** button.
10. In the **Agent Component Settings** dialog box, select the component to be included in the management relay server, and then click the **Next** button.
11. In the dialog box that appears, confirm that the installation settings are correct, and then click the **Install** button.
    Installation starts. If the installation settings are not correct, click the **Back** button and make the necessary corrections in the settings.
12. Click the **Finish** button to complete installation.

Now you have installed JP1/IT Desktop Management 2 - Manager on the computer to be used as a management relay server. If you are prompted to restart the computer, restart it.

After completing installation, you must perform setup to create a database. If you select the **Setup** check box, setup automatically starts when installation finishes.

> **Tip**
>
> When installation finishes, a shortcut for logging in to the operation window is created on the desktop. However, you can use this shortcut only after setup finishes.

> **Important**
>
> After installing JP1/IT Desktop Management 2 - Manager, even though the following messages might be output to the event log (system), these messages do not affect the operation of the product.
>
> - The JP1_ITDM2_Agent Remote Control service is marked as an interactive service.
>   However, the system is configured to not allow interactive services.
>   This service may not function properly.
> - The JP1_ITDM2_Agent Service service is marked as an interactive service.
>   However, the system is configured to not allow interactive services.
>   This service may not function properly.
> - The JP1_ITDM2_Agent Monitor Control service is marked as an interactive service.
>   However, the system is configured to not allow interactive services.
>   This service may not function properly.

1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration

When you perform a custom installation of JP1/IT Desktop Management 2 - Manager, you must perform setup as soon as installation is complete to create a database and specify environment settings.

To set up a management server:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.

2. In the **Setup** view, click the **Next** button.

3. In the **Select a Setup** view, select a setup type, and then click the **Next** button.
   This view does not appear for the initial setup after installation.

4. In the **Database Settings** view, select whether to change the password for accessing the database, and then click the **Next** button.
   If you decide to change the password, enter the current password and the new password, and go to step 18.
   This view does not appear during the initial setup after installation. It appears when you perform setup of the Manager in a non-cluster environment or of the active node in a cluster environment for the second and subsequent time after selecting **Settings Modification** in the **Select a Setup** view in step 3.

   > **Tip**
   >
   > The user ID you set during quick installation or during the initial setup is displayed. As the password, specify a maximum of 28 single-byte alphanumeric characters, the first of which is an alphabetic character. The password you specify is needed to use JP1/IT Desktop Management 2 - Asset Console. Take care not to forget it.

5. In the **Cluster Environment** view, specify the settings for using a cluster system, and then click the **Next** button.
   When specifying the settings for using a cluster system, if you select **Secondary**, you do not need to perform steps 6 to 8 and steps 10 to 18.

6. In the **Select the Server Configuration** view, select the server configuration, and then click the **Next** button.

7. In the **Database Settings** view, set the user ID and password required to access the database, and then click the **Next** button.
   This view does not appear when you perform setup in a non-cluster environment or of the active node in a cluster environment for the second or subsequent time.

   > **Tip**
   >
   > Specify the user ID using a maximum of 8 single-byte alphanumeric characters. The first character must be an alphabetic character. The default is `itdm2m`. The password can be a maximum of 28 single-byte alphanumeric characters, of which the first character is an alphabetic character. Take care to remember this user ID and password, which will be required when using JP1/IT Desktop Management 2 - Asset Console.

Important

Do not specify `root`, `ALL`, `MASTER`, `netmdm`, or `PUBLIC` for the user ID (case-insensitive).

8. In the window that appears, set the IP address of the management server and the cache size to use when accessing the database. Then, click the **Next** button.

Tip

For the cache size to use when accessing the database, as a guide, specify 1 GB when the number of the managed computers is 10,000 or fewer, specify 16 GB when the number of the managed computers is from 10,000 to 50,000.

When the **For large-scale management** check box is selected during installation, specify the cache size for database access based on the number of managed devices.

9. In the **Folder Settings** view, specify the folders that will be used by JP1/IT Desktop Management 2 - Manager, and then click the **Next** button.

   If you selected **Secondary** in the settings for using a cluster system in step 5, skip steps 7 to 11.

10. In the **Operation Log Settings** view, specify whether to record an operation log, and then click the **Next** button.

    If you do not want to acquire operation log data, go to step 14.

11. In the view that appears, set whether to retain operation log data, and then click the **Next** button.

12. In the view that appears, set the number of managed devices, the maximum number of days for which to store operation log data in the database, and the database folder for operation log data. Then, click the **Next** button.

13. You can improve the performance when searching operation log data by increasing the size of the database cache. Specify the amount of cache you want to add, and then click the **Next** button.

14. In the **Output Settings for Saving the Revision History** view, specify whether to periodically output a revision history archive, and then click the **Next** button.

15. In the **Port Number Settings** view, specify the port number to be used by JP1/IT Desktop Management 2 - Manager, and then click the **Next** button.

16. In the **Settings for Address Resolution** view, select the type of information (host name or IP address) the management server uses to identify the computers with which it communicates. If you select **Host name**, specify the method of name resolution and the action to take when name resolution fails.

    The type of information used to identify computers is called the *ID key for operations*.

17. In the **User Management Settings** window, select whether to manage users by using JP1/Base. If you select this option, specify the name of the JP1 resource group to which the JP1 users in JP1/IT Desktop Management 2 are associated.

Tip

To manage users by using JP1/Base, before performing setup, you will need to set JP1 users, JP1 resource groups, and JP1 permission levels on the JP1/Base authentication server. For details about how to build a configuration system that manages users by using JP1/Base, see 2.7.1 Building a configuration system that uses JP1 authentication. For details about the setup procedures to be performed on the authentication server, see the *JP1/Base User's Guide*.

18. In the **Other Settings** view, select the currency symbol to display in the user interface, and whether to control bandwidth when performing ITDM-compatible distribution. Then, click the **Next** button.

19. In the view that appears, specify how many times a user can enter the wrong password in succession before the account is locked, the valid period for user passwords, and whether to suppress operations on asset information from the operation window. Then, click the **Next** button.

20. In the **Confirm Setup Settings** view, make sure the setup is correct, and then click the **Next** button.

    If you notice a problem, click the **Back** button and make the necessary correction.

21. In the **Setup for Distribution by Using Remote Install Manager** view, enter the settings related to distribution using Remote Install Manager, and then click the **OK** button.

    To change settings from the default, select each tab and enter the new settings. For details about the settings on each tab and the values you can specify, see the description of setup parameters in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*. An overview of each tab is given below.

    Related to Communications

    You can set communication-related parameters including the port number used for distribution by Remote Install Manager and the interval to use when transferring files to agents and relay systems.

    Server Customization Options

    You can set server parameters including the number of lower systems that can connect to the management server concurrently and the number that can execute jobs concurrently. You can also specify whether to monitor the startup of lower systems, and whether to monitor file transfer errors.

    Multicast Distribution

    You can specify settings related to multicast distribution, such as the port number used for multicast distribution, the multicast address, and the packet size to use when distributing jobs.

    Result Recording Options

    You can specify settings related to job results, including whether to record job execution results, and whether to record execution results for each client when a job is executed with an ID group as the destination. You can also specify the job execution statuses for which you want to record execution results.

    Related to System Configurations

    You can specify settings related to the system configuration. This includes whether to automatically apply changes to lower systems when configuration information is changed in JP1/IT Desktop Management 2, and whether to keep a record of computers deleted from the system configuration information in JP1/IT Desktop Management 2. In a multi-server configuration, the **Synchronize when the system configuration changes** setting is always enabled.

    Event Service

    You can specify settings relating to the event service. This includes whether to notify JP1/IM of job results and errors in JP1/IT Desktop Management 2 as JP1 events, and whether to notify JP1/IM when a job or command ends normally or with an error.

    Related to Failures

    Settings you can specify include the number of log generations to keep, the number of log entries to output, and the types of message to output to the Event Viewer in Windows NT.

    Audit Log

    You can specify the degree of detail to use when outputting audit log data.

22. In the **Setup Complete** window, click the **OK** button.

In some circumstances, **Register components**, **Automatically update components**, or **Register components as a distribution package** will appear in the **Setup Complete** window and can be selected. Which of these options appears depends on the timing with which setup was performed and the setup type that was selected.

If **Register components** is displayed:

Select this check box when creating an installation set or when using ITDM-compatible distribution to distribute components from the management server. If you select this check box, the **Component Registration** dialog box will appear when you close the **Setup Complete** dialog box. In the **Component Registration** dialog box, specify the components to register in the folders. When executing the setup from the installer, **Register components** will not be displayed and the component will be registered automatically.

If **Automatically update components** is displayed:

Select this check box to automatically send the component registered in **Register components** to the agent and update it when the agent connects to the management server.

If **Register components as a distribution package** is displayed:

Select this check box to register the components as a distribution package. When not updating automatically, this allows you to update components by registering them as packages for distribution using ITDM-compatible distribution.

You can also select these settings after setup is complete by selecting **Component Registration** from the **Start** menu.

For details about updating components, see 5.8 Updating components.

When setup is complete, the management server starts operation with the specified settings.

> **Tip**
>
> In the initial setup after a custom installation, a new database is created as part of the setup process.

1.2.5 Procedure for setting up a management relay server

If you have just installed JP1/IT Desktop Management 2 - Manager on a computer that is to be used as a management relay server, you must perform setup to create a database and specify environment settings.

To set up a management relay server:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
2. In the setup window, click the **Next** button.
3. In the **Select a Setup** window, select the setup type, and then click the **Next** button.
   This window does not appear during the first setup after installation.
4. In the **Database Settings** window, select whether to change the password for accessing the database, and then click the **Next** button.
   If you choose to change the password, enter the current and new passwords, and then go to step 22.
   This window appears when you select **Reconfiguration** as the setup type in step 3.
   This window does not appear during the first setup after installation.

> **Tip**
>
> The user ID you specified during the first setup is displayed in this window. The password is a character string consisting of 28 or fewer single-byte alphanumeric characters and begins with an alphabetic character. Do not forget the new password entered here because it will be needed to use JP1/IT Desktop Management 2 - Asset Console.

5. In the **Database Settings** window, set the user ID and password for accessing the database, and then click the **Next** button.

   This window appears during the first setup after installation, and when you select **Server reconfiguration** as the setup type in step 2.

   This window appears only during the first setup after installation.

> **Tip**
>
> For the user ID, enter a character string consisting of eight or fewer single-byte alphanumeric characters and begins with an alphabetic character. The default value is itdm2m. For the password, enter a character string that consists of 28 or fewer single-byte alphanumeric characters and begins with an alphabetic character. Do not forget the user ID and password entered here because they will be needed to use JP1/IT Desktop Management 2 - Asset Console.

> **Important**
>
> Do not specify `root`, `ALL`, `MASTER`, `netmdm`, or `PUBLIC` for the user ID (case-insensitive).

6. In the **Database Settings** window, set the IP address of the management server that is used to access the database and the size of cache to be used when accessing the database, and then click the **Next** button.

   You can only select the size of the cache to be used when accessing the database during the first setup after installation. The second and subsequent times setup is performed, the cache size selected during the initial setup is already selected and cannot be changed.

> **Tip**
>
> For the cache size to use when accessing the database, as a guide, specify 1 GB when the number of the managed computers is 10,000 or fewer, specify 16 GB when the number of the managed computers is from 10,000 to 30,000.

7. In the **Folder Settings** window, specify the folders used by JP1/IT Desktop Management 2 - Manager, and then click the **Next** button.

8. In the **Operation Log Settings** window, specify whether to use the operation log, and then click the **Next** button.

   If you choose not to use the operation log, go to step 12.

9. In the window that appears, specify whether to store the operation log data, and then click the **Next** button.

10. In the window that appears, specify the number of devices to be managed, maximum number of days to keep logged data in the operation log database, and the location and name of the operation log database folder, and then click the **Next** button.

11. You can increase the database cache size to improve the search performance of the operation log. To do so, in the window that appears, set the size of cache to be added, and then click the **Next** button.

12. In the **Output Settings for Saving the Revision History** window, specify whether to periodically output the revision history archive, and then click the **Next** button.

13. In the **Port Number Settings** window, set the port numbers used by JP1/IT Desktop Management 2 - Manager, and then click the **Next** button.

    Set the same port numbers on the local server, higher management server, and lower management relay servers.

14. In the **Settings for Address Resolution** window, select the type of information (host name or IP address) that is used to determine the computer to be connected during inter-host communication. If you choose to use the host name, also set the address resolution method and the action to be taken if address resolution fails.

    The type of information you select here is called the *ID key for operations*.

15. In the **Management Relay Server Settings** window, specify the higher management server of the connection-destination host. In addition, select whether to notify the higher management server of the operation log information and USB device registration information collected from the managed computers.

    For **Host name or IP address**, specify the setting by using the operation key selected in the **Settings for Address Resolution** window of the higher management server.

16. In the **Communication Settings** window, set the interval for polling to the higher-level server, polling interval, and whether to try again if a communication error occurs, and then click the **Next** button.

    If **Remote control agent** was not selected in the **Agent Component Settings** dialog box during installation of JP1/IT Desktop Management 2 - Manager, go to step 19.

17. In the **Remote Control Settings** window, specify the startup processing mode, connection settings, and connection mode as the remote control settings on the management relay servers, and then click the **Next** button.

18. To specify the advanced remote control settings, in the **Remote Control Settings** window, specify the settings as you want, and then click the **Next** button.

    To limit the controllers you want to allow to perform remote control, in **Settings of Allowed Controllers**, click the **Add** button to enter the host name or IP address of the controllers to be allowed, and add those controllers.

    To use user authentication when users attempt to connect to controllers, in **User Settings**, click the **Add** button to add the users permitted to connect to the controllers.

19. In the **User Management Settings** window, select whether to manage users by using JP1/Base. If you select this option, specify the name of the JP1 resource group to which the JP1 users in JP1/IT Desktop Management 2 are associated.

    Tip

    To manage users by using JP1/Base, before performing setup, you will need to set JP1 users, JP1 resource groups, and JP1 permission levels on the JP1/Base authentication server. For details about how to build a configuration system that manages users by using JP1/Base, see 2.7.1 Building a configuration system that uses JP1 authentication. For details about the setup procedures to be performed on the authentication server, see the *JP1/Base User's Guide*.

20. In the **Other Settings** window, set the currency sign to be displayed in the operation window and whether to perform traffic control when using the ITDM-compatible distribution function, and then click the **Next** button.

21. In the window that appears, set the number of consecutive login failures before the account is locked, number of days until the password expires, and whether to suppress operation on asset information from the operation window. Then, click the **Next** button.

22. In the **Confirm Setup Settings** window, confirm that the specified setup settings are correct, and then click the **Next** button.

    If the specified setup settings are incorrect, click the **Back** button, and make the necessary changes.

23. In the **Setup for Distribution by Using Remote Install Manager** window, specify settings related to distribution using Remote Install Manager, and then click the **Next** button.

    When you click the **Next** button, the setup process begins. If you click **Cancel** button, setup is canceled and the window closes.

    To change a setting from its default, select the relevant tab, and then specify the new setting. For details about settings and values that can be specified in each tab, see the description of setup parameters in the *JP1/IT Desktop Management 2 Overview and System Design Guide*. The following provides only a brief explanation of settings that can be specified in each tab.

    Related to Communications

    In this tab, you can specify settings such as: The port number to be used for distribution using Remote Install Manager and the interval for transferring files to agents and relay systems.

    Server Customization Options

    In this tab, you can specify settings such as: The maximum number of lower systems that can connect to a management server, maximum number of lower systems that can execute jobs simultaneously, monitoring of started lower systems, and monitoring file transfer errors.

    Multicast Distribution

    In this tab, you can specify settings such as: The port number used for multicast job distribution, multicast address, and packet size for job distribution.

    Result Recording

    In this tab, you can specify settings such as: Whether to record job execution results, whether to record the execution results of a job executed with an ID group as the destination for each client, and the execution status of jobs subject to recording.

    Related to System

    In this tab, you can specify settings such as: Whether to store the historical data logged when hosts are removed from the JP1/IT Desktop Management 2 system configuration information.

    Event Service

    In this tab, you can specify settings such as: Whether to report (to JP1/IM) the results of executed jobs and errors that occurred in JP1/IT Desktop Management 2 as JP1 events, and whether to report (to JP1/IM) normal terminations and error occurrences for jobs or commands.

    Related to Failures

    In this tab, you can specify settings such as: The number of log generations to be managed, maximum number of log entries that can be output, and types of messages to be output to the Windows NT event viewer.

    Audit Log

    In this tab, you can specify the granularity of audit log data to be output.

24. In the Setup Complete window, click the **OK** button.

    In some circumstances, **Register components**, **Automatically update components**, or **Register components as a distribution package** will appear in the **Setup Complete** window and can be selected. Which of these options appears depends on the timing with which setup was performed and the setup type that was selected.

    If **Register components** is displayed:

    Select this check box when creating an installation set or when using ITDM-compatible distribution to distribute components from the management server. If you select this check box, the **Component Registration** dialog box will appear when you close the **Setup Complete** dialog box. In the **Component Registration** dialog box, specify

the components to register in the folders. When executing the setup from the installer, **Register components** will not be displayed and the component will be registered automatically.

If **Automatically update components** is displayed:

Select this check box to automatically send the component registered in **Register components** to the agent and update it when the agent connects to the management server.

If **Register components as a distribution package** is displayed:

Select this check box to register the components as a distribution package. When not updating automatically, this allows you to update components by registering them as packages for distribution using ITDM-compatible distribution.

You can also select these settings after setup is complete by selecting **Component Registration** from the **Start** menu.

For details about updating components, see 5.8 Updating components.

Setup finishes, and the management relay server is ready to operate with the specified settings.

Tip

During the first setup, a new database is created.

1.3 Registering a Product License

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

1.3.1 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:

- 1.3.2 Adding a product license

1.3.2 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:

- 1.3.1 Registering a product license

1.3.3 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:

- 1.3.1 Registering a product license
- 8.11 distributelicense (distributing licenses)

1.4 Logging in to the Operation Window

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

1.4.1 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:

- 1.4.4 Unlocking a user account

1.4.2 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**.

1.4.3 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.

1.4.4 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.

1.5 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:

- 1.5.2 Planning the installation of agents

1.5.1 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:

- 4.1.1 Specifying search conditions (discovery from IP address)
- 1.7.3 Checking the device discovery status

1.5.2 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:

- 1.6 Manually installing agents on computers
- 1.7 Automatically installing agents on computers

1.6 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 1.6.1 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:

- 1.6.3 Uploading an agent to a Web server
- 1.6.4 Uploading an agent to a file server
- 1.6.5 Distributing the agent installation media (CD-R or USB memory) to users
- 1.6.6 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:

- 1.6.7 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:

- 1.6.8 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.

1.6.1 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:

- 4.1.3 Adding agent configurations
- 1.6.2 Installing agents on computers

1.6.2 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:

- 1.6.3 Uploading an agent to a Web server
- 1.6.4 Uploading an agent to a file server
- 1.6.5 Distributing the agent installation media (CD-R or USB memory) to users
- 1.6.6 Distributing agents to users as a file attached to an email
- 1.6.7 Installing an agent on the computer by using a logon script
- 1.6.8 Installing an agent on the computer by using the disk copy feature

1.6.3 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.

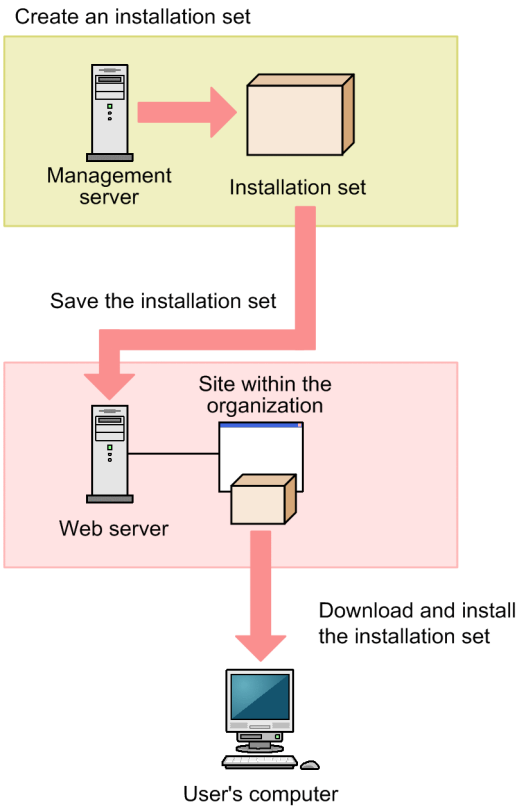
Advantage:

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:

- 1.6.1 Creating an installation set
- 1.7.1 General procedure for checking the agent installation status

1.6.4 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.

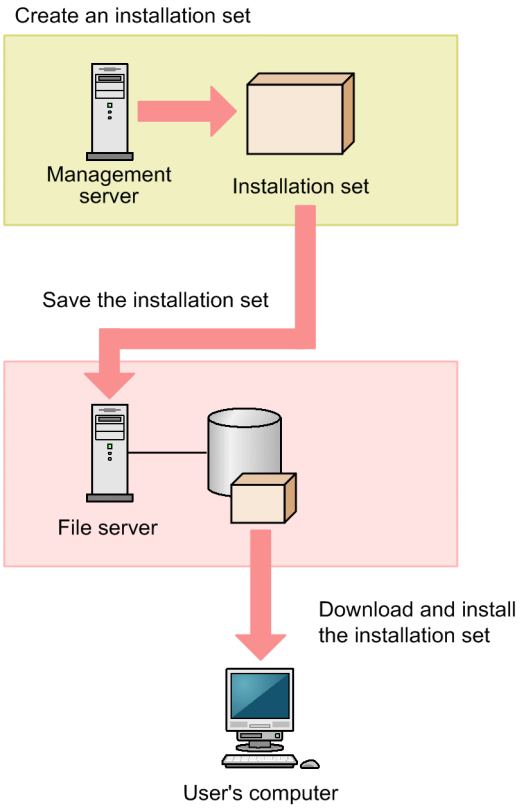
Advantage:

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:

- 1.6.1 Creating an installation set
- 1.7.1 General procedure for checking the agent installation status

1.6.5 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.

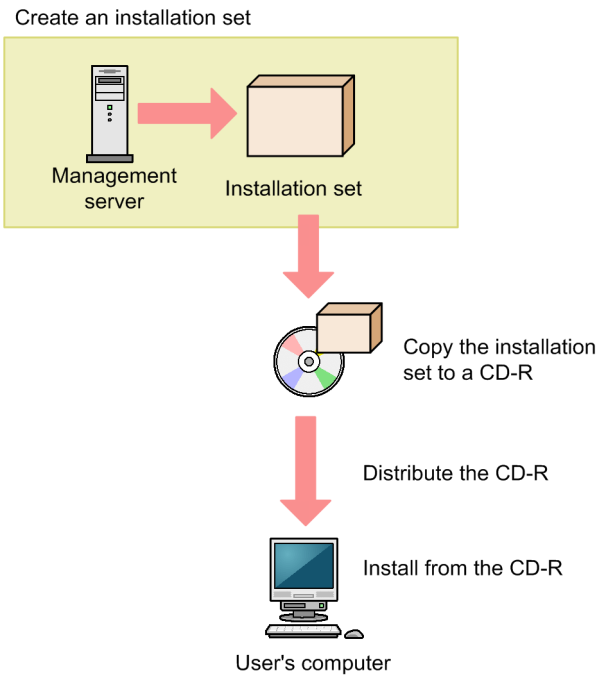
Advantage:

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:

- 1.6.1 Creating an installation set
- 1.7.1 General procedure for checking the agent installation status

1.6.6 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.

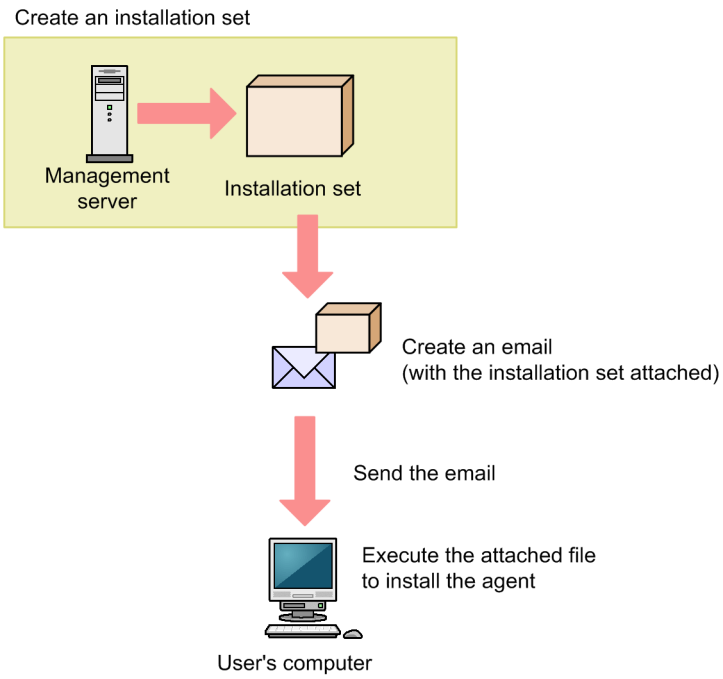
Advantage:

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:

- 1.6.1 Creating an installation set
- 1.7.1 General procedure for checking the agent installation status

1.6.7 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)
)
```

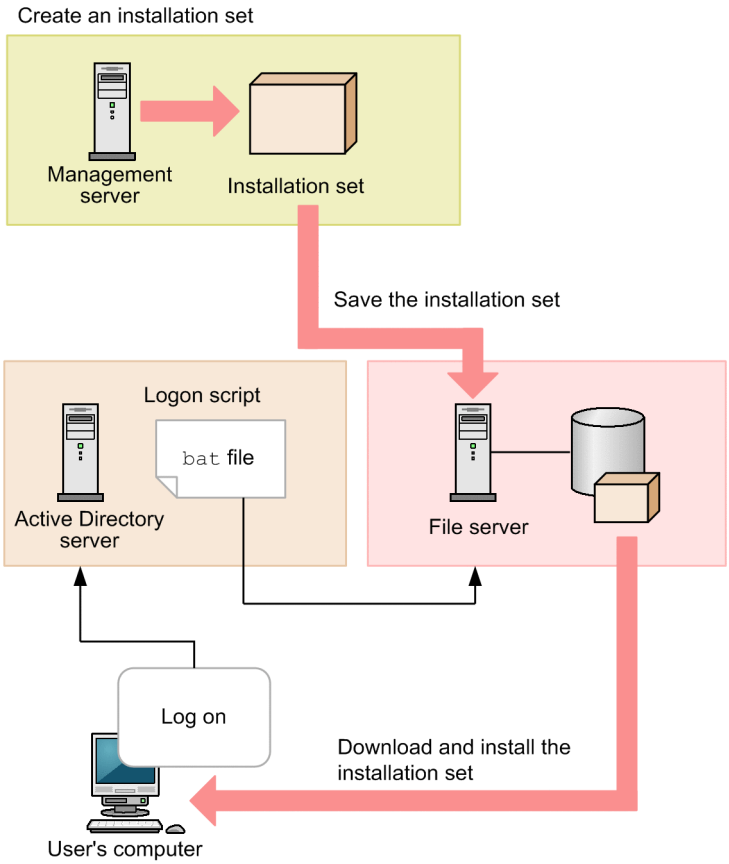
Advantage:

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:

- 1.6.1 Creating an installation set
- 1.7.1 General procedure for checking the agent installation status

1.6.8 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.

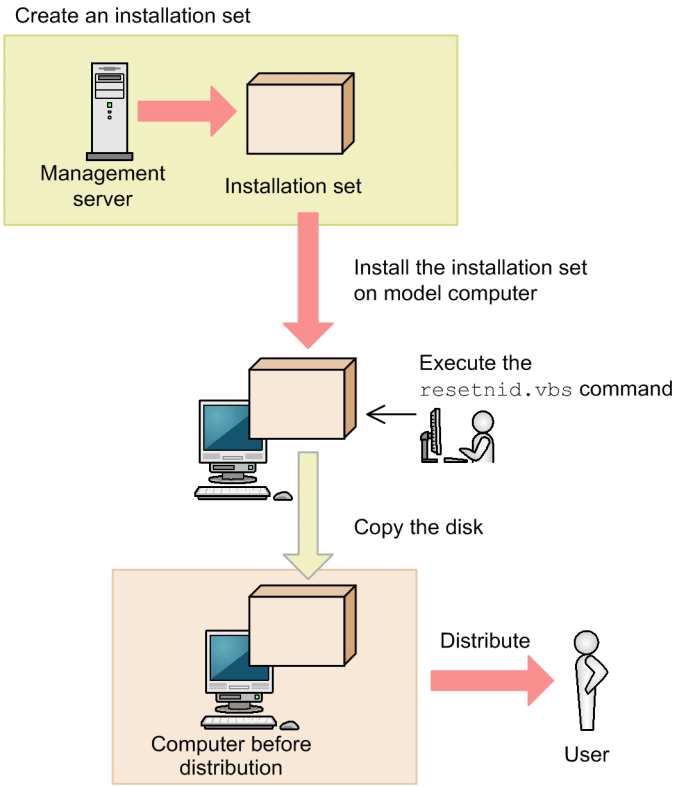
Advantage:

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:

- 1.6.1 Creating an installation set
- 1.7.1 General procedure for checking the agent installation status
- 8.10 resetnid.vbs (resetting the host ID)

1.6.9 Procedure for installing the agent from supplied media

When you install an agent, you must log on to the OS as a user with administrator permissions.

Important

When you install the agent on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the user permission level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the agent might not operate correctly even if you install it again later.

Important

On a computer that runs Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, or Windows Server 2012, do not specify the following folders during installation:

- Folders under *system-drive*`:\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

Important

When creating the agent environment, make sure that the directories defined in the TEMP and TMP user environment variable and system environment variable exist on the computer.

In case of the 64-bit Windows OS, do not define a directory which is under `%windir%\system32`, as TEMP and TMP for system variables and user variables. Also, do not install an agent in a directory under `%windir%\system32`.

Important

Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

To install the agent:

1. Insert the supplied media in the CD/DVD drive.
2. In the displayed **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Agent**, and then click the **Install** button.
3. In the dialog box indicating the start of installation, click the **Next** button.
4. In the **Installation type** dialog box, select the installation type, and then click the **Next** button.
   If you want to specify the installation folder, select custom installation. If you select quick installation, the default installation folder is set.
   If you selected quick installation, go to step 9.

Tip

The default installation folder for the agent is `C:\Program Files\HITACHI\jp1itdma`. If the OS is a 64-bit version of Windows, the default folder will be under the folder defined by *environment-variable*`%ProgramFiles(x86)%`(`C:\Program Files (x86)\Hitachi\jp1itdma\` when the OS is installed on the C drive).

Important

When the OS is 64-bit Windows, do not install the agent to a folder under `%WINDIR%\system32`.

Important

The SYSTEM and Administrators groups must have full control of the installation folder. For these groups, the **This folder, subfolders and files** option must be selected for **Apply To**.

5. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.
6. In the **Types of components to be installed** dialog box, select **Agent** and then click the **Next** button.
7. In the **Components to be installed** dialog box, select the component and subcomponents you want to install, and the installation method you want to use. Then, click the **Next** button.

Tip

The remote control agent is installed as a subcomponent of the agent.

You can select the installation method from the pull-down menu displayed by clicking the icon to the left of the label.

8. In the dialog box indicating the preparations for starting installation are complete, click the **Install** button.
   Installation starts.
9. When the installation finishes, click the **Complete** button.

Installation of the agent is complete, and the Setup dialog box opens. If a message asking you to restart the computer appears, restart it.

Tip

When you install JP1/IT Desktop Management 2 - Agent, Remote Control Agent is also installed. The Remote Control Agent program required on the destination computer when the remote control functionality is used.

Important

After installing JP1/IT Desktop Management 2 - Agent, even though the following messages might be output to the event log (system), these messages do not affect the operation of the product.

- The JP1_ITDM2_Agent Remote Control service is marked as an interactive service.

However, the system is configured to not allow interactive services.
This service may not function properly.

- The JP1_ITDM2_Agent Service service is marked as an interactive service.
  However, the system is configured to not allow interactive services.
  This service may not function properly.
- The JP1_ITDM2_Agent Monitor Control service is marked as an interactive service.
  However, the system is configured to not allow interactive services.
  This service may not function properly.

Important

This product does not support multiple execution of installation including a case that automatic update of an agent or a network monitor agent overlaps with a version upgrade installation by user operation. In this case, the dialog of the following message might be displayed.

"An error occurred during the installation of JP1/IT Desktop Management 2 - Agent. Please contact the administrator."

1.6.10 Procedure for setting up the agent

When you install the agent from supplied media, you must setup the agent in order to connect to a management server.

To setup the agent, you must log on to the OS as a user with administrator permissions.

Note that setup of the agent for a management relay server is included in the setup of the management relay server. For details about the procedure for setting up a management relay server, see 1.2.5 Procedure for setting up a management relay server.

Tip

If you install the agent after distribution of the installation set or distribution from a management server, the connection destination is set automatically. You therefore do not need to set it yourself.

You can also use the file for connection destinations (`itdmhost.conf`) or the information file for higher connection destinations (`dmhost.txt`) to set the connection destination. You can store the file for connection destinations (`itdmhost.conf`) or information file for higher connection destinations (`dmhost.txt`) in the JP1/IT Desktop Management 2 - Manager data folder. When you create the installation data set, the file is incorporated into the installation set and distributed to the agents. However, if an agent already contains the file for connection destinations or the information file for higher connection destinations, the connection destination specified in that file has priority over the destination specified under **Basic Settings** in the agent configuration. If both the file for connection destinations and the information file for higher connection destinations exist on the agent, the information file for higher connection destinations is ignored. For details about the file for connection destinations (`itdmhost.conf`), see 1.6.11 Procedure for automatically setting the connection destination of agents. For details about the information file for higher connection destinations, see the description of automatically changing the agent connection destination in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

To set up the agent:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Administrator Tool**, and then **Setup**.

   If password protection is set for the agent, a dialog box for entering the password opens. Enter the password set for the applicable agent. The default password is `manager`.

2. On the **Connection-destination settings** tab of the **Setup (Agent)** dialog box, specify the host name or IP address of the connection-destination management server and the port number.

   In operation that uses a connection-destination configuration file (`itdmhost.conf`), this file is prioritized and connection destinations cannot be changed during setup.

3. In an environment where a computer incorporates multiple network adapters with multiple LAN connections, you can assign an order of priority to the network connections used by JP1/IT Desktop Management 2. To do so, on the **Communication settings** tab of the **Setup (Agent)** dialog box, click the **Settings for network adapters** button. In the dialog box that appears, specify the priority levels and whether to automatically update network adapter information, and then click the **OK** button.

4. In the confirmation dialog box that opens, click the **Yes** button.

When setup is complete, the agent starts operation with the specified settings.

Tip

If the connection between the agent and the management server already exists, you can set up the agent from the operation window. To set up the agent from the operation window, use the agent configurations.

1.6.11 Procedure for automatically setting the connection destination of agents

After information for determining connection destinations is distributed to agents, you can automatically set the connection destination by selecting an appropriate higher system from the IP addresses of managed computers. Because the connection destination automatically changes when the IP address of a computer changes, this function is useful when computers are moved. You can also manage distributed devices by providing multiple management servers for each range of IP addresses assigned to devices. This prevents the number of devices managed by a management server from exceeding the limit. This subsection describes how to automatically set the connection destination of agents.

You can use this function in JP1/IT Desktop Management 2 - Agent. Note that you cannot use this function in relay systems, agents for UNIX, and agents for Mac.

Note

To use this function, do not select the **Settings to Perform Polling for Multiple Higher Systems** check box under **Communication Settings** in the agent configuration. If, however, you are using the function that enables switching from one higher distribution system to another, enable multi-polling.

Note

If the connection destination of an agent is changed during startup of Package Setup Manager, a dialog box prompting you to update the Package Setup Manager window appears, and then the connection destination is switched to the new one.

Note

This function is not supported on the Citrix XenApp and Microsoft RDS server.

(1) Automatically setting and changing the higher system to connect to

To automatically set or change the higher system to connect to, you need to create a file for connection destinations (`itdmhost.conf`) in advance, and then distribute it to managed computers. The connection destination is automatically set at a certain time after distribution.

Creating a file for connection destinations

The file for connection destinations is used to determine the higher system to connect to. This file defines how the higher systems to connect to correspond with the IP address ranges of managed computers. For example, for the computers with IP addresses 172.16.22.1 through 172.16.22.255, a management server at the Tokyo branch office is defined as the connection destination. Similarly, for the computers with IP addresses 172.17.22.1 through 172.17.22.255, a management server at the Nagoya branch office is defined as the connection destination. For details about how to create the file for connection destinations, see (2) Creating the file for connection destinations (itdmhost.conf).

You can store the created file for connection destinations in the JP1/IT Desktop Management 2 - Manager data folder so that the file is incorporated in the installation set when you create the installation set.

Distributing the file for connection destinations to managed computers

If JP1/IT Desktop Management 2 - Agent is installed by using an installation set that contains a file for connection destinations, the file for connection destinations is stored in the following folder on each managed computer:

```
JP1/IT Desktop Management 2 Agent-installation-folder\MASTER\DB
```

If you register the file for connection destinations as a package and then create a job that distributes that package, you can distribute the package to managed computers. When doing so, specify the above folder as the distribution destination.

For computers that are not yet managed, you can store the file manually.

Time when the connection destination is determined

After you store the file for connection destinations on a managed computer, wait until polling (a job inquiry from the agent) is performed or restart the OS on the managed computer. The higher system to which the agent is connected is set according to the contents of the file for connection destinations.

The following three types of polling can be used to determine the connection destination for the agent:

- Polling based on system startup

  Used if the **Perform poll based on the system startup** check box is selected in **Basic Settings** in the agent configuration
- Regular polling (every 30 minutes by default)

- Polling at a specified time

  Used if the **Perform polling at the specified time** check box is selected in **Basic Settings** in the agent configuration.

To reset the connection destination you have set, perform either of the following operations, and then wait for polling to be performed or restart the OS:

- Change the IP address of the managed computer.
- Edit or overwrite the file for connection destinations.

  You can re-distribute the file for connection destinations in which the connection destination information is changed to agents, or directly edit and overwrite the file for connection destinations stored in the *installation-folder*\MASTER\DB of each agent. Then, restart the computer to apply the change to the connection destination.

If you move a managed computer and change its IP address, all you have to do to change the connection destination to an appropriate higher system is to wait for polling to be performed or restart the OS. End users need not be aware of changes to connection destinations.

If connection destinations of agents are automatically set or changed based on the file for connection destinations, log data for each agent is collected in the *installation-folder*\LOG\USER.LOG file. For details about logs relating to automatic changes to connection destinations, see the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

Tip

If multiple IP addresses are specified for an agent, the agent connects to a higher-level system by using the IP address that has the highest priority defined by the operating system. If the connection succeeds, that system is set as the connection destination of the agent.

Relationship between automatic changes to connection destinations and other functions

Automatic changes to connection destinations by using the file for connection destinations might not be possible in conjunction with other JP1/IT Desktop Management 2 functions. Note the following:

- If the file for connection destinations exists under *JP1/IT-Desktop-Management-2-Agent-installation-folder*¥MASTER¥DB¥ when you start managed computers, the agents are not connected to the management server or higher distribution system specified in the agent configuration. Instead, they are connected to a higher system (management server or relay system) based on the connection destination information specified in the file for connection destinations.
- If both the file for connection destinations (itdmhost.conf) and the information file for higher connection destinations (dmhost.txt) exist in *JP1/IT-Desktop-Management-2-Agent-installation-folder*¥MASTER¥DB¥ on a managed computer, the information file for higher connection destinations (dmhost.txt) is ignored.
- Even when the function that enables switching from one higher distribution system to another is enabled and the connection destination of a higher system is in fact switched, the following information and setting remain unchanged: information inside the file for connection destinations (itdmhost.conf), information inside the information file for higher connection destinations (dmhost.txt), and the **Higher Systems to Be Polled** setting specified in **Settings to Perform Polling for Multiple Higher Systems** under **Communication Settings** in the agent configuration.

To disable the connection destination settings in the file for connection destinations, perform one of the operations listed below. In any case, an agent that does not contain an information file for higher connection destinations will be connected to the connection destination specified in the agent configuration. An agent that contains an information file for higher connection destinations will be connected to the connection destination specified in that file.

- Distribute an empty file for connection destinations to the agents.
- Delete the file for connection destinations from *installation-folder*¥MASTER¥DB¥ on every agent.
- Rename the file for connection destinations in *installation-folder*¥MASTER¥DB¥ on every agent to a name other than `itdmhost.conf`.

To also disable the connection destination in the information file for higher connection destinations, perform one of the above operations with the information file for higher connection destinations rather than the file for connection destinations.

Depending on the combination of whether the file for connection destinations(itdmhost.conf) exists/notand the setting of **Perform a switchover of the higher system for distribution if polling fails for a specified period of time**, whether the switching is performed/not and the switching destination are as follows.

File for connection destinations exists/not	The setting of **Perform a switchover of the higher system for distribution if polling fails for a specified period of time**	
	Disable	Enable
File for connection destinations not exist	Polling switchover: not performed Higher system for distribution switchover: not performed	Polling switchover: not performed Higher system for distribution switchover: performed (follows Agent settings)
File for connection destinations exists	Polling switchover: performed (follows itdmhost.conf) Higher system for distribution switchover: not performed	Polling switchover: performed (follows itdmhost.conf) Higher system for distribution switchover: performed (follows itdmhost.conf)

(2) Creating the file for connection destinations (itdmhost.conf)

The file for connection destinations is a text file named `itdmhost.conf`. The following describes how to create it.

Format of the file for connection destinations

In the file for connection destinations, define the IP address ranges of managed computers and the corresponding connection destinations. You can define one combination per line. Separate items by using commas (`,`). A line beginning with a semicolon (`;`) is handled as a comment. Note that the last line cannot end with a line break. In addition, use UTF-8 for the character code of the file.

The following shows the format of the file for connection destinations.

```
[ITDM]
minimum-IP-address,maximum-IP-address,connection-destination
minimum-IP-address,maximum-IP-address,connection-destination
 :
[DM]
minimum-IP-address,maximum-IP-address,connection-destination,connection-type
 [,multicast-distribution-address]
minimum-IP-address,maximum-IP-address,connection-destination,connection-type
 [,multicast-distribution-address]
 :
```

The following table lists and describes the items in the file for connection destinations.

Section	Item	Description	Value that can be entered	Required?
ITDM	Specify the management server to which the agent is connected.			Required
	Minimum IP address	Specify the minimum IP address in the range of the IP addresses of managed computers.	Single-byte numbers in *xxx.xxx.xxx.xxx* format	Required
	Maximum IP address	Specify the maximum IP address in the range of the IP addresses of managed computers.	Single-byte numbers in *xxx.xxx.xxx.xxx* format	Required
	Connection destination	Specify the host name or IP address#1 of the connection-destination management server.	For a host name, a maximum of 255 single-byte alphanumeric characters For an IP address, single-byte numbers in *xxx.xxx.xxx.xxx* format	Required
DM	Specify a higher system for distribution that uses Remote Install Manager.			Required
	Minimum IP address	Specify the minimum IP address in the range of the IP addresses of managed computers.	Single-byte numbers in *xxx.xxx.xxx.xxx* format	Required
	Maximum IP address	Specify the maximum IP address in the range of the IP addresses of managed computers.	Single-byte numbers in *xxx.xxx.xxx.xxx* format	Required
	Connection destination#2	Specify the host name or IP address#1 of the higher system used as the connection destination for distribution that uses Remote Install Manager.	For a host name, a maximum of 64 single-byte alphanumeric characters For an IP address, single-byte numbers in *xxx.xxx.xxx.xxx* format	Required
	Connection type#2	If the connection destination is a management server, specify `netmdm`. If the connection destination is a relay system, specify `netmdmw`.		Required
	Multicast distribution address	To distribute jobs to managed computers by multicasting, specify the multicast address set for the connection destination.	Single-byte numbers in *xxx.xxx.xxx.xxx* format (in the range from 224.0.1.0 to 239.255.255.255)	Optional

#1: Specify the host name or IP address in accordance with the value of the operation key specified for **Address Resolution Method** during setup of the management server.

#2: You can specify a maximum of eight sets of connection destinations and connection types per line. If multiple connection destinations and connection types are specified, connection destinations that are specified earlier have higher priority.

The following shows the notes for the file for connection destinations.

- If an IP address of a managed computer is outside the defined range, its connection destination is not changed.
- If the same range of IP addresses of managed computers is defined more than once, the line that is defined first takes effect.
- If the same section is defined more than once, the section that is defined first takes effect.
- If there are no sections, the defined lines are ignored.
- The definition on a specified line is invalidated in the following cases:
  - A required item is omitted.

- An invalid IP address is specified.
- The value specified for *connection-destination* exceeds the maximum number of characters that can be entered.
- A value other than `netmdm` or `netmdmw` is specified for *connection-type*.
- The line contains only a line break.

- If you do not specify *multicast-distribution-address* or specify an invalid value, you cannot set the multicast address. However, the combinations of IP address ranges and connection destinations specified for items other than *multicast-distribution-address* are still valid.
- Any specification of an item other than the items that can be specified for a line is ignored.
- Any text following a semicolon is handled as a comment, and is ignored during processing.
- Single-byte spaces at the beginning or end of an item are ignored.

Sample file for connection destinations

The following is a sample file for connection destinations.

```
;Connection destination settings
[ITDM]
172.17.12.1,172.17.12.250,manager01
172.17.13.1,172.17.13.250,manager02
0.0.0.0,255.255.255.254,manager04
[DM]
172.17.12.1,172.17.12.250,dmsub01,netmdmw,dmsub02,netmdmw,dmman01,netmdm
172.17.13.1,172.17.13.250,dmman01,netmdm,dmman02,netmdm
0.0.0.0,255.255.255.254,dmman02,netmdm
```

In this example, if the IP address of the managed computer is `172.17.13.6`, the connection-destination management server is a host whose name is `manager02`. The higher system for distribution that uses Remote Install Manager is a management server whose name is `dmman01` or `dmman02`.

In the file for connection destinations, you can define 0.0.0.0 to 255.255.255.254 (all IP addresses) on the last line of each section to indicate a connection destination that is to be used if no appropriate IP address is found. In this example, for computers with IP addresses outside the range from 172.17.12.1 to 172.17.12.250 and from 172.17.13.1 to 172.17.13.250, the connection-destination management server is `manager04`. For these computers, the connection-destination higher system for distribution that uses Remote Install Manager is `dmman02`. If you specify multiple connection destinations, the connection destination that is defined first has higher priority. In this example, `dmsub01` and `dmman01` has the highest priority.

Tip

After creating the file for connection destinations, you can check whether the file conforms to the required file format by using the `checkitdmhost` command. For details about the `checkitdmhost` command, see 8.13 checkitdmhost (checking the format of the file for connection destinations).

Note after distribution of the file for connection destinations

Before you change the IP address of the connection destination host that is set by distributing the file for connection destinations to managed computers, delete that file from the relevant managed computers. If the file is not deleted, changing the IP address of the connection destination host might automatically change the connection destination. As a result, a connection destination different from the expected higher system might be set.

1.7 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**

1.7.1 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.

1.7.2 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.

1.7.3 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:

- 1.7.4 Checking the latest discovery status
- 1.7.5 Checking the discovered devices
- 1.7.6 Checking the managed devices
- 1.7.7 Checking the excluded devices

1.7.4 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.

1.7.5 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:

- 1.7.6 Checking the managed devices
- 1.7.7 Checking the excluded devices

1.7.6 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:

- 1.7.7 Checking the excluded devices

1.7.7 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:

- 1.7.6 Checking the managed devices

1.7.8 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.

1.8 Building the environment of a relay system

1.8.1 Installing a relay system

There are two ways to install a relay system. Use the method that is appropriate for your environment.

Installation using supplied media

This method involves installing the relay system program on the target computer, specifying the required settings as you go. After installation, you need to perform the setup process. We recommend this method if you need to set different values during the installation and setup of individual relay systems.

Installation using an installation set

First, you need to create the installation set for the relay system. You can then use this installation set to install the relay system on the target computer. To distribute the installation set you created to the relay system, you can place it on a Web server or file server, write it to CD-R or USB memory, or attach it to an email. The values specified in the agent configuration are used during installation and setup.

Unless you need to specify special settings, we recommend that you use the installation method that uses an installation set.

Tip

You can find out whether the relay system program is installed by viewing the **Device List** view in the Inventory module.

Related Topics:

- 1.8.2 Procedure for installing a relay system from supplied media
- 1.6.1 Creating an installation set
- 1.6.3 Uploading an agent to a Web server
- 1.6.4 Uploading an agent to a file server
- 1.6.5 Distributing the agent installation media (CD-R or USB memory) to users
- 1.6.6 Distributing agents to users as a file attached to an email

1.8.2 Procedure for installing a relay system from supplied media

To install the relay system, you need to log on to the OS on the computer as a user with administrator permissions.

Important

When installing the software on a Windows computer that uses User Account Control (UAC), a dialog box might appear prompting you to elevate your permission level. In this case, give your permission to continue.

Important

Do not shut down the operating system during installation. If you shut down the operating system while installation is in progress, the program might not operate correctly even if you install it again.

Important

On a computer that runs Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, or Windows Server 2012, do not specify the following folders during installation:

- Folders under *system-drive*`:\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

Important

When creating the agent environment, make sure that the directories defined in the TEMP and TMP user environment variable and system environment variable exist on the computer.

Important

Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

Tip

You cannot install the relay system program on a management server.

To install a relay system from supplied media:

1. Place the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box, select **JP1/IT Desktop Management 2 - Agent**, and then click the **Install** button.
3. In the dialog box indicating that installation will start, click the **Next** button.
4. In the **Installation type** dialog box, select **Custom installation**, and then click the **Next** button.
5. In the **Installation folder** dialog box, specify the folder in which to install the program and then click the **Next** button.

   Tip

   The default installation folder for a relay system is `C:\Program Files\HITACHI\jp1itdma`. If the OS is 64-bit Windows, the software is installed under the folder defined in the `%ProgramFiles(x86)%` environment variable. For example, if the OS is installed on the `C:` drive, the installation folder will be `C:\Program Files (x86)\Hitachi\jp1itdma\`.

Important

If the OS is 64-bit Windows, do not install the software in a folder under `%windir%\system32`.

Important

The SYSTEM and Administrators groups must have full control of the installation folder. For these groups, the **This folder, subfolders and files** option must be selected for **Apply To**.

6. In the **Types of components to be installed** dialog box, select **Relay system** and then click the **Next** button.
7. In the **Components to be installed** dialog box, select the component and subcomponents you want to install, and the installation method you want to use. Then, click the **Next** button.

Tip

The remote control agent is installed as a subcomponent of the relay system.

You can select the installation method from the pull-down menu displayed by clicking the icon to the left of the label.

8. In the dialog box indicating that the preparation for the installation is complete, click the **Install** button.
   The installation process begins. If you identify a problem in a setting, click the **Back** button and correct the setting.
9. When the installation process has finished, click the **Complete** button.

Installation of the relay system is complete, and the setup dialog box appears. Restart the computer if requested to do so.

Tip

By default, when you install JP1/IT Desktop Management 2 - Agent, the remote control agent is also installed. The remote control agent must be installed on the computer you want to remotely control.

1.8.3 Procedure for setting up a relay system

When you install a relay system from supplied media, you must set up the system so it can connect to the management server.

When you set up a relay system, you must log on to the OS as a user with administrator permissions.

Tip

If you install the agent by distributing an installation set or by deploying the agent software from the management server, the connection destinations are set automatically. You do not need to set them yourself.

You can also use an information file for higher connection destinations (`dmhost.txt`) to set connection destinations. If this file is in the JP1/IT Desktop Management 2 - Manager data folder when you create the installation set, it is incorporated into the installation set and distributed to the agents. When there is an

information file for higher connection destinations on the agent, the connection destination specified in the file has priority over the connection destination specified under **Basic Settings** in the agent configuration. For details about the information file for higher connection destinations, see the description of changing agent connection destinations in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

To set up the relay system:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Administrator Tool**, and then **Setup**.

   If the agent configuration is password-protected, a dialog box appears in which you can enter the password. Enter the password set for the agent configuration. The default password is `manager`.

2. On the **Connection-destination settings** tab of the **Setup (Relay system)** dialog box, specify the host name or IP address of the connection-destination management server and the port number, and then click the **OK** button.

3. In an environment where a computer incorporates multiple network adapters with multiple LAN connections, you can assign an order of priority to the network connections used by JP1/IT Desktop Management 2. To do so, on the **Communication settings** tab of the **Setup (Relay system)** dialog box, click the **Settings for network adapters** button. In the dialog box that appears, specify the priority levels and whether to automatically update network adapter information, and then click the **OK** button.

4. In the confirmation dialog box, click the **OK** button.

When setup is complete, the relay system starts operation with the specified settings.

Tip

If the connection between the relay system and the management server already exists, you can set up the relay system from the operation window. To set up the relay system from the operation window, you can use agent configurations.

Important

Do not register a relay system using the same ID key. If you do so, the update of the key name of the relay system will not be correctly reflected on the route information in the system configuration. In this case, to update the system configuration information, execute a **Get system configuration information** job to the systems with the key names before and after the change.

1.9 Installing Remote Install Manager only

1.9.1 Procedure for installing Remote Install Manager only

To install Remote Install Manager, you need to log on to the OS on the computer as a user with Administrator permissions.

Important

When installing the software on a Windows computer that uses User Account Control (UAC), a dialog box might appear prompting you to elevate your permission level. In this case, give your permission to continue.

Important

Do not shut down the operating system during installation. If you shut down the operating system while installation is in progress, the program might not operate correctly even if you install it again.

Important

On a computer that runs Windows Server 2019, Windows Server 2016, Windows 10, Windows 8.1, Windows 8, or Windows Server 2012, do not specify the following folders during installation:

- Folders under *system-drive*:\program files\WindowsApps
- Folders in storage areas created by virtual provisioning

Important

Before installation, make sure that all Windows applications have been closed. If you perform installation without terminating Remote Install Manager, restart the OS regardless of whether installation was successful. If the service does not start or Remote Install Manager does not run when you restart the operating system, use the following procedure to install it again:

1. Close all Windows applications.
2. Perform an overwrite installation again.

Important

Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

To install Remote Install Manager:

1. Place the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box, select **JP1/IT Desktop Management 2 - Manager**, and then click the **Install** button.

3. In the dialog box indicating that installation will start, click the **Next** button.
4. Check the information displayed in the **License Agreement** dialog box, select **I accept the terms in the license agreement**, and then click the **Next** button.
5. In the **Installation type** dialog box, select **Custom installation**, and then click the **Next** button.
6. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.
7. In the **Installation folder** dialog box, specify the installation folder and then click the **Next** button.
8. In the **Custom installation** dialog box, select the options as follows and then click the **Next** button:
   - From the pull-down menu for Manager, select **This feature will not be available.**
   - From the pull-down menu for Remote Install Manager, select **This feature, and all subfeatures, will be installed on local hard drive.**
9. In the confirmation dialog box, make sure that all the settings are correct, and then click the **Install** button.
   The installation process starts. If you identify a problem in a setting, click the **Back** button and correct the setting.
10. When the installation process has finished, click the **Complete** button.

Installation of Remote Install Manager is complete. Restart the computer if requested to do so.

If you installed Remote Install Manager only, you can start using it immediately. To do so, start Remote Install Manager, specify the host name or IP address of the management server, and log in using your user account information for JP1/IT Desktop Management 2.

2 Building system configurations

This chapter describes how to build each system configuration.

If you want to build a system that uses Asset Console to manage assets, you also need to install JP1/IT Desktop Management 2 - Asset Console separately. For details about the procedure for installing and setting up JP1/IT Desktop Management 2 - Asset Console, see the *JP1/IT Desktop Management 2 - Asset Console Configuration and Administration Guide*.

2.1 Building offline management configuration systems

2.1.1 Overview of building an offline management configuration system

To build an offline management configuration system, you first need to build a minimal configuration system, and then install the offline management agent on a computer.

1. Build the minimal configuration system.
2. Create the offline management agent.
3. Install the agent on the computer you want to manage offline.

Building of the offline management configuration system is complete.

Related Topics:

- 1. Building Management Servers and Agents

2.2 Building agentless configuration systems

2.2.1 Overview of building an agentless configuration system

To build an agentless configuration system, first build a management server, and then, run discovery to include discovered devices as managed devices.

1. Build the management server.
2. In the operation window, run IP discovery to discover devices.
   If you want to manage all devices, you can use the discovery setting that automatically includes all discovered devices as managed devices. To do so, go to step 4.
3. Include discovered devices as managed devices.
4. Specify settings that will cause the device information to be updated regularly.

Building of the agentless configuration system is complete.

Tip

If you want to build a system in which some computers have the agent installed and some are agentless, build a minimal configuration system first, and then go to step 2.

Related Topics:

- 4.1.1 Specifying search conditions (discovery from IP address)
- 1.7.5 Checking the discovered devices
- 4.2.1 Regularly updating agentless device information

2.3 Building support service linkage configuration systems

2.3.1 Overview of building a support service linkage configuration system

To build a support service linkage configuration system, you first need to build a minimal configuration system. You can then specify the information needed to access the support service site.

1. Build a minimal configuration system.
2. In the operation window, set the information for accessing the support service site.

> **Tip**
>
> If you want to determine the status of security updates on managed computers or execute automated actions based on these statuses, you need to define a security policy. For details about how to use a security policy to manage security updates, see the *JP1/IT Desktop Management 2 Administration Guide*.

Building of the support service linkage configuration system is complete.

Related Topics:

- 4.3.1 Setting information for connecting to the support service

2.4 Building Active Directory linkage configuration systems

2.4.1 Overview of building an Active Directory linkage configuration system

To build an Active Directory linkage configuration system, connect to Active Directory and include the computers registered in Active Directory as managed devices.

1. Build a management server in a system in which Active Directory is installed.
2. Set the information for connecting JP1/IT Desktop Management 2 to Active Directory.
3. If necessary, specify settings so that information managed by Active Directory is obtained as an additional management item.
4. Discover the computers registered in Active Directory.
   If you want to include all devices as managed devices, you can use the discovery setting that automatically includes them as managed devices. Similarly, the agent can be distributed automatically during device discovery. Perform steps 5 and 6 as necessary.
5. Include discovered computers as managed devices.
6. Install an agent on the managed computers.

Building of the Active Directory linkage configuration system is complete.

Related Topics:

- 1.2 Creating a management server environment
- 4.4.1 Setting information for connecting to Active Directory
- 4.4.2 Setting the information acquired from Active Directory as an additional management item
- 4.4.3 Searching for devices registered in Active Directory

2.5 Building MDM linkage configuration systems

2.5.1 Overview of building a MDM linkage configuration system

To build an MDM linkage configuration system, you first need to build a minimal configuration system. You can then obtain information about smart devices from the MDM system.

1. Build the minimal configuration system.
2. Set the information for linking JP1/IT Desktop Management 2 with the MDM system.
3. Obtain information about the smart devices registered in the MDM system.

   To include all smart devices as managed devices, you can use the MDM linkage setting to automatically include the discovered smart devices as managed devices. Perform step 4 as necessary.
4. Include the discovered smart devices as managed devices.

Building of the MDM linkage configuration system is complete.

Related Topics:

- 4.5.1 Specifying settings to link with an MDM system

2.6 Building network monitoring configuration systems

2.6.1 Overview of building a network monitoring configuration system

To build a network monitoring configuration system, you first need to build a minimal configuration system. You can then enable network access control in each network segment.

1. Build the minimal configuration system.
2. In the operation window, run IP discovery to discover all devices in the organization.
3. In the network filter list, make sure the setting for whether to permit network access is correct.

   Tip

   If a device for which you want to reject access is found, set network access for the device to deny.

4. In the operation window, enable network access control for each network segment.

   In the dialog box that opens, select the network access control setting for permitting connection to the network.

Building of the network monitoring configuration system is complete.

Note that a system built by using this procedure can detect new devices that have connected to a network, but the devices cannot be disconnected automatically. If you want to disconnect newly connected devices, use the following setting after you have completed building the system.

Automatically blocking connection of devices that are newly connected to a network

Apply the network access control setting you specified to the desired network segment so that discovered devices will not be able to connect to the network. For details, see the description of general procedure for denying network access for unregistered devices in the manual *JP1/IT Desktop Management 2 Administration Guide*.

Tip

You can automatically block network connection of a device that has a security problem. To do so, use the network connection control setting that is listed as an action item in the security policy to control the network connection based on a security status judgment.

Important

On agents for UNIX or Mac, a network monitor is not enabled. In addition, with agents for UNIX, automatic control of network connections based on the security policy is not used. However, you can manually permit or block network connections. With agents for Mac, network connections can be automatically enabled or disabled based on a security status judgment.

Related Topics:

- 4.1.1 Specifying search conditions (discovery from IP address)
- 4.6.1 Editing devices in the network control list
- 2.6.2 Enabling the network monitor

- 4.6.3 Adding network monitor settings
- 4.6.4 Changing assignment of network monitor settings

2.6.2 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.

2.7 Building a configuration system that uses JP1 authentication

2.7.1 Building a configuration system that uses JP1 authentication

To build a configuration system that uses JP1 authentication, register JP1 users on the JP1/Base authentication server, and then set a JP1 resource group and JP1 permission level for each JP1 user. Next, install JP1/IT Desktop Management 2, and then set up JP1/Base user management in the **User Management Settings** view.

The procedure for configuring the system is described below. For details about the setup procedures to be performed on the authentication server, see the *JP1/Base User's Guide*.

1. In an environment where Windows firewall is enabled, specify the settings so that the JP1/Base authentication server can connect to the management server.

   Specify the settings on the authentication server so that port 20240 is used.

2. If the version of JP1/Base is 11-10, update the access permission level file of JP1/Base.

   Copy the file from the installation folder of JP1/IT Desktop Management 2, and then overwrite the access permission level file of JP1/Base with the copied file. After that, execute the `jbsaclreload` command on the JP1/Base authentication server to apply the update.

   Source of the file to be copied

   When the authentication server uses Windows:

   installation-folder-of-JP1/IT Desktop Management 2 - Manager\mgr\conf\JP1_AccessLevel.1110Windows

   When the authentication server uses UNIX:

   installation-folder-of-JP1/IT Desktop Management 2 - Manager\mgr\conf\JP1_AccessLevel.1110UNIX

   Destination of the file to be copied

   When the authentication server uses Windows:

   installation-folder-of-JP1/Base\conf\user_acl\JP1_AccessLevel

   When the authentication server uses UNIX:

   shared-folder\jp1base\conf\user_acl\JP1_AccessLevel

3. Check the user accounts to be used in JP1/IT Desktop Management 2, as well as the user ID, password, permissions, and task allocations of each user account.

   Important

   If you use JP1 authentication, you cannot set an administration scope.

   For details about the characters that can be used for user IDs and passwords, see the *JP1/Base User's Guide*.

   The following is an example of the check results:

Role	User ID	Password	Permissions	Task allocation
General system administrator	Account01	********	• system management authority • user account management authority	Entire system
System administrator A in the development department	Account02	********	system management authority	• Security management • Asset management • Device management

Role	User ID	Password	Permissions	Task allocation
System administrator B in the development department	Account03	********	system management authority	Device management

4. Determine the name of the JP1 resource group to be configured for the JP1 user account to be used in JP1/IT Desktop Management 2.

   Specify the JP1 resource group name in 1 to 64 bytes. You can use single-byte alphanumeric characters and the following symbols:

   exclamation mark (!), hash mark (#), dollar sign ($), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), hyphen (-), period (.), at mark (@), backslash (\), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), right curly bracket (}), and swung dash (~)

   Tip

   You can configure one resource group for each management server. In a multi-server configuration, you can specify different JP1 permission levels by setting different JP1 resource groups for individual management servers.

5. Register JP1 users on the authentication server, and then specify user IDs and passwords.

6. On the authentication server, set a JP1 resource group and JP1 permission level for each JP1 user.

   For the JP1 permission level, assign permissions and task allocations according to the check results. For details about the correspondence between JP1 permission levels, and the permissions and task allocations in JP1/IT Desktop Management 2, see 2.7.4 Correspondence between JP1 permission levels, and the permissions and division of work responsibilities in JP1/IT Desktop Management 2.

7. Install JP1/IT Desktop Management 2 - Manager.

8. Set up JP1/IT Desktop Management 2 - Manager. In the **User Management Settings** window, select **Manage users by using JP1/Base**, and then specify a JP1 resource group.

   Important

   To run JP1/IT Desktop Management 2 in a cluster system, you must specify the same logical host name when configuring the JP1/Base cluster environment and when configuring JP1/IT Desktop Management 2 - Manager.

2.7.2 Overview of switching from ITDM2 authentication to JP1 authentication

To change a configuration system that uses ITDM2 authentication to one that uses JP1 authentication, on the JP1/Base authentication server, register as JP1 users the ITDM2 user accounts that were being used. Next, set a JP1 resource group and JP1 permission level for each JP1 user, change the setup information of JP1/IT Desktop Management 2, and then set up JP1/Base user management. If necessary, in the **Account Management** view of the Settings module, add recipients to whom notification emails are to be sent.

The procedure for changing the authentication method is described below. For details about the setup procedures to be performed on the authentication server, see the *JP1/Base User's Guide*.

Important

If you use JP1 authentication, you cannot set an administration scope. If you want to set an administration scope, use ITDM2 authentication.

1. In an environment where Windows firewall is enabled, specify the settings so that the JP1/Base authentication server can connect to the management server.

   Specify the settings on the authentication server so that port 20240 is used.

2. If the version of JP1/Base is 11-10, update the access permission level file of JP1/Base.

   Copy the file from the installation folder of JP1/IT Desktop Management 2, and then overwrite the access permission level file of JP1/Base with the copied file. After that, execute the `jbsaclreload` command on the JP1/Base authentication server to apply the update.

   Source of the file to be copied

   When the authentication server uses Windows:

   installation-folder-of-JP1/IT Desktop Management 2 - Manager\mgr\conf\JP1_AccessLevel.1110Windows

   When the authentication server uses UNIX:

   installation-folder-of-JP1/IT Desktop Management 2 - Manager \mgr\conf\JP1_AccessLevel.1110UNIX

   Destination of the file to be copied

   When the authentication server uses Windows:

   installation-folder-of-JP1/Base\conf\user_acl\JP1_AccessLevel

   When the authentication server uses UNIX:

   shared-folder-\jp1base\conf\user_acl\JP1_AccessLevel

3. Determine the name of the JP1 resource group to be configured for each JP1 user account to be used in JP1/IT Desktop Management 2.

   Specify the JP1 resource group name in 1 to 64 bytes. You can use single-byte alphanumeric characters and the following symbols:

   exclamation mark (!), hash mark (#), dollar sign ($), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), hyphen (-), period (.), at mark (@), backslash (\), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), right curly bracket (}), and swung dash (~)

   Tip

   You can configure one resource group for each management server. In a multi-server configuration, you can specify different JP1 permission levels by setting different JP1 resource groups for individual management servers.

4. On the JP1/Base authentication server, register as JP1 users the ITDM2 user accounts that were being used.

   Important

   If a user ID or password uses characters that are not supported by JP1/Base, you will need to change the user ID or password. For details about the characters you can use in JP1/Base, see the *JP1/Base User's Guide*.

5. On the authentication server, set a JP1 resource group and JP1 permission level for each JP1 user.

   For the JP1 permission level, assign permissions and task allocations based on the assigned permissions and task allocations in JP1/IT Desktop Management 2. For details about the correspondence between JP1 permission levels,

and the permissions and task allocations in JP1/IT Desktop Management 2, see 2.7.4 Correspondence between JP1 permission levels, and the permissions and division of work responsibilities in JP1/IT Desktop Management 2.

6. Set up JP1/IT Desktop Management 2 - Manager. In the **User Management Settings** window, select **Manage users by using JP1/Base**, and then specify a JP1 resource group.

> **Important**
>
> To run JP1/IT Desktop Management 2 in a cluster system, you must specify the same logical host name when configuring the JP1/Base cluster environment and when configuring JP1/IT Desktop Management 2 - Manager.

7. To set a JP1 user as a recipient of notification emails (such as those for events and reports), add the email address of the JP1 user to the list of email notification destinations in the **Account Management** view of the Settings module.

2.7.3 Overview of switching from JP1 authentication to ITDM2 authentication

To change a configuration system that uses JP1 authentication to one that uses ITDM2 authentication, in the **Account Management** view of the Settings module, register as ITDM2 users the JP1 user accounts that were being used. Next, change the setup information of JP1/IT Desktop Management 2, and then clear the setting for managing users by using JP1/Base.

The procedure for changing the authentication method is as follows.

1. In the **Account Management** view of the Settings module, add as ITDM2 users the JP1 user accounts that were being used.

2. Change the setup information of JP1/IT Desktop Management 2 - Manager. In the **User Management Settings** window, clear the **Manage users by using JP1/Base** setting.

2.7.4 Correspondence between JP1 permission levels, and the permissions and division of work responsibilities in JP1/IT Desktop Management 2

The correspondence between JP1 permission levels, and the permissions and division of work responsibilities in JP1/IT Desktop Management 2 are as follows.

No.	Type	Permission or division of work responsibilitiy	Operation permission name of the JP1 permission level
1	Common	A permission level that includes the system management authority, user management permission, and permissions for all division of work responsibilities. This permission level has the same permissions as those of the JP1/IT Desktop Management 2 built-in account.	JP1_ITDM_Admin
2	Permission[#1]	System management authority	JP1_ITDM_SystemAdmin
3		User account management authority	JP1_ITDM_UserManage

No.	Type	Permission or division of work responsibilitiy	Operation permission name of the JP1 permission level
4	Permission[#1]	Reference authority	JP1_ITDM_Reference
5		API authority	JP1_ITDM_API_Admin
6	Division of work responsibility[#2]	Security management and distribution management	JP1_ITDM_Security
7		Asset management	JP1_ITDM_Assets
8		Device management	JP1_ITDM_Inventory
9		Distribution management	JP1_ITDM_Distribution
10		System configuration management[#3]	JP1_ITDM_Settings

#1

If multiple permissions including the reference authority are specified for the same JP1 resource group, permissions other than the reference authority and API authority are given higher priority.

Furthermore, if multiple permissions including the API authority are specified for the same JP1 resource group, the API authority is ignored.

#2

If an operation permission for a division of work responsibilitiy is specified, even if the reference authority is not specified, the reference authority of the applicable division of work responsibilitiy will be automatically assigned.

#3

If you specify system configuration management, you will also need to specify the system management authority. If you specify system configuration management but not the system administration permission, system configuration cannot be performed.

Note that operations are restricted depending on the combination of permissions and division of work responsibilities that are specified. For details, see the descriptions about the scope of operations for permissions of user accounts and for the division of work responsibilities of user accounts in the *JP1/IT Desktop Management 2 Overview and the System Design Guide*.

2.8 Building JP1/NETM/NM - Manager linkage configuration systems

2.8.1 Overview of building a JP1/NETM/NM - Manager linkage configuration system

To build a system that links with JP1/NETM/NM - Manager, you first need to build a minimal configuration system. You can then deploy network control appliances. Next, install JP1/NETM/NM - Manager, and enable linkage with JP1/NETM/NM - Manager.

1. Build a minimal configuration system.
2. Deploy and set up a network control appliance in each monitored network segment.
3. Install JP1/NETM/NM - Manager on the management server.
4. Set up JP1/NETM/NM - Manager.
   To run JP1/IT Desktop Management 2 in a cluster system, also run JP1/NETM/NM - Manager in a cluster system by installing JP1/NETM/NM - Manager on the same secondary server.
5. Register network segments and groups to be monitored in JP1/NETM/NM - Manager.
6. Specify the environment settings of network control appliances in JP1/NETM/NM - Manager.
7. Set quarantine communication information (settings for quarantine-exempt connections) on the network control appliances.
8. In the Settings module of JP1/IT Desktop Management 2, click **Network Access Control** to display the **Assign Network Access Control Settings** view. Then, for the network segments to be monitored that were registered in JP1/NETM/NM - Manager, change the settings so that notification is not sent when the segments are not monitored.
   If you use the blacklist method to manage network connections, skip step 9. Perform step 9 only if you use the whitelist method to manage network connections.
9. Edit the network control settings file (`jdn_networkcontrol.conf`) stored on the management server. For details about this procedure, see 4.6.6 Procedure for editing the network control settings file.
10. In JP1/IT Desktop Management 2, enable linkage with JP1/NETM/NM - Manager.
    For details about this procedure, see 4.6.5 Enabling the JP1/NETM/NM - Manager linkage settings.

Building of the JP1/NETM/NM - Manager linkage configuration system is complete.

> **Important**
>
> When linking with JP1/NETM/NM - Manager, a list of access-permitted devices and a list of access-denied devices for network control appliance will be replaced by the content of the network control list of JP1/IT Desktop Management 2 - Manager. For this reason, if you have registered a list of access-permitted devices and a list of access-denied devices for network control appliance before linking with JP1/IT Desktop Management 2 - Manager, the content will be lost. When the content is different between the network control list and the list of access-permitted devices and list of access-denied devices for network control appliance that were already registered before linking with JP1/IT Desktop Management 2 - Manager, register them to the network control list first and then link with JP1/NETM/NM - Manager if necessary.

Important

When linking with JP1/NETM/NM - Manager, register the following server in the quarantine communication information on the network control appliances. Also even when the device is disconnected from the network, maintain the communication with the server.

- Management server

Related Topics:

- 1.1.1 Overview of building a minimal configuration system

2.8.2 Overview of building a NX NetMonitor/Manager linkage configuration system

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

2.9 Building JP1/IM linkage configuration systems

2.9.1 Overview of building a JP1/IM linkage configuration system

To build a JP1/IM linkage configuration system, first build a management server. Then install JP1/IM and specify the necessary settings.

1. Build a management server.
2. Install JP1/Base on the management server.
3. Set properties in the configuration file.
4. Install JP1/IM - Manager and JP1/IM - View.
5. Copy the definition file for extended event attributes to the specified JP1/IM folder.

   Source file of the definition file for extended event attributes

   JP1/IT Desktop Management 2-installation-folder`\mgr\definition\hitachi_jp1_itdm_attr_ja.conf`

   JP1/IT Desktop Management 2-installation-folder`\mgr\definition\hitachi_jp1_itdm_attr_en.conf`

   JP1/IT Desktop Management 2-installation-folder`\mgr\definition\hitachi_jp1_itdm_attr_zh.conf`

   Destination folder of the definition file for extended event attributes

   JP1/IM-Manager-console-path`\conf\console\attribute`

   The default JP1/IM - Manager console path is as follows:

   system-drive`:\Program Files\HITACHI\JP1Cons`
6. Restart JP1/IM - Manager.

   The settings for the definition file for extended event attributes take effect when JP1/IM - Manager is restarted.
7. Specify connection settings for JP1/Base and JP1/IM.
8. Restart JP1/IT Desktop Management 2 and JP1/Base.

   Building of the JP1/IM linkage configuration system is complete. When an event requiring notification occurs, it is reported to JP1/IM.

For details about the JP1/Base installation procedure and settings, see the *JP1/Base User's Guide*. For details about the JP1/IM installation procedure and settings, see the *JP1/Integrated Management - Manager Configuration Guide*. For details about the location and format of the definition file for extended event attributes, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Important

If JP1/IM and JP1/Base are not connected, error messages or events requiring notification are not reported to JP1/IM during system operation. When building a JP1/IM linkage system, check the connection status of JP1/IM and JP1/Base.

Related Topics:

- 4.7.1 Procedure for setting the configuration file used for linkage with JP1/IM

2.10 Building a cluster system

2.10.1 Overview of building a cluster system

When building a cluster system, start by building a management server.

To build a cluster system:

1. Install JP1/IT Desktop Management 2 - Manager .
   Select custom installation as the installation type. When the installation has finished, do not continue by performing setup.
2. Create a resource group on the primary server.
3. Set up the primary server.
4. Copy the file that is output when the primary server setup finishes to the standby server.
5. To perform setup on the standby server, move the owner of the resource group you created in step 2 to the standby server.
6. Set up the standby server.
7. To start using the cluster system, move the owner of the resource group you created in step 2 to the primary server.
8. Bring the service resources that are a part of JP1/IT Desktop Management 2 online.
   Bring the service resources (generic services) other than `JP1_ITDM2_Service` and `JP1_ITDM2_Agent Control` that are registered in a management server group online by using Windows Server Failover Cluster.
9. In the operation window, register the license.
10. Bring the JP1/IT Desktop Management 2 services online.
    Bring `JP1_ITDM2_Service` and `JP1_ITDM2_Agent Control` online.

Building of the cluster system is complete.

Related Topics:

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 2.10.2 Procedure for creating a resource group on the primary server
- 2.10.3 Setting up JP1/IT Desktop Management 2 on the primary server
- 2.10.4 Setting up JP1/IT Desktop Management 2 on the standby server
- 1.3.1 Registering a product license

2.10.2 Procedure for creating a resource group on the primary server

After JP1/IT Desktop Management 2 has been installed, use Windows Server Failover Cluster to create a JP1/IT Desktop Management 2 group and register resources. To register resources:

1. Create a management server group.
   Create a new empty role for the management server.

2. Register the resources that are necessary for the group you created.
   The following table lists the resources you need to register in the group:

Resource type	Resource name
Resources other than JP1/IT Desktop Management 2 service resources	Client access point[#1]
	Storage (shared disk)
JP1/IT Desktop Management 2 service resources (generic services)	JP1_ITDM2_DB Service
	JP1_ITDM2_DB Cluster Service
	JP1_ITDM2_Web Container
	JP1_ITDM2_Web Server[#2]
	JP1_ITDM2_Service
	JP1_ITDM2_Agent Control
	JP1_ITDM2_Relay Manager Service[#3]

   #1: For the network name, specify the logical host name used in JP1/IT Desktop Management 2. For the IP address, specify the logical IP address used in JP1/IT Desktop Management 2.

   #2: If the OS is Windows Server 2019, Windows Server 2016 or Windows Server 2012, you must create resources from the CLI.

   Start PowerShell from the command prompt as a user with administrator permissions, and then execute the following command:

   ```
   Get-ClusterResource "name-of-JP1_ITDM2_Web Server-service-resource" | Set-
   ClusterParameter -Name StartupParameters -value ""
   ```

   #3: Only perform in the case of the primary management server with multi-server configuration.

3. Set the primary server as the priority server.

4. Bring the resources other than JP1/IT Desktop Management 2 service resources online.
   The JP1/IT Desktop Management 2 service resources (generic services) remain offline.

The setting items and the setting values for each resource are as follows.

Settings for resources other than JP1/IT Desktop Management 2 service resources

Resource name	Setting item	Setting value
• Client access point • Storage (shared disk)	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)

JP1_ITDM2_DB Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_DB Service	Name	Specify a name.
	Type	Generic Service

Resource name	Setting item	Setting value
JP1_ITDM2_DB Service	Service name	Set HiRDBEmbeddedEdition_JE1.
	Dependency	Set the network name resource and the shared disk (physical disk) resource.
	Period for restarts (mm:ss)	00:00 (fixed)
	Maximum restarts in the specified period	0 (fixed)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owners	Set both the primary and standby servers.
	Registry Replication	Not specified.

JP1_ITDM2_DB Cluster Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_DB Cluster Service	Name	Specify a name.
	Type	Generic Service
	Service name	Set HiRDBClusterService_JE1.
	Dependency	Set a resource for JP1_ITDM2_DB Service.
	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owners	Set both the primary and standby servers.
	Registry Replication	Not specified.

JP1_ITDM2_Web Container settings

Resource name	Setting item	Setting value
JP1_ITDM2_Web Container	Name	Specify a name.
	Type	Generic Service
	Service name	Set JP1_DTNAVI_WEBCON.
	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owner	Set both the primary and standby servers.
	Registry Replication	Not specified.

JP1_ITDM2_Web Server settings

Resource name	Setting item	Setting value
JP1_ITDM2_Web Server	Name	Specify a name.
	Type	Generic Service
	Service name	Set JP1_DTNAVI_WEBSVR.
	Dependency	Set the network name resource.
	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owner	Set both the primary and standby servers.
	Registry Replication	Not specified.

JP1_ITDM2_Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_Service	Name	Specify a name.
	Type	Generic Service
	Service name	Set JP1_DTNAVI_MGRSRV.
	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owner	Set both the primary and standby servers.
	Registry Replication	Not specified.

JP1_ITDM2_Agent Control settings

Resource name	Setting item	Setting value
JP1_ITDM2_Agent Control	Name	Specify a name.
	Type	Set a generic service.
	Service name	Set JP1_DTNAVI_AGCTRL.
	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owner	Set both the primary and standby servers.

Resource name	Setting item	Setting value
JP1_ITDM2_Agent Control	Registry Replication	Not specified.

JP1_ITDM2_Relay Manager Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_Relay Manager Service	Name	Specify a name.
	Type	Set a generic service.
	Service name	Set the JP1_DTNAVI_RLYMGRSRV Service resource.
	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Period for restarts (mm:ss)	15:00 (recommended)
	Maximum restarts in the specified period	1 (recommended)
	Pending timeout (mm:ss)	05:00 (recommended)
	Possible owner	Set both the primary and standby servers.
	Registry Replication	Not specified.

2.10.3 Setting up JP1/IT Desktop Management 2 on the primary server

This subsection describes the setup views that require settings that are needed to run cluster systems.

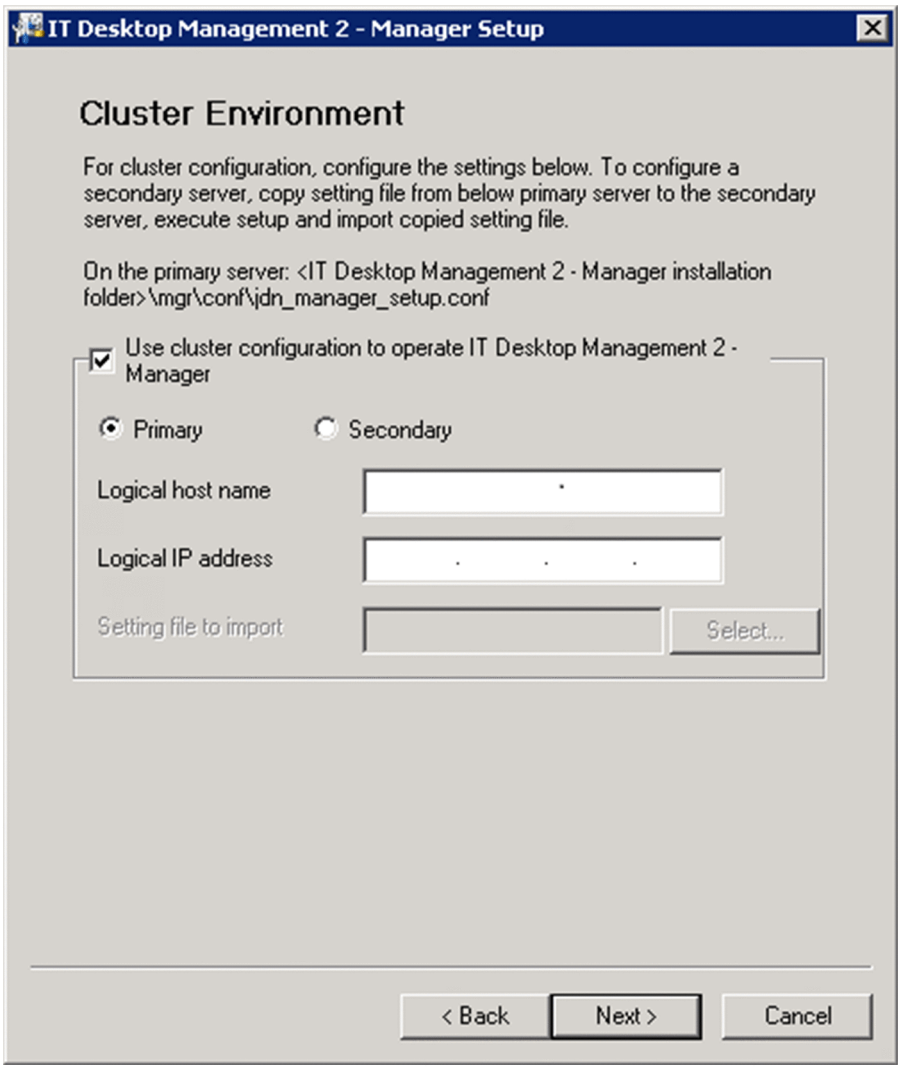
Important

If the OS is Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders:

- Folders under *system-drive*:`\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

Settings in the Cluster Environment view

In the **Cluster Environment** view for setup, specify the settings needed to run a cluster system. The following figures show the **Cluster Environment** view.



Do the following:

- Select **Use cluster configuration to operate IT Desktop Management 2 - Manager**.
- Select **Primary**.
- Set **Logical host name** and **Logical IP address**.

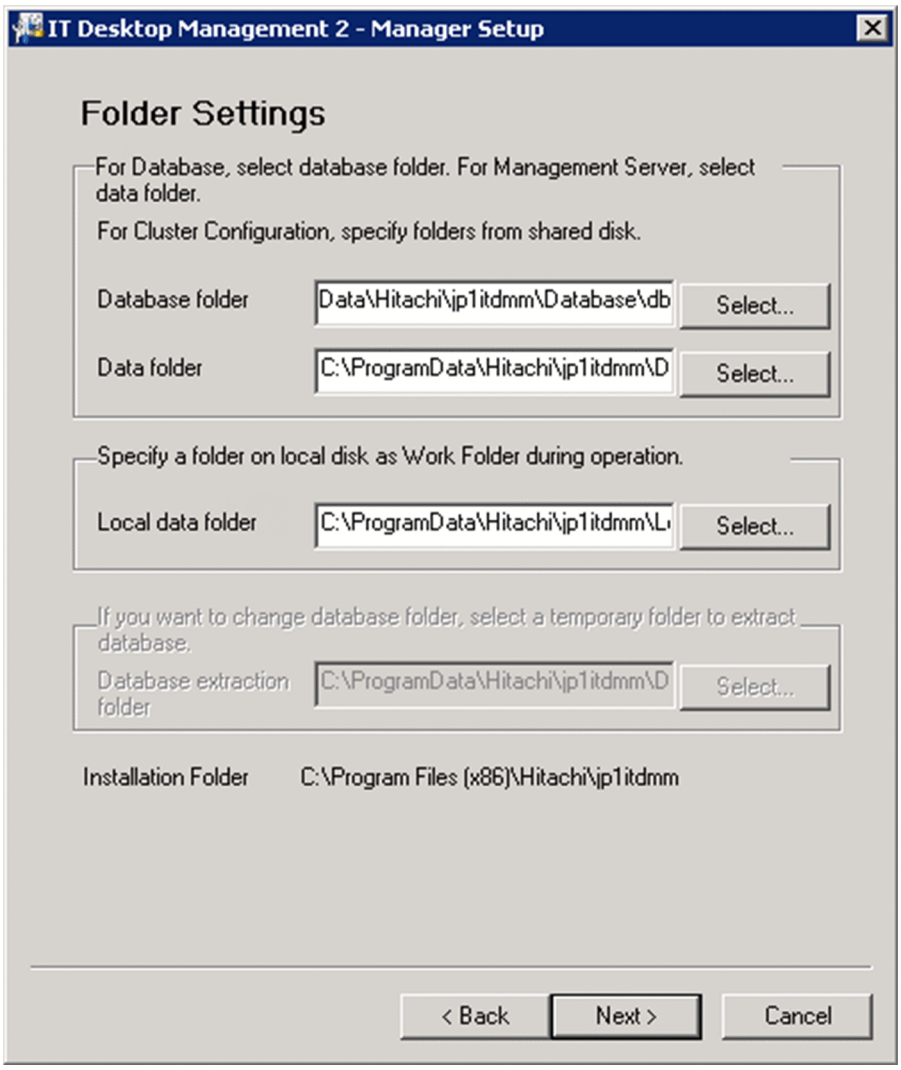
For this operation, you do not need to set **Setting file to import**.

When setup finishes the following, file is output. Copy this file to the standby server.

JP1/IT Desktop Management 2-installation-folder`\mgr\conf\jdn_manager_setup.conf`

Settings in the Folder Settings view

In the **Folder Settings** view for setup, specify the settings needed to run a cluster system. The following figure shows the **Folder Settings** view.



Enter the path to the shared disk in the following items:

- **Database folder**
- **Data folder**

In the following views, enter the path to the shared disk in following items:

- **Operation log database folder** (when acquiring operation log data) and **Operation log backup folder** (when specifying a folder on a local disk as the folder for storing operation log data) in the **Operation Log Settings** view
- **Output folder for the revision history** in the **Output Settings for Saving the Revision History** view (when specifying a folder on the local disk as the folder for storing revision histories)

For other items, use the normal setup procedure.

Related Topics:

- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration

2.10.4 Setting up JP1/IT Desktop Management 2 on the standby server

Perform setup on the standby server as you did on the primary server.

This subsection describes the Setup window that require settings that are needed to run a cluster system.

In the **Cluster Environment** view for setup, do the following:

- Select **Use cluster configuration to operate IT Desktop Management 2 - Manager**.
- Select **Secondary**.
- Specify the file you copied during setting of the primary server in **Setting file to import**.

The settings in the **Folder Settings** view are the same as the normal setup settings . Note, however, that if you set up a standby server, you cannot specify the following items because they are not available:

- **Database folder**
- **Data folder**
- **Database extraction folder**

Also, you do not need to register the agent on the standby server.

Related Topics:

- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration

2.11 Building an environment for managing the devices used outside the company

2.11.1 Building an Internet gateway

To build an Internet gateway, first build a management server. Then install Microsoft Internet Information Services and an Internet gateway. You can build an Internet gateway as follows.

Important

The Internet gateway does not support a cluster system.

Important

Only install this product on a local disk. Do not install this product on network connection disks (NFS, NAS, and others).

How to build an Internet gateway

You can build an Internet gateway by following the steps described below. Perform steps 1 to 5 on the Internet gateway server, step 6 on the firewall at the boundaries between the Internet and the DMZ and between the DMZ and the internal network, and steps 7 and 8 on managed computers.

1. Install an agent or a relay system. If you want to use distribution by using Remote Installation Manager, install a relay system.

   In that case, change the number of concurrent connections to the relay system from 50 to 100. Change the setting value of **Relay System Settings - Processing Settings for the Relay System - Number of JP1/IT Desktop Management 2 - Agents that can Be Connected to the Relay System Concurrently** in the Agent Configuration.

2. Install Microsoft Internet Information Services.

3. Install an Internet gateway.

4. Set up the installed Internet gateway.

5. Specify the Microsoft Internet Information Services settings.

6. Specify the firewall setting.

7. Install an agent for Internet connection on the computers to be managed by JP1/IT Desktop Management 2.

8. Confirm that managed computers have successfully established a communication with the Internet gateway.

Related Topics:

- 2.11.1 Building an Internet gateway
- (1) Installing Microsoft Internet Information Services
- (2) Installing an Internet gateway
- (3) Setting up the Internet gateway
- (4) Setting up Microsoft Internet Information Services

- 2.11.2 Setting up firewalls
- 2.11.3 Building an agent for devices used outside the company

(1) Installing Microsoft Internet Information Services

Install Microsoft Internet Information Services on the Internet gateway server. Add information regarding the roles of `Web Server (IIS)` described in the following table:

Item		Role service
Web Server	Common HTTP Features	HTTP Errors
		Directory Browse
		Default Document
		Static Content
	Security	Basic Authentication
	Application Development	ISAPI Extensions
Management Tools		IIS Management Console

(2) Installing an Internet gateway

To install an Internet gateway, you have to log on to the OS as a user having administrator permissions.

Important

If you install an Internet gateway on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the user permission level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the program might not operate correctly even if you install it again later.

Important

Before installing an Internet gateway, shut down all Windows applications.

Important

Do not specify a folder in which other products (including JP1/IT Desktop Management 2) are installed as the folder in which to install the Internet gateway.

To install an Internet gateway:

1. Insert the media supplied with the product in the CD/DVD drive.

2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Internet Gateway**, and then click the **Install** button.
3. In the dialog box indicating the start of installation, click the **Next** button.
4. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.
5. In the confirmation dialog box for the installation, click the **Install** button.
   Installation starts.
6. When the installation finishes, click the **Completed** button.

Installation of an Internet gateway is complete. If a message asking you to restart the computer appears, restart it.

(3) Setting up the Internet gateway

If you install JP1/IT Desktop Management 2 - Internet Gateway, you must perform setup as soon as installation is complete.

To set up the Internet gateway:

1. If the World Wide Web Publishing Service is up and running, stop it.
2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Internet Gateway**, and then **Internet Gateway Setup**.
3. In the **IT Desktop Management 2 - Internet Gateway Setup** dialog box, set a higher system for the Internet gateway#.
4. Click the **OK** button.

#:

Using Remote Install Manager for distribution

Install a relay system to the Internet gateway server, and specify **Relay system** to **Higher system for distribution that uses Remote Install Manager** and `localhost` to **Host name or IP address**.

Not using Remote Install Manager for distribution

Specify **Management server** to **Higher system for distribution that uses Remote Install Manager** and the host name or the IP address of the management server to **Host name or IP address**.

(4) Setting up Microsoft Internet Information Services

You have to first set up the Internet gateway before you can set up Microsoft Internet Information Services. For details about how to set up Microsoft Internet Information Services, see the Microsoft Internet Information Services manual.

To set up Microsoft Internet Information Services:

1. Set ISAPI restrictions.
2. Set a server certificate.
3. Add and set an application.
4. Set permissions for folders.

5. Start the World Wide Web Publishing Service.

To set ISAPI restrictions:

Under ISAPI and CGI Restrictions on the Internet gateway server, add the following settings:

ISAPI or CGI path	Allow extension path to execute
Internet-gateway-installation-folder\igw\web\itdm\jdngwsvr.dll	Select the check box.
Internet-gateway-installation-folder\igw\web\dm\jdngwsvr_dm.dll	Select the check box.

To set a server certificate:

By using **Server Certificate** of the Internet gateway server, complete server certificate request.

Server certificate certified by a certification authority that can complete server certificate request

Path to the file containing the server certificate certified by the certification authority[#]

#: Do not store the server certificate file in the folder in which the Internet gateway has been installed.

Friendly name

Any

To add and set an application:

Add the following configuration in Microsoft Internet Information Services:

Item in Microsoft Internet Information Services	Setting	Description	
Sites	Name	Default Web Site	
	Site Bindings[#1]	• Type: https • IP address: All Unassigned • Port: 443[#2] • Host name: FQDN of the Internet gateway server • Require Server Name Indication: Select this check box. • SSL certificate: Specify the friendly name you have set by following the steps described under *To set a server certificate:* in this section.	
	Enabled Protocols	https	
	Authentication	• Basic Authentication: Enabled[#3] • Anonymous Authentication: Disabled	
Applications	Alias	jp1itdmigw1	jp1itdmigw2
	Application Pools	AppPooljp1itdmigw1	AppPooljp1itdmigw2
	Physical path	*Internet-gateway-installation-folder*\igw\web\itdm	*Internet-gateway-installation-folder*\igw\web\dm
	Enabled Protocols	https	
	Edit Feature Permissions under Handler Mappings	Execute: Selected	
	HTTP Response Header	• Name: X-Content-Type-Options Value: nosniff	

Item in Microsoft Internet Information Services	Setting	Description	
Applications	HTTP Response Header	• Name: `X-XSS-Protection` Value: `1; mode=block` • Name: `Content-Security-Policy` Value: `frame-ancestors 'none'`	
Application Pools	Name under General	AppPooljp1itdmigw1	AppPooljp1itdmigw2
	Enable 32-Bit Applications under General	True	
	Idle Time-out Action under Process Model	• Windows Server 2012 (IIS 8.0): No setting • Windows Server 2012 R2 (IIS 8.5) or later: Suspend	
	Regular Time Interval (minutes) under Recycling	0	

#1: Delete the line showing the default settings (Type: http, Port: 80).

#2: Specify this setting for the following in **Internet Connection Settings** - **Internet Gateway** - **Port Number** in the Agent Configurations view.

#3: Enable or disable this option as necessary. Furthermore, specify this setting for the following in the Agent Configurations view: **Internet Gateway Communication Settings**.

To set permissions for folders:

For the following folders, grant the Modify permissions to the authentication user[#]:

- *Internet-gateway-installation-folder*\log
- *Internet-gateway-installation-folder*\igw\Web\work

This refers to the user specified by **User ID** of **Internet Gateway Communication Settings** in the Agent Configurations view. If no user ID is specified (if Anonymous Authentication is to be used to authenticate the site), `IUSR` is the authentication user.

2.11.2 Setting up firewalls

Firewall between the Internet gateway and the Internet

Configure the firewall between the Internet gateway and the Internet to allow inbound communication from the Internet to the DMZ so that data can pass through 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**).

Firewall between the Internet gateway and the management server or Remote Installation Manager

Configure the firewall between the Internet gateway and the management server or Remote Installation Manager to allow inbound communication from the DMZ to the internal network so that data can pass through the port used for communication with the management server and Remote Installation Manager. For details, see A.1 Port number list.

2.11.3 Building an agent for devices used outside the company

To manage computers used outside the company with JP1/IT Desktop Management 2, you have to install an agent on the computers so that they can connect to a higher system via the Internet gateway.

For details about how to install an agent on a managed computer, see 1.6.2 Installing agents on computers.

For details about how to set up an agent, see 1.6.10 Procedure for setting up the agent.

For details about how to set up an agent to allow computers to connect to a higher system via the Internet gateway, see the description of managing devices used outside the company in the manual *JP1/IT Desktop Management 2 Administration Guide*.

To perform a connection check:

After setting up an agent, check if a connection is established with the Internet gateway. To perform a connection check, refer to the agent log file.

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
```

If `SUCCESS` is output as *connection-result* and `200` is output as *HTTP-response-code*, it means that the agent has successfully established a connection with the Internet gateway. If any other information is output, see the description of troubleshooting problems with the Internet gateway in the manual *JP1/IT Desktop Management 2 Administration Guide* to find out the possible causes of the error and corrective action.

3 Changing settings

This chapter describes how to change the settings you specified during setup of a management server.

3.1 Procedure for changing the setting for connection to the database

You can change the password used to access JP1/IT Desktop Management 2, and the address used to connect to the database.

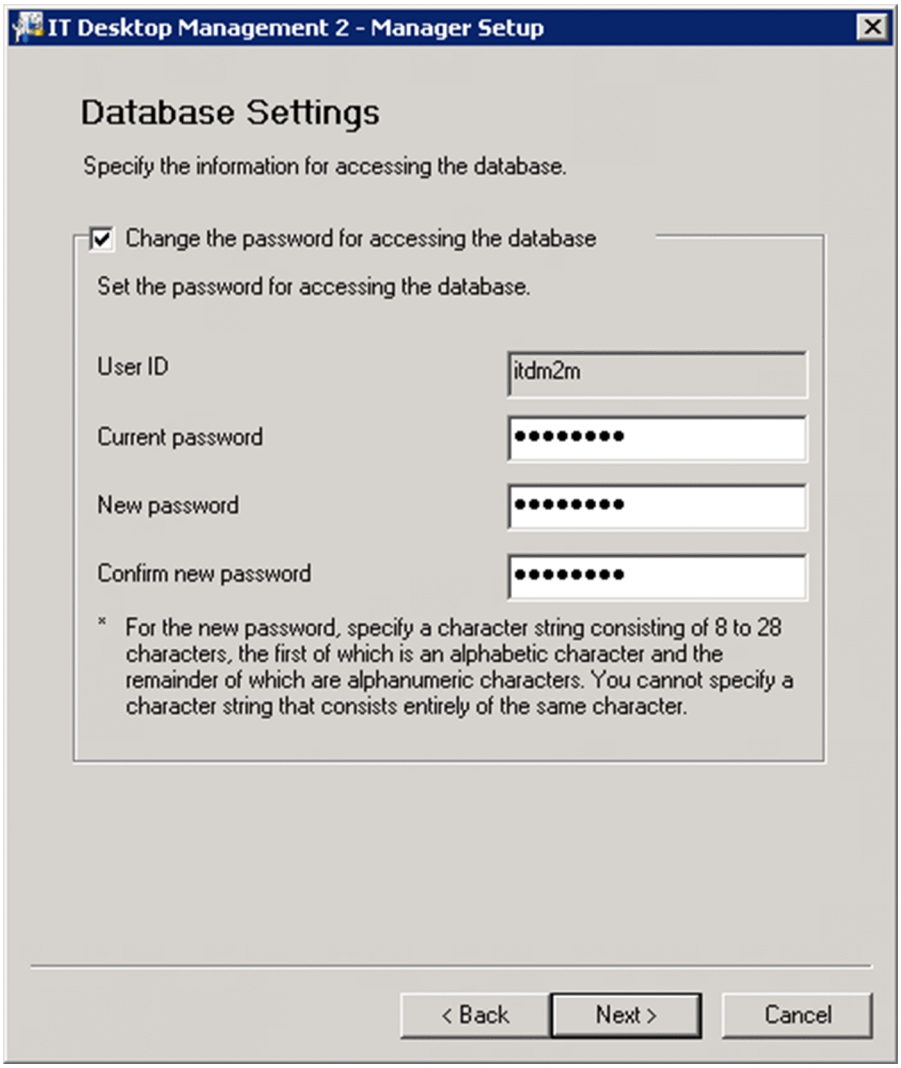
To set the password for accessing the database:

1. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.

2. In the Setup view, click the **Next** button.

3. In the **Select a Setup** view, select **Settings Modification** and then click the **Next** button.

4. In the **Database Settings** (change password) view, select the **Change the password for accessing the database** check box, enter the current and new passwords, and then click the **Next** button.



5. Review the settings in the **Confirm Setup Settings** view, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

6. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

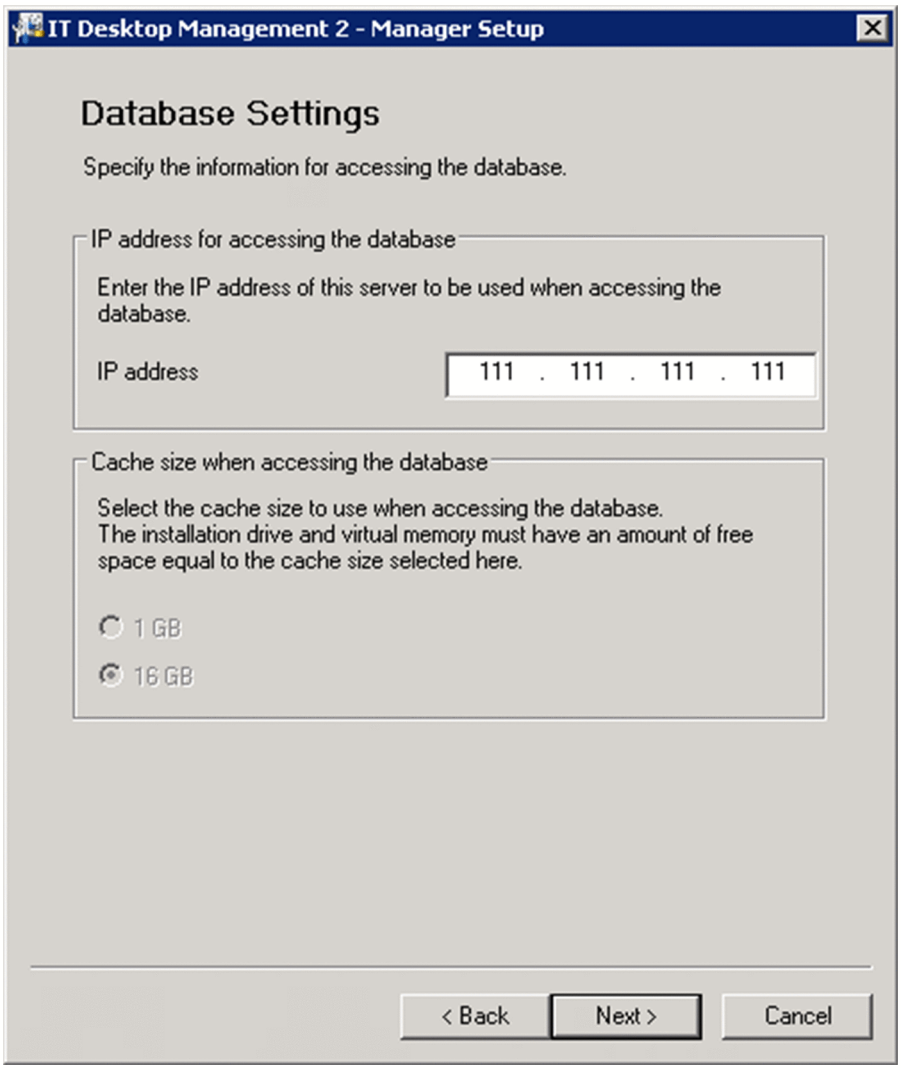
The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.

7. In the **Setup Complete** view, click the **OK** button.

The password used to access the JP1/IT Desktop Management 2 database is changed.

To change the database connection address:

1. On the management server, execute the `stopservice` command to stop the service.
2. On the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. In the **Database Settings** (change password) view, click the **Next** button without changing the password.
6. In the **Cluster Environment** view, select the setting indicating that a cluster configuration is not being used, and then click the **Next** button.
7. In the **Database Settings** (IP address and cache settings) view, change the IP address used to access the database on the management server, and then click the **Next** button.



8. Continue to click the **Next** button until the **Confirm Setup Settings** view opens.

9. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button.

10. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

    The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.

11. In the **Setup Complete** view, click the **OK** button.

    The stopped service will be started automatically after setup is completed.

The database connection address for JP1/IT Desktop Management 2 is changed.

To modify the cache size to use when accessing the database:

In the **Setup** view, the value of the cache size to use when accessing the database specified in the initial setup cannot be modified. Follow the steps below to modify it.

1. Back up the database.

Use Database Manager to back up the database. Leave at least 20 gigabytes of free space on the drive containing the backup folder.

2. Uninstall JP1/IT Desktop Management 2 - Manager.

   For details about how to uninstall JP1/IT Desktop Management 2 - Manager, see 6.2 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager.

3. Install JP1/IT Desktop Management 2 - Manager.

   For details about how to install JP1/IT Desktop Management 2 - Manager, see 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration).

4. Specify the cache size in the **Setup** view.

   For details about the cache size settings, see 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration.

5. Restore the database by using the data that you backed up in step 1.

   On the replacement-destination computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Start the database manager of JP1/IT Desktop Management 2 - Manager, and restore the database.

3.2 Procedure for changing the folders that are used

You can change the folders you use on a management server. If disk space for the database is insufficient, change the folder for the database to a folder on a disk that has enough space.

Important

On a computer running Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012, do not specify the following folders during setup:

- Folders under *system-drive*`:\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

To change folders:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Folder Settings** view opens.
6. Change a folder as needed.
7. Continue to click the **Next** button until the **Confirm Setup Settings** view opens.
8. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.

The database folder for a database is deleted from the old folder, and is created in the new folder. The data other than the operation logs in the database in the old folder is passed to the new folder, but the old data for operation logs is deleted. Perform manual acquisition of operation log data as needed.

The data in the data folder is moved to the new folder.

When you change the operation log backup folder, the original folder and its contents remain in the system. Log data collected from that point onward is stored in the new folder. If you want all operation log data to be stored in one folder, transfer the data from the old folder to the new folder.

When you change the database folder for operation logs, the existing data is deleted. Perform manual import of operation log data as needed.

3.3 Procedure for configuring operation log acquisition

This is a management server setup item.

You can log user operations in a log. Operation logs enable you to keep track of files that enter or leave the system, and to identify computers on which suspicious operations have been performed.

Note that you can obtain operation logs on computers that are managed online (agents for Windows).

Tip

You must set whether to record operation logs during setup and in the security policy. To record operation logs, in addition to this setting, enable the setting for recording operation logs in the security policy. You can also set the types of operation logs you want to record in the security policy.

Important

If you set that operation logs are not to be recorded during management server setup, the operation logs for a computer are not saved even when you enable the setting for recording operation logs in the security policy.

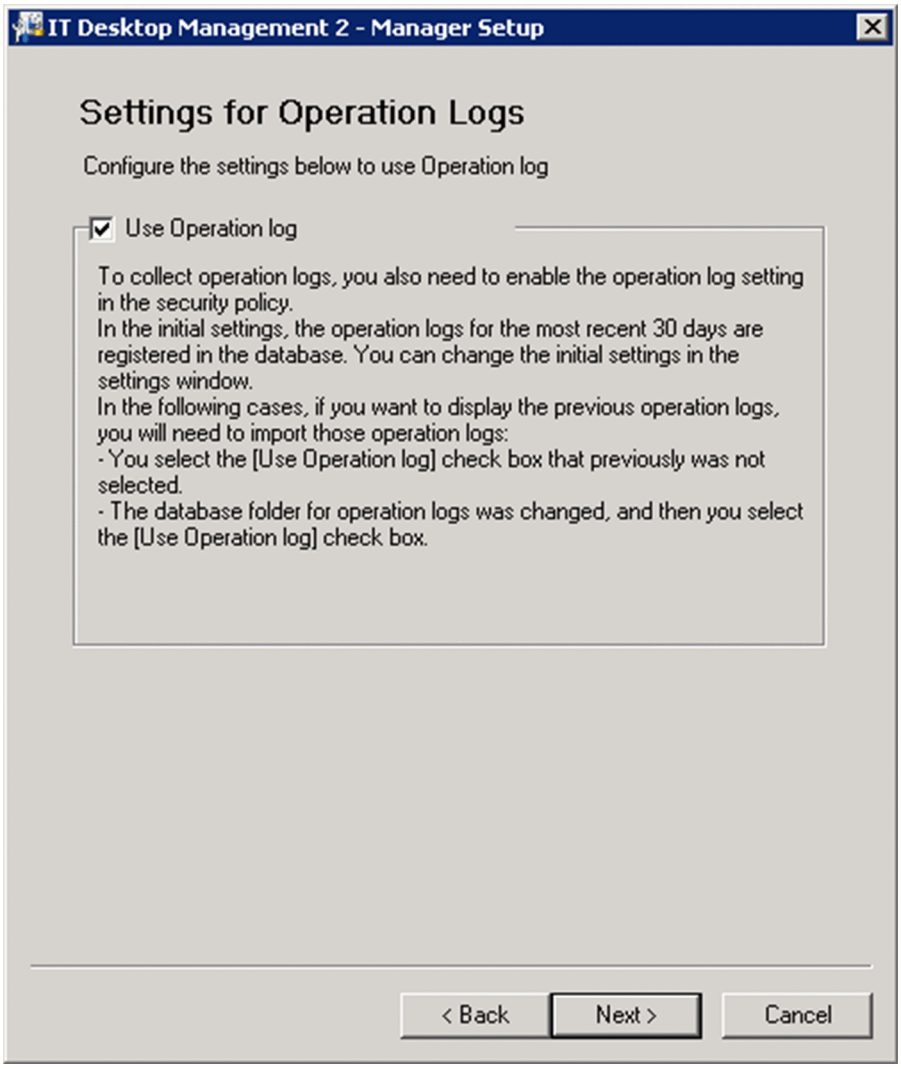
Important

On a computer running Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012, do not specify the following folders during setup:

- Folders under *system-drive*:\program files\WindowsApps
- Folders in storage areas created by virtual provisioning

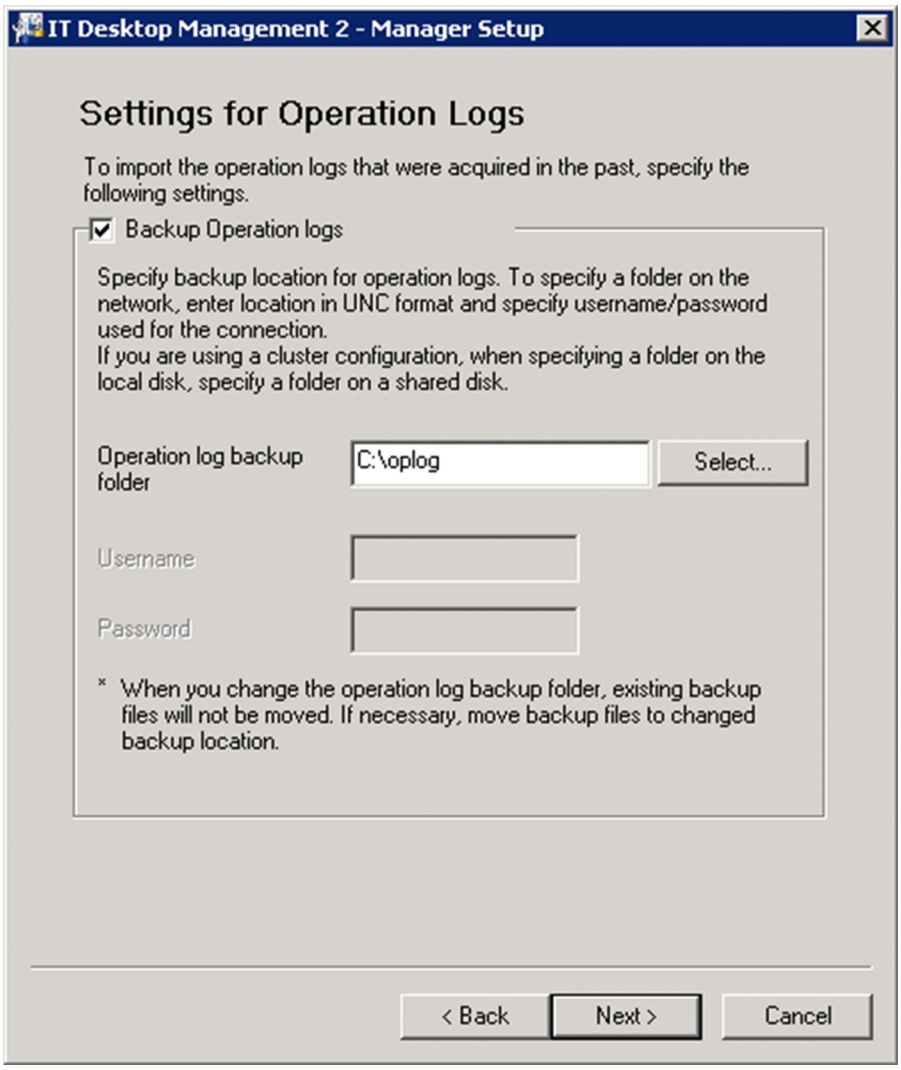
To specify settings for obtaining operation logs:

1. Log on to the OS as a user with administrator permissions.
2. On the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Operation Log Settings** view opens.



6. Select the **Use Operation log** check box, and then click the **Next** button.

7. If you intend to store operation log data, in the window that appears, select the **Store the operation logs** check box, and specify the storage folder in **Operation log backup folder**. You can also specify the user name and password for connecting to the storage folder as needed.



8. Click the **Next** button.

9. In the window that appears, set the following items:

   - **Total Managed Nodes**

     Specify the approximate number of computers for which you want to obtain operation logs.

   - **Maximum number of days for which the operation logs are to be stored in the database**

     Specify the number of days for which to store (Automatically and Manually) operation log data in the database. The default is 60 days. If you have configured the system to automatically acquire operation log data, by default, 30 days of user operation logs are stored in the folder specified in **Database folder for the operation logs**. You can change the length of time for which automatically acquired operation log data is stored in the **Operation Log Settings** area.

   - **Required capacity**

     This value is calculated automatically based on the values specified in **Total Managed Nodes** and **Maximum number of days for which operation logs are to be stored in the database**.

     The formula is as follows:

     Total Managed Nodes x **Maximum number of days for which operation logs are to be stored in the database** x 1.52 (Megabyte)

     If the result of the calculation is smaller than **Maximum number of days for which operation logs are to be stored in the database** x 1.5 (Gigabyte). The following formula is used:

Maximum number of days for which operation logs are to be stored in the database x 1.5 (Gigabyte)

The **Required Capacity** value is used as the default value of the Warning threshold and Error threshold for the free space of the operation log database folder.

The Warning threshold and Error threshold can be changed in the configuration file (`jdn_manager_config.conf`).

- **Operation log database**

  Specify the folder in which you want to create the database for saving the operation logs.

> **Tip**
>
> The **Maximum number of days for which operation logs are to be stored in the database** and **Required capacity** values are approximate. The number of days you can import operation logs and the disk capacity that is used vary according to the number of devices actually managed and the amount of logged information.

10. Click the **Next** button.
11. If you want to increase the database cache size to improve search performance for operation log data, specify the cache to add in the view that appears.

    We recommend approximately 1 GB for every 2,500 managed computers.
12. Click the **Next** button.
13. Continue to click the **Next** button until the **Confirm Setup Settings** view opens.
14. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.

    A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
15. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

    Setup starts, and a dialog box indicating the progress appears. When the setup finishes, the **Setup Complete** view opens.
16. In the **Setup Complete** view, click the **OK** button.

Operation logs are now available.

> **Important**
>
> If you want to change a setting related to operation logs after operation logs have been obtained, you cannot set a value smaller than the current value in **Total Managed Nodes** and **Maximum number of days for which the operation logs are to be stored in the database**.

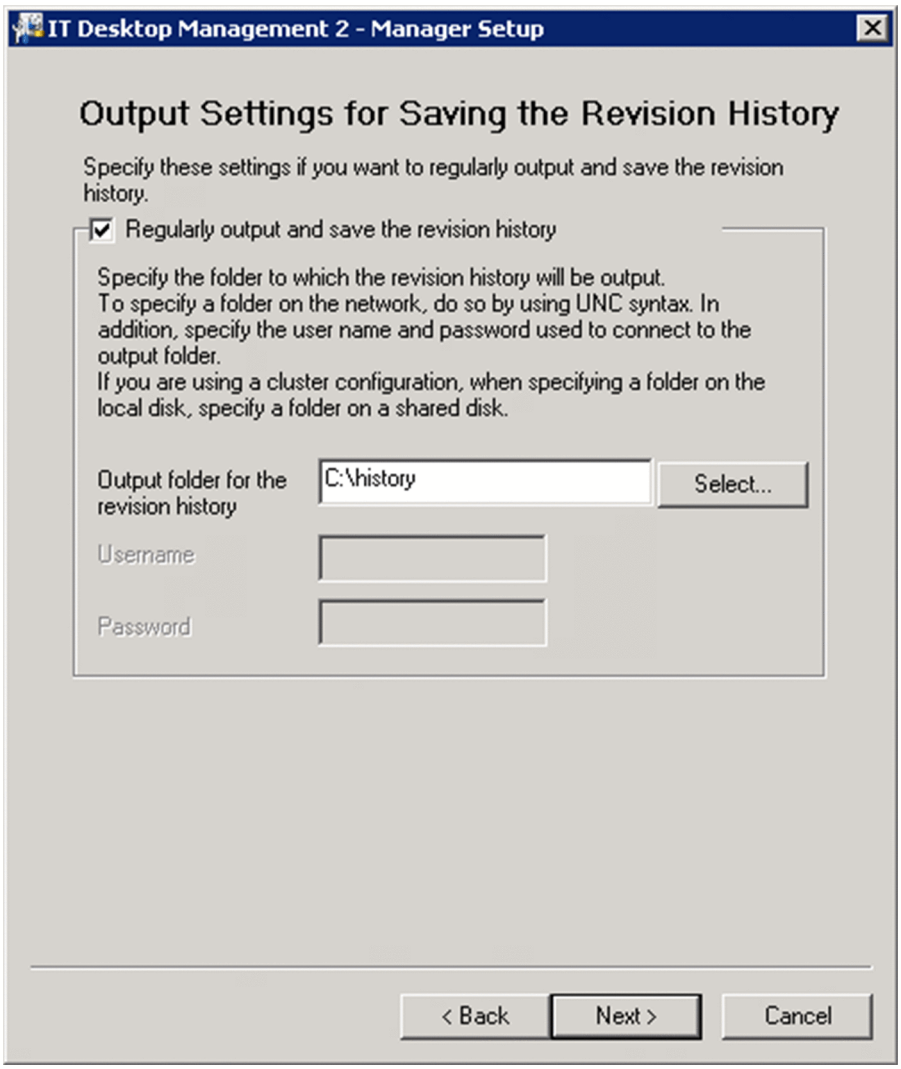
3.4 Procedure for setting up the output folder for the revision history

Perform the procedure described below on the management server.

If the output of revision history archive is enabled, revision history archive is periodically saved in a CSV file. If you output revision history archive, even if revision history entries exceed 600,000, the revision contents can be saved.

To enable the output of revision history archive:

1. Log on to the OS as a member of the Administrators group.
2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Click the **Next** button until the **Output Settings for Saving the Revision History** view appears.



6. Select the **Regularly output and save the revision history** check box, and specify a folder in **Output folder for the revision history**.

Important

On a computer that runs Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012, do not specify the following folders during setup:

- Folders under *system-drive*`:\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

7. Click the **Next** button until the **Confirm Setup Settings** view appears.
8. In the **Confirm Setup Settings** view, confirm that the specified settings are correct, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
9. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.
10. In the **Setup Complete** view, click the **OK** button.

A revision history archive is output periodically to a CSV file. Each entry in the CSV file consists of the following items:

Revision history item	Description
Date Modified	The time at which device information was changed is output. This time is the same as the device information update time. If device information is reported to the management server via external storage media, the time at which the device information was collected by a collection tool , or a tool for applying policy offline is output.
Item Modified	The device information item that was changed is output.
Before Change	The device information before the change is output.
After Change	The device information after the change is output.
Host Name When Change Occurred	The name of the host whose device information was changed is output. If the host name itself was changed, the new host name is output. This item identifies the device on which the change occurred.

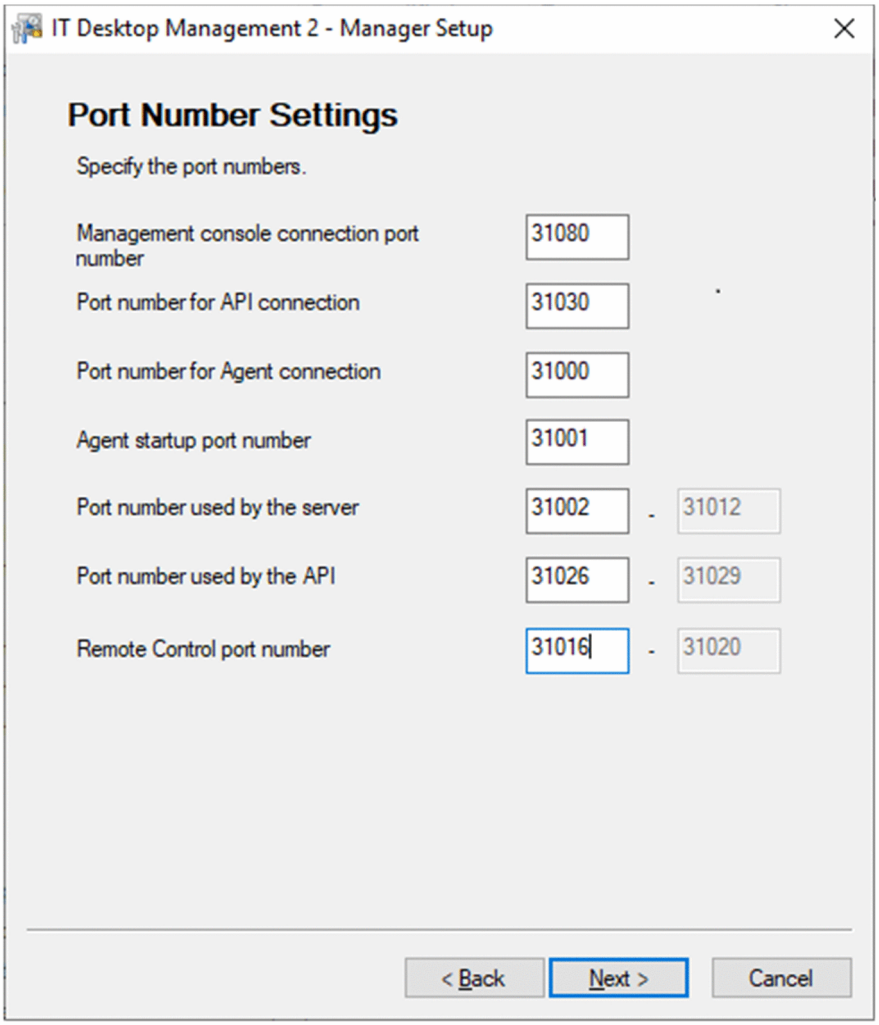
3.5 Procedure for changing a port number

You can change a port number that is used on a management server.

> **Important**
>
> If you change a port number during operation, the agent connection is lost. When you change a port number, do not forget to change the port number setting on the agent.

To change a port number:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Port Number Settings** view opens.



6. Change a port number as needed.

You can change the following settings:

Management console connection port number

On the computer on which JP1/IT Desktop Management 2 is used, enter the port number used to connect to the management server.

Port number for API connection

Enter the port number used for connecting to the management server from the external system via the API.

Port number for Agent connection

Enter the port number used to connect to the management server from the agent.

Agent startup port number

Enter the port number used for communication from the management server to the agent.

Port number used by the server

Enter the port number used by JP1/IT Desktop Management 2.

Port number used by the API

Enter the port number used by the management server when the API is used.

Remote Control port number

Enter the port number used by the remote control functionality.

Port number for multi-server configuration connections

In a multi-server configuration, enter the port number to be used by the management relay server.

For details about port numbers, see A.1 Port number list.

7. Continue to click the **Next** button until the **Confirm Setup Settings** view opens.
8. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
9. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.
10. In the **Setup Complete** view, click the **OK** button.

The port number is changed.

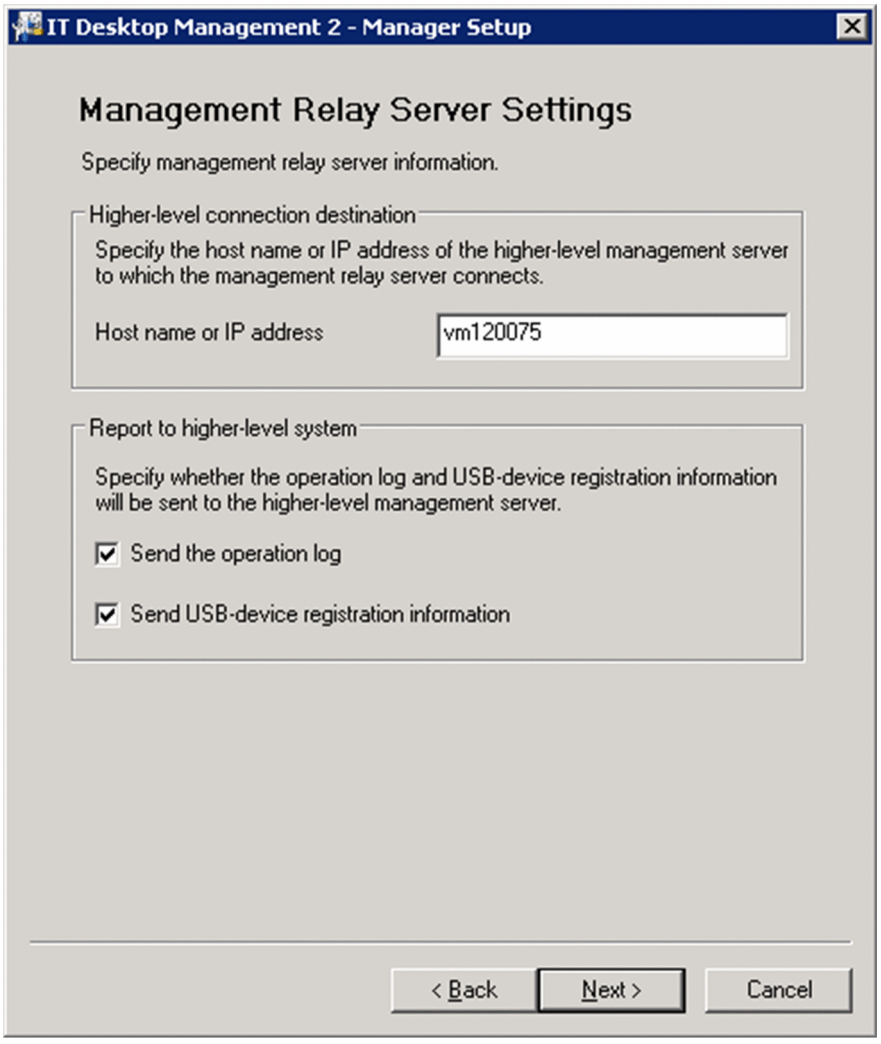
3.6 Procedure for changing the higher connection destination settings of a management relay server

The procedure described here is included in the setup of a management relay server.

You can change the higher connection destination settings of a management relay server.

To change the higher connection destination settings of a management relay server:

1. Log on 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 **Setup**.
3. In the setup window, click the **Next** button.
4. In the **Select a Setup** window, select **Modify settings**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Management Relay Server Settings** window appears.



6. In **Host name or IP address**, specify the connection-destination host name or IP address, and then click the **Next** button.

To specify this setting, use the ID key for operations selected in the **Settings for Address Resolution** window of the higher management server.

7. Continue to click the **Next** button until the **Confirm Setup Settings** window appears.

8. In the **Confirm Setup Settings** window, confirm the specified settings, and then click the **Next** button.
   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

9. In the **Setup for Distribution by Using Remote Install Manager** window, click the **OK** button.
   Setup starts, and a dialog box indicating that processing is in progress appears. When setup ends, the **Setup has Completed** window appears.

10. In the **Setup has Completed** window, click the **OK** button.

Now you have changed the higher connection destination settings of the management relay server.

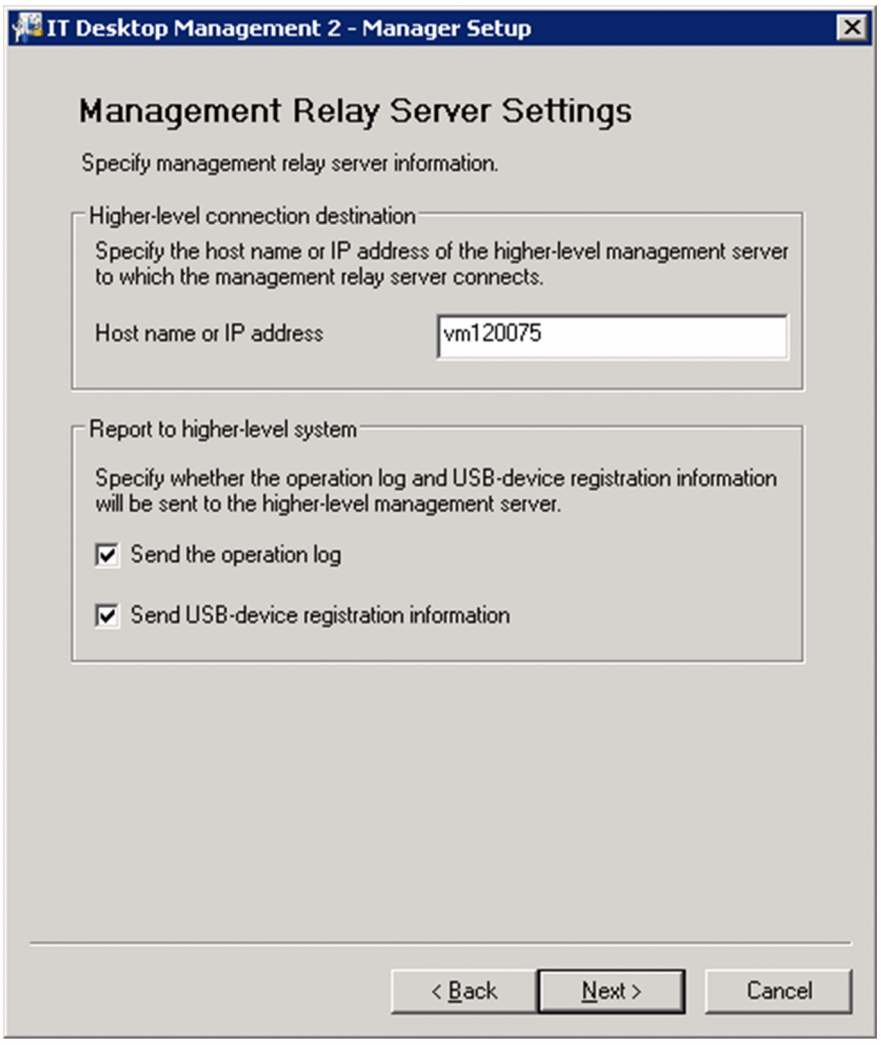
3.7 Procedure for changing the settings for reporting to a higher-level system of a management relay server

The procedure described here is included in the setup of a management relay server.

If reporting to the higher-level system is enabled on a management relay server, the operation log information and USB device registration information collected by the management relay server can be sent to the higher management server. The higher management server can centrally manage the information sent from the lower management relay servers, as well as the information about the directly connected subordinate devices.

To change the settings for reporting to the higher-level system:

1. Log on 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 **Setup**.
3. In the setup window, click the **Next** button.
4. In the **Select a Setup** window, select **Modify settings**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Management Relay Server Settings** window appears.



6. Optionally, change the following settings as necessary, and then click the **Next** button:
   - Send the operation log
     Select this option to send the collected operation log data to the higher management server.
   - Send USB-device registration information
     Select this option to send the collected USB-device registration information to the higher management server.

   > **Tip**
   >
   > To collect operation log data, on the management relay server that manages it, enable *Acquisition of Operation Logs* in the security policy.

7. Continue to click the **Next** button until the **Confirm Setup Settings** window appears.
8. In the **Confirm Setup Settings** window, confirm the specified settings, and then click the **Next** button.
   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console are not being used is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
9. In the **Setup for Distribution by Using Remote Install Manager** window, click the **OK** button.
   Setup starts, and a dialog box indicating that processing is in progress appears. When setup ends, the **Setup has Completed** window appears.
10. In the **Setup has Completed** window, click the **OK** button.

Now you have changed the settings for reporting to the higher-level system of the management relay server.

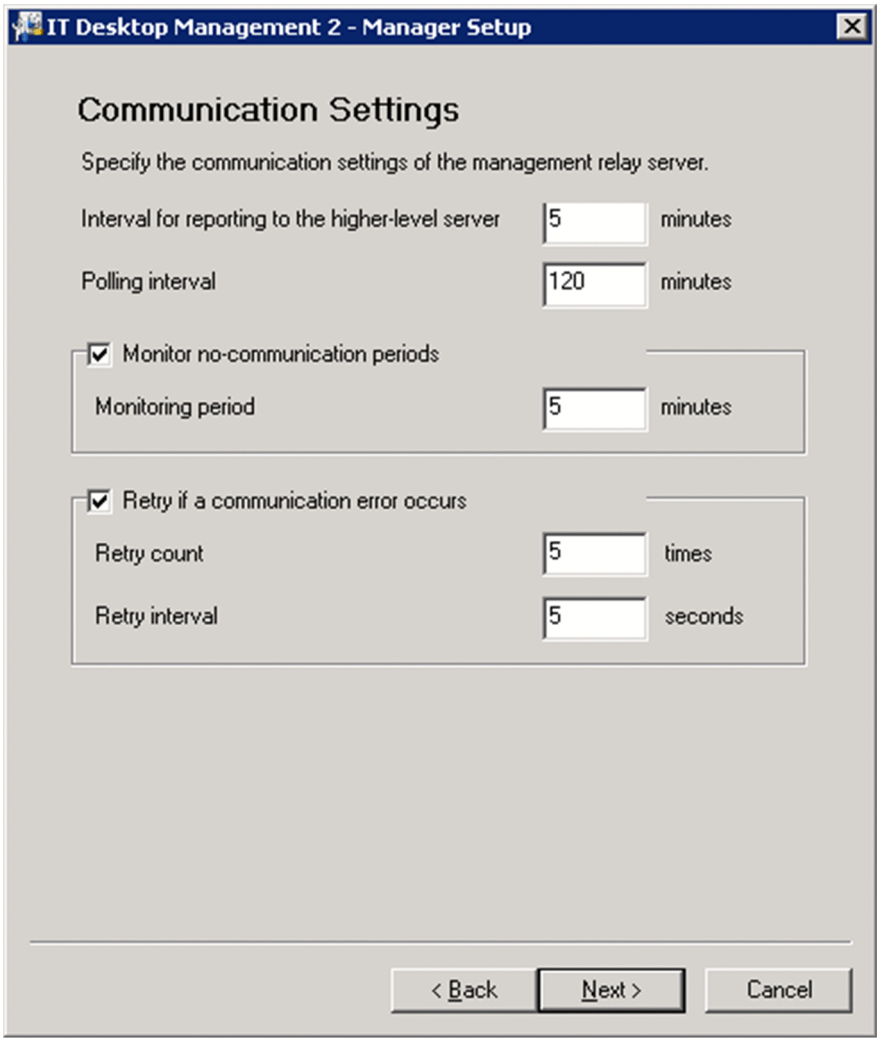
3.8 Procedure for changing the communication settings on a management relay server

The procedure described here is included in the setup of a management relay server.

You can change the communication settings on a management relay server.

To change the communication settings on a management relay server:

1. Log on 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 **Setup**.
3. In the setup window, click the **Next** button.
4. In the **Select a Setup** window, select **Modify settings**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Communication Settings** window appears.



6. Optionally, change the following settings as necessary, and then click the **Next** button:
   - Interval for reporting to a higher-level server

Specify the interval at which to report the device information and device-related data to the higher management server.

- Polling interval

  Specify the interval at which to perform polling between the management relay server and the higher management server.

- Monitor no-communication periods

  If you select this option, the system assumes that a communication error occurred when the length of time during which the higher management server does not respond exceeds the preset time. Set the time for **Monitoring period**.

- Retry if a communication error occurs

  If you select this option, the system retries communication when a communication error occurs. Specify **Retry count** and **Retry interval**.

7. Continue to click the **Next** button until the **Confirm Setup Settings** window appears.

8. In the **Confirm Setup Settings** window, confirm the specified settings, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console are not being used is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

9. In the **Setup for Distribution by Using Remote Install Manager** window, click the **OK** button.

   Setup starts, and a dialog box indicating that processing is in progress appears. When setup ends, the **Setup has Completed** window appears.

10. In the **Setup has Completed** window, click the **OK** button.

Now you have changed the communication settings on the management relay server.

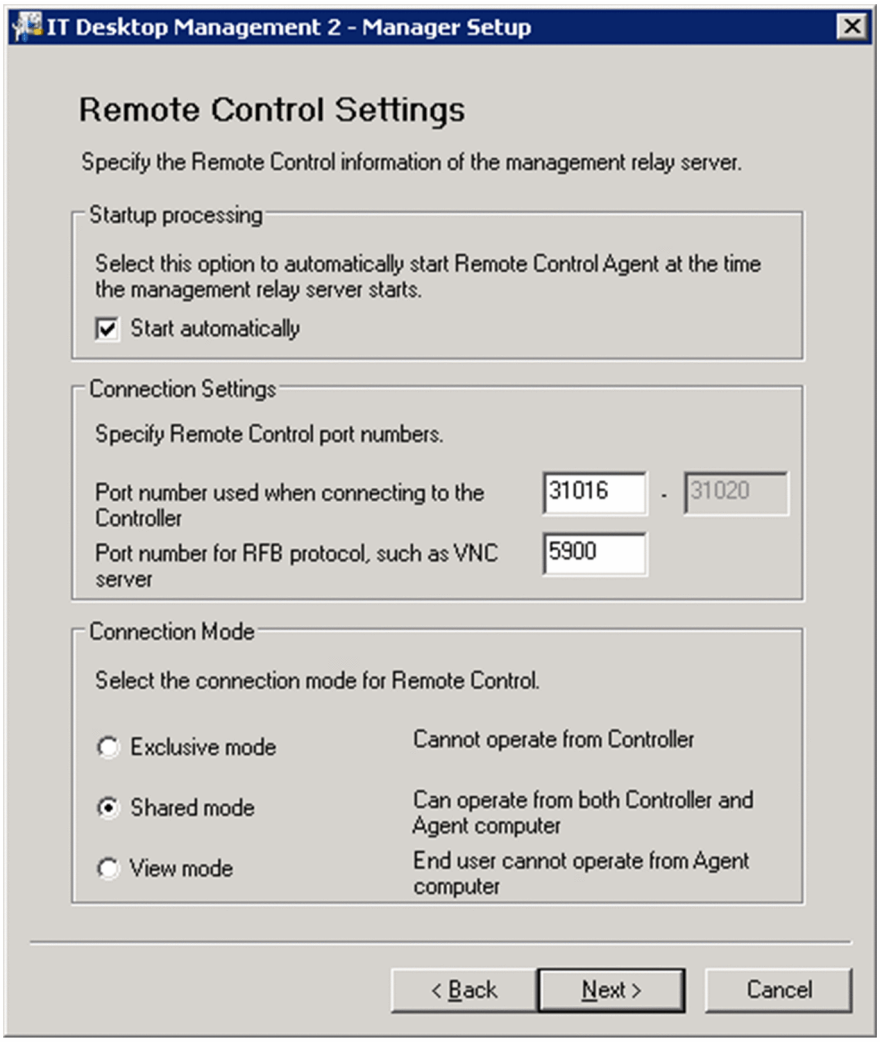
3.9 Procedure for changing the remote control settings on a management relay server

The procedure described here is included in the setup of a management relay server.

You can change the remote control settings on a management relay server.

To change the remote control settings on a management relay server:

1. Log on 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 **Setup**.
3. In the setup window, click the **Next** button.
4. In the **Select a Setup** window, select **Modify settings**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Remote Control Settings** window appears.



6. Optionally, change the following settings as necessary, and then click the **Next** button:
   - Startup processing

You can set whether to automatically start the remote control agent when the agent for the management relay server starts.

- Connection Settings

  For **Port number used when connecting to the Controller**, specify the port number to be used for a standard connection. For **Port number for RFB protocol, such as VNC server**, specify the port number to be used for RFB connection.

- Connection Mode

  Select the mode in which the connection-destination computer permits connection.

7. In the window that appears, optionally specify the following settings as necessary, and then click the **Next** button:

   - Settings of Allowed Controllers

     You can add the controllers for which you want to allow to use the remote control function.

   - User Settings

     To authenticate the users who attempt to connect to controllers, add the **Name** and **Type** settings for those users.

8. Continue to click the **Next** button until the **Confirm Setup Settings** window appears.

9. In the **Confirm Setup Settings** window, confirm the specified settings, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

10. In the **Setup for Distribution by Using Remote Install Manager** window, click the **OK** button.

    Setup starts, and a dialog box indicating that processing is in progress appears. When setup ends, the **Setup has Completed** window appears.

11. In the **Setup has Completed** window, click the **OK** button.

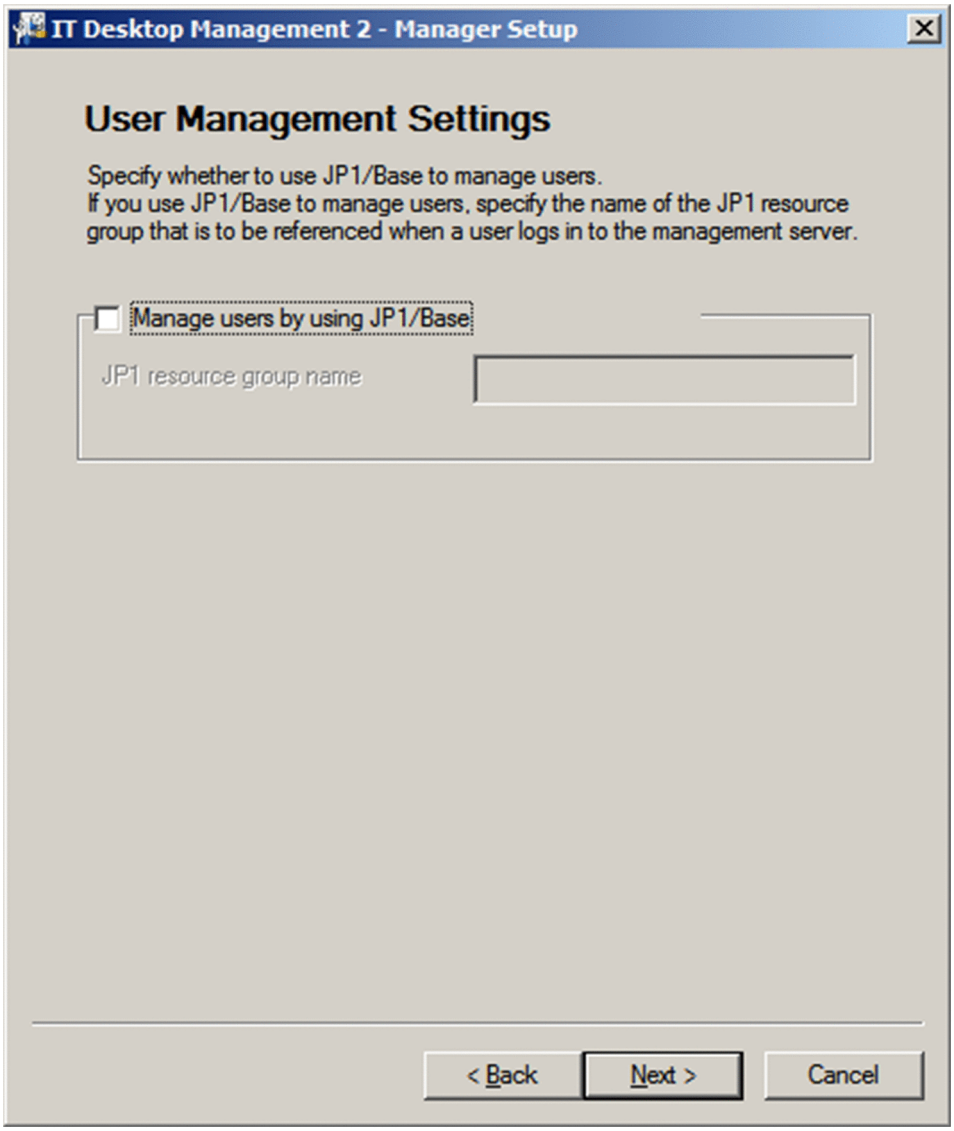
Now you have changed the remote control settings on the management relay server.

3.10 Changing the user management settings

You can change the user management settings to specify whether to use JP1/Base for user management. When changing the settings, you can select to use either ITDM2 authentication or JP1 authentication.

To change the user management settings:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **User Management Settings** window appears.



6. Specify the following items, and then click the **Next** button.
   - Manage users by using JP1/Base

Select this check box if you want to use JP1 authentication as the authentication method at login. To use this method, you must register the JP1 users on the JP1/Base authentication server before you start using JP1/IT Desktop Management 2. In addition, if you select this check box, you will become unable to set expiration periods for locks and passwords for the user accounts in JP1/IT Desktop Management 2.

Clear this check box if you want to use ITDM2 authentication as the authentication method at login.

- JP1 resource group name

  If you selected **Manage users by using JP1/Base**, you must also specify the JP1 resource group name. Make sure that you specify the same resource group name as the name you specified when you registered the JP1 user account.

7. Continue to click the **Next** button until the **Confirm Setup Settings** view appears.
8. In the **Confirm Setup Settings** view, confirm the settings, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console are not being used is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
9. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

   The setup process begins, and a dialog box appears, indicating that setup is in progress. When setup finishes, the **Setup Complete** view will appear.
10. In the **Setup Complete** view, click the **OK** button.

The user management settings have been changed.

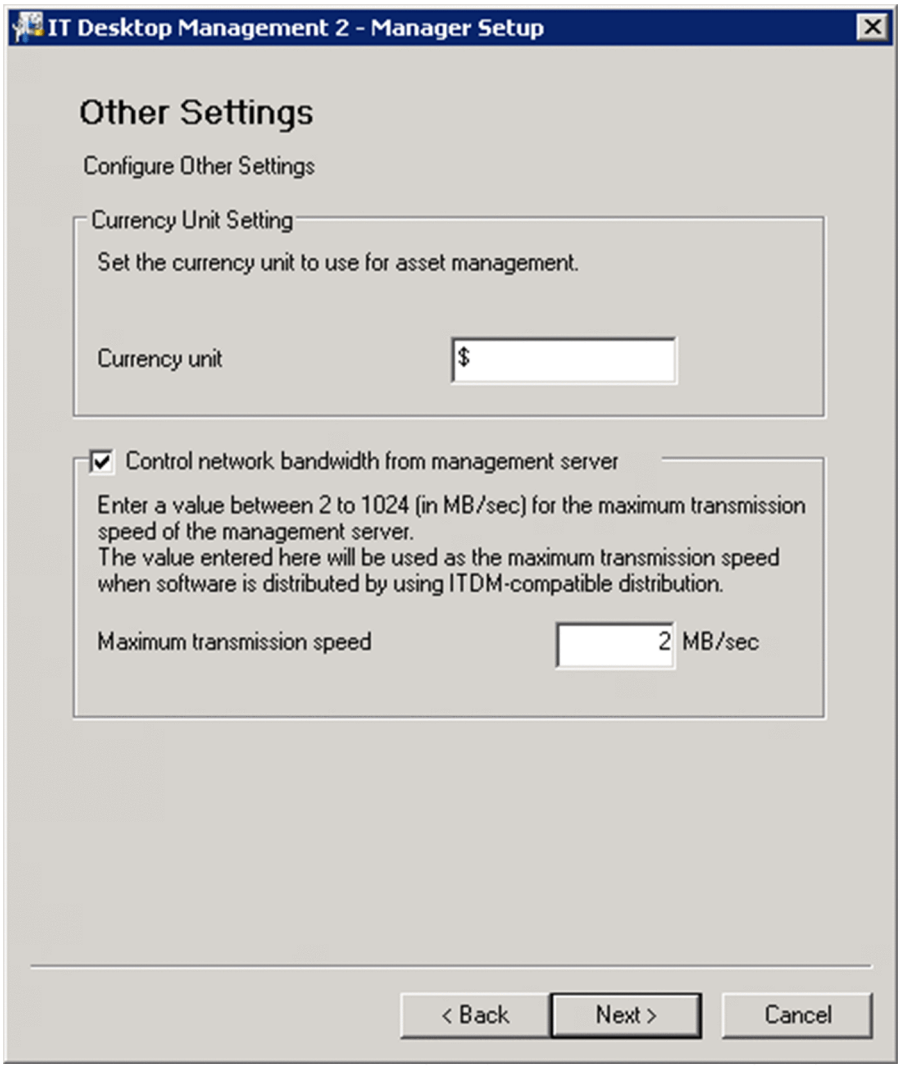
3.11 Procedure for changing the currency unit

This is a management server setup item.

You can change the currency unit you use for asset management.

To change the currency unit:

1. Log on to the OS as a user with administrator permissions.
2. On the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Other Settings** view opens.



6. In the **Currency Unit Setting** section, enter a value in **Currency Unit**, and then click the **Next** button.
7. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.

A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console are not being used is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

8. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.

9. In the **Setup Complete** view, click the **OK** button.

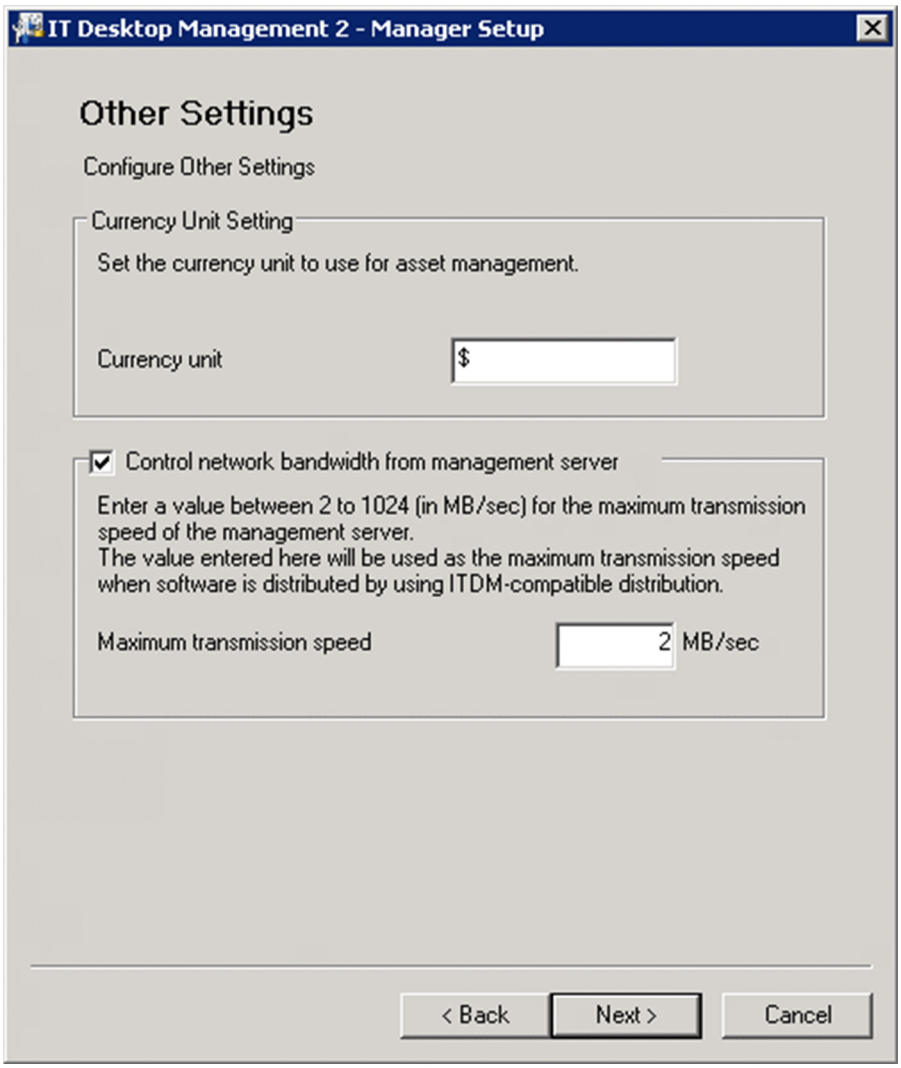
The currency unit is changed.

3.12 Procedure for controlling the network bandwidth used for distribution

By setting a maximum transfer speed, you can ensure that the distribution of software and files from the management server to managed computers does not monopolize the network bandwidth.

To control the network bandwidth used for ITDM-compatible distribution:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Click the **Next** button until the **Other Settings** view opens.



6. Select **Control network bandwidth from management server**, enter a value in **Maximum transmission speed**, and then click the **Next** button.
7. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.

A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console are not being used is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

8. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.
   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.

9. In the **Setup Complete** view, click the **OK** button.

You can now control the network bandwidth.

To control the network bandwidth used for distributions using Remote Install Manager:

1. Stop the service of JP1/IT Desktop Management 2 - Manager.

2. Add the required setting to the configuration file.
   The configuration file (jdn_rim_distr_bwc.conf) is stored in the following location:
   instalation-folder-of-JP1/IT Desktop Management 2\mgr\conf

3. Start the service of JP1/IT Desktop Management 2 - Manager.

Network bandwidth can now be controlled.

The following tables list and describe the definitions in the configuration file:

Section	Key name	Description	Initial values	Required?
BandwidthCtrl	Function	Specify whether to control data flow when using Remote Install Manager to distribute software and files. • `ON`: Control data flow. • `OFF`: Do not control data flow.	`OFF`	Yes
Setting*N*[#1]	MinIP[#2]	Specify the first value of the IP addresses in the range from 0.0.0.0 to 255.255.255.255.	`0.0.0.0`	Yes
	MaxIP	Specify the last value of the IP addresses in the range from 0.0.0.0 to 255.255.255.255.	`255.255.255.255`	Yes
	MaxTransSpeedKbps	Specify the maximum transfer speed in Kbps by using an integer in the range from 32[#3] to 8388608[#4].	`15360`	Yes

#1: *N* represents a value in the range from 1 to 30. If multiple IP address ranges are specified, specify the definition like this: `Setting1`,`Setting2`,`Setting3`. Also, if you specify multiple IP address ranges, make sure that the IP address ranges of different `Setting`*N* sections do not overlap.

#2: Specify a value smaller than the value of MaxIP. If you specify a value lager than the value of MaxIP, the settings in the `Setting`*N* section will be ignored.

#3: 32 Kbps is equal to 4 KB per second (32 ÷ 8 bits = 4).

#4: 8,388,608 Kbps is equal to 1,048,576 KB per second (8,388,608 ÷ 8 bits = 1,048,576) or 1,024 MB per second.

Examples of setting the configuration file are shown below.

When controlling the data flow of the network bandwidth of the entire LAN on which the management server is configured

```
[BandwidthCtrl]
Function=ON

[Setting1]
MinIP=0.0.0.0
MaxIP=255.255.255.255
MaxTransSpeedKbps=1024
```

When controlling the data flow of a specific network bandwidth

```
[BandwidthCtrl]
Function=ON

[Setting1]
MinIP=192.168.0.0
MaxIP=192.168.0.255
MaxTransSpeedKbps=1024

[Setting2]
MinIP=192.168.100.0
MaxIP=192.168.100.255
MaxTransSpeedKbps=320
```

Note the following regarding the configuration file:

- If duplicate sections exist, the section defined first takes effect.
- If duplicate keys exist, the key defined first in a section takes effect.
- If the IP address ranges of the `Setting`*N* sections overlap (example: a range including 192.168.100.* is included in both `Setting1` and `Setting2`), data flows according to the settings in the section that has the highest priority (according to the value of *N*; `Setting1` has the top priority). In other words, the maximum transfer speed for distribution to an agent whose IP address is 192.168.100.* (where the * is a value from 0 to 255) is 1,024 Kbps.

```
[BandwidthCtrl]
Function=ON

[Setting1]
MinIP=192.168.0.0
MaxIP=192.168.100.255
MaxTransSpeedKbps=1024

[Setting2]
MinIP=192.168.100.0
MaxIP=192.168.200.255
MaxTransSpeedKbps=320
```

- If `OFF` is specified for the `Function` key of the `BandwidthCtrl` section, data flow is not controlled even if one or more `Setting`*N* sections exist.
- If `ON` is specified for the `Function` key of the `BandwidthCtrl` section, data flow is not controlled if none of the `Setting`*N* sections are valid.
- If the configuration file (jdn_rim_distr_bwc.conf) could not be opened, data flow is not controlled.

Tip

You can check the application of flow control for the distribution function that uses Remote Install Manger either in the MAIN.LOG file output when the management server starts up or the messages in the Windows event log file.

Tip

Data flow is not controlled in the following situations:

- Collecting files by using the remote collection function
- Distributing software or files when multicast distribution is enabled

To control network bandwidth for distribution by using Remote Install Manager in relay system:

1. Add the settings to relay system configuration file.
   The storage location of the configuration file (jdn_rim_distr_bwc.conf) is as follows.
   JP1/IT Desktop Management 2-Agent installation folder\conf\jdn_rim_distr_bwc.conf
   The following table describes the definitions to be set in the configuration file.

Section	Key name	Description	Initial value	Required?
BandwidthCtrl	Function	Specifies whether to control the data flow with relay system during distribution by using Remote Install Manager. • `ON`: Control data flow. • `OFF`: Do not control data flow.	`OFF`	Yes
Setting	MaxTransSpeedKbps	Specify the maximum transfer speed in Kbps by using an integer in the range from 32[#1] to 8388608[#2].	`15360`	Yes

   #1: 32 Kbps is equal to 4 KB per second (32 ÷ 8 bits = 4).
   #2: 8,388,608 Kbps is equal to 1,048,576 KB per second (8,388,608 ÷ 8 bits = 1,048,576) or 1,024 MB per second.
   The following shows a sample configuration file for relay system.

```
[BandwidthCtrl]
Function=ON

[Setting]
MaxTransSpeedKbps=1024
```

   Note the following regarding the configuration file:

   - If duplicate sections exist, the section defined first takes effect.
   - If duplicate keys exist, the key defined first in a section takes effect.
   - If `OFF` is specified for the `Function` key of the `BandwidthCtrl` section, data flow is not controlled even if one or more `Setting` sections exist.
   - If `ON` is specified for the `Function` key of the `BandwidthCtrl` section, data flow is not controlled if none of the `Setting` sections are valid.
   - If the configuration file (jdn_rim_distr_bwc.conf) could not be opened, data flow is not controlled.

2. Restart OS of relay system.

3. Check MAIN.LOG file of relay system.

   Check that all the settings specified in the setting file have been outputted in the message about the application status of the flow rate control in distribution by using Remote Install Manager function.

To disable control for network bandwidth on distribution by using Remote Install Manager in relay system, specify `OFF` in `Function` in `BandwidthCtrl` section of the configuration file, and then perform the same steps.

For an administrator to distribute configuration files from Remote Installation Manager to subordinate relay systems:

1. On the administrator's terminal, create a configuration file to distribute to relay system.

   For more information about the configuration file to create, see step 1 in “To control network bandwidth for distribution by using Remote Install Manager in relay system”.

2. On the administrator's terminal, package the created configuration file from Packager.

3. From the Remote Install Manager, distribute the packaged configuration files to the relay system in a distribution job.

   When creating a distribution job, set the following items in the **Change Installation Conditions** dialog box that is displayed by clicking the **Change** button in the **Package** page.

   System Conditions page

   - Specify the following path in installation target directory

   JP1/IT Desktop Management 2-Agent installation folder\conf

   - Select the **Replace existing package** checkbox.

   Options page

   Select the **Restart computer after installation** check box.

   For more information on job creation, see the instructions on running remote installation in “JP1/IT Desktop Management 2 Distribution Function Administration Guide” manual.

4. In Remote Install Manager Job Execution Status window, verify that distribution job to relay system is complete.

5. Run the remote collect job in the Remote Installation Manager to collect the configuration files and public logs distributed from the relay system.

   Specify the following files to be collected:

   - Distributed configuration file
   - Publishing log: *JP1/IT Desktop Management 2-Agent installation folder*\log\MAIN_0000.log

6. Make sure that the collected configuration file is the same as the file created in step 1.

7. Review the collected publishing logs.

   Check that all the settings specified in the setting file have been outputted in the message about the application status of the flow rate control in distribution by using Remote Install Manager function.

To disable control for network bandwidth on distribution by using Remote Install Manager in relay system, specify `OFF` in `Function` in `BandwidthCtrl` section of the configuration file, and then perform the same steps.

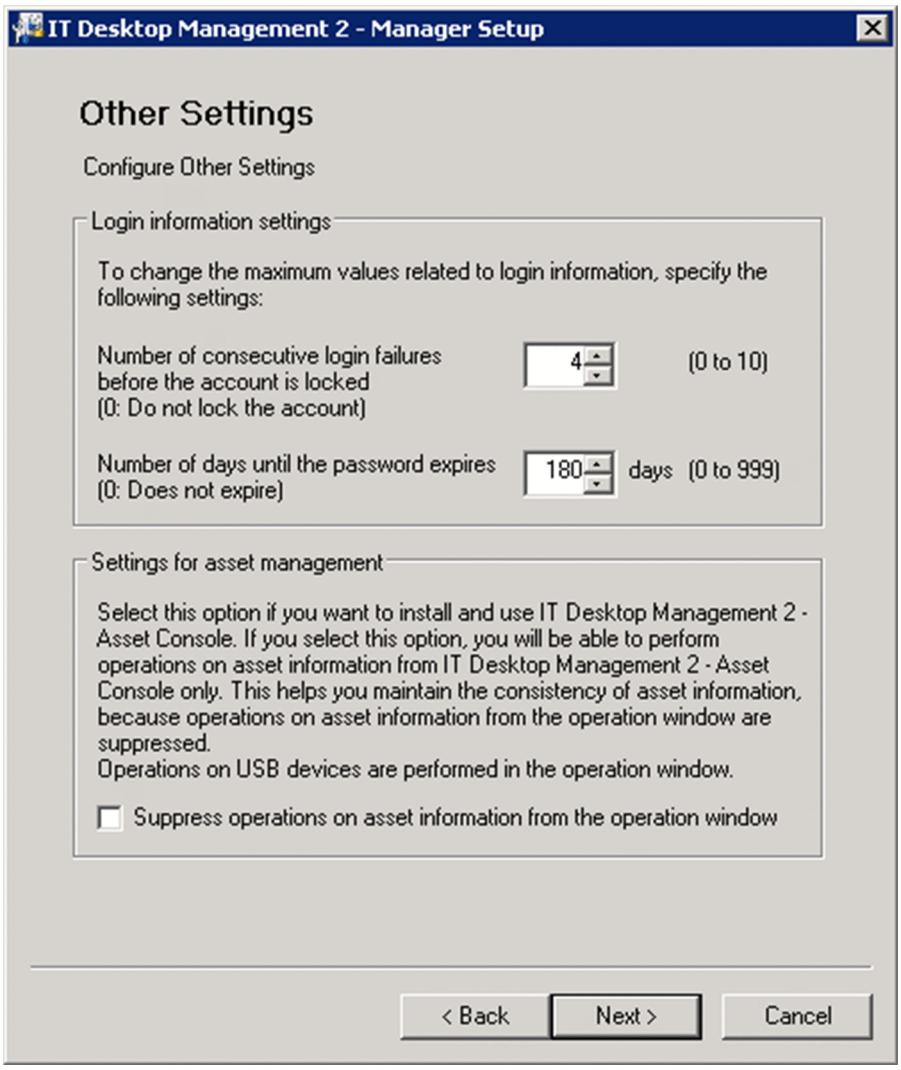
3.13 Procedure for changing login restrictions

You can change how many times a user can enter the wrong password in succession before the account is locked, and the valid period for user passwords.

> **Important**
>
> If the setting to use JP1 authentication is specified in the **User Management Settings** window during setup, you will become unable to set expiration periods for locks and passwords for the user accounts in JP1/IT Desktop Management 2. In such a case, the value specified for **Login information settings** in the **Other Settings** window is not applied.

To set the number of login attempts before an account is locked and the valid period for passwords:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Other Settings** view appears.
   An example of the **Other Settings** view is shown below.



6. Set the following items as needed, and then click the **Next** button.
   - **Number of consecutive login failures before the account is locked**
     Specify how many times a user can enter the wrong password in succession before the account is locked.
   - **Number of days until the password expires**
     Specify the number of days a user password is valid.
7. In the **Confirm Setup Settings** view, confirm that the specified settings are correct, and then click the **Next** button.
   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
8. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.
   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.
9. In the **Setup Complete** view, click the **OK** button.

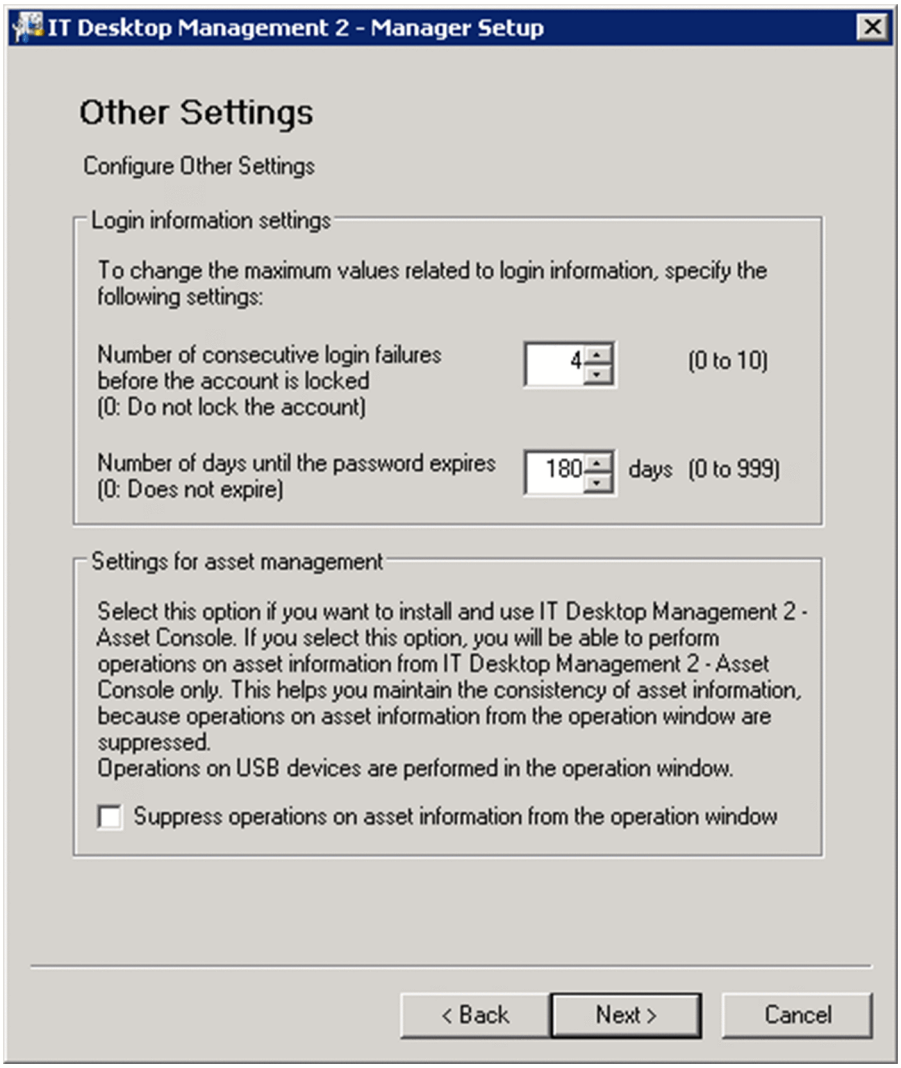
The changes to login restrictions take effect.

3.14 Procedure for suppressing asset information registration and modification

If you intend to use Asset Console to manage assets, you need to suppress the registration and editing of asset information from the user interface.

To suppress the registration and editing of asset information:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Other Settings** view appears.
   An example of the **Other Settings** view is shown below.



6. Select the **Suppress operations on asset information from the operation window** check box, and then click the **Next** button.

7. Review the settings in the **Confirm Setup Settings** view, and then click the **Next** button.

   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

8. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.

   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.

9. In the **Setup Complete** view, click the **OK** button.

The registration and editing of asset information in the user interface is now suppressed.

3.15 Procedure for upgrading a database

This is a management server setup item.

If you performed an overwrite installation of JP1/IT Desktop Management 2, upgrade a database when you need.

> **Important**
>
> If the **Setup** check box was cleared at completion of the overwrite installation, setup will not have taken place. In this case, upgrade the database by performing the following procedure.

To upgrade a database:

1. Log on to the OS as a user with administrator permissions.
2. On the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Database Upgrade**, and then click the **Next** button.
   You can only select **Database Upgrade** if JP1/IT Desktop Management 2 determines that a database upgrade is required. If **Database Upgrade** is unavailable, this means that the database does not need to be upgraded. In this case, click **Cancel** button to exit setup.
5. In the **Database Upgrade Settings** view, specify the upgrade settings, and then click the **Next** button.
   When you change the database folder, the data other than the operation logs in the database in the old folder is passed to the new folder, but the old data for operation logs is deleted. Perform manual acquisition of operation log data as needed.
6. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.
7. In the dialog box indicating that setup is complete, set whether to register components after setup, and then click the **OK** button.
   Components include agents and network monitor agents. Registering these programs on the management server allows you to deploy the agent software, and to install the network monitor agent from the user interface.
   To register a component, specify the settings related to component registration and update when the **Component Registration** dialog box opens.

   > **Tip**
   >
   > If you start setup after installation, you can update a component in the dialog box indicating that setup is complete.

   For details about updating components, see 5.8 Updating components.

The database is upgraded.

3.16 Procedure for initializing a database

You can initialize a database used by JP1/IT Desktop Management 2.

To initialize a database:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Database Re-creation**.
5. Click the **Next** button to set the database in each view.
6. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.
   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
7. In the dialog box indicating that setup is complete, set whether to register components after setup, and then click the **OK** button.
   Components include agents and network monitor agents. Registering these programs on the management server allows you to deploy the agent software, and to install the network monitor agent from the user interface.
   To register a component, specify the settings for component registration and update when the **Component Registration** dialog box opens.
   For details about updating components, see 5.8 Updating components.

The database is initialized.

> **Important**
>
> Even if you initialize a database, the files in the folders are not deleted. If you do not need the data in the work folder or the data in the save folder for the backup of operation logs, delete the data manually.

3.17 Procedure for configuring to use the API

This is a management server setup item.

You can configure to use the API on a management server.

To specify settings for using the API:

1. Log on 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 **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Click the **Next** button until the **API Settings** view opens.
6. Select the **Use the API** check box, and then click the **Next** button.
7. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.
   A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console are not being used is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.
8. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.
   The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.
9. In the **Setup Complete** view, click the **OK** button.

The API is now available.

4 Customizing the settings specified when building a system

This chapter describes the settings that you can customize when building a system.

4.1 Settings for building a minimal configuration system

4.1.1 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 4.1.2 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:

- 1.7.3 Checking the device discovery status
- 4.1.2 Credentials used in discovery from IP address

4.1.2 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.

4.1.3 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.

4.1.4 Procedure for adding relay system configurations

In environments in which Remote Install Manager is used to distribute software, you might want to use different settings on different relay systems. For example, such settings as the system where ID groups are registered, the ID key for operations, notification to the management server, and processing on the relay system might differ between systems. You can achieve this kind of environment by adding relay system configurations, which the system handles as a subset of agent configurations.

To add a relay system configuration:

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 dialog box that appears, select **Relay system settings** and enter the configuration information.
5. Enter configuration information for the other items as needed, and then click the **OK** button.

The agent configuration for the relay system is added, and appears in the list of agent configurations.

From the **Windows Agent Configurations Assignment** view, you can apply the agent configuration you added to a computer with the relay system software installed.

4.1.5 Procedure for using configuration files to configure processing

You can use the configuration file to make changes to certain settings, including the time at which processing starts and whether a device is to be considered scrapped after JP1/IT Desktop Management 2 - Agent is uninstalled. The settings in the configuration file are applied after the JP1/IT Desktop Management 2 service is restarted.

For details about the properties that can be specified in the configuration file, see Lists of properties in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

To apply settings using the configuration file (`jdn_manager_config.conf`):

1. Add settings to the configuration file.
   The configuration file (`jdn_manager_config.conf`) is stored in the following folder:
   JP1/IT-Desktop-Management-2-installation-folder`\mgr\conf`

The following table describes the definitions you can set in the configuration file:

Property	Description	Setting values	Default value
`State_AfterAgentUninstalling`[#1]	Specifies whether the system interprets	• `0`: Handle as uninstallation • `1`: Handle as scrapping device	`0`

Property	Description	Setting values	Default value
State_AfterAgentUninstalling[#1]	uninstallation of JP1/IT Desktop Management 2 - Agent as scrapping of the device, or merely the uninstallation of the JP1/IT Desktop Management 2 - Agent software.	• 0: Handle as uninstallation • 1: Handle as scrapping device	0
Report_Data_MakeTime[#4]	When to compile data for reports	00:00 to 23:59	23:00
Report_Digest_MakeTime[#4]	When to create digest reports	00:00 to 23:59	06:00
DB_MentenanceTime[#4]	When to perform database maintenance	00:00 to 23:59	05:00
ChangeHistory_GetTime[#4]	When to acquire revision history data	00:00 to 23:59	00:00
OpLog_DB_DeleteTime[#4]	When to maintain the database of automatically acquired operation log data	00:00 to 23:59	01:00
DeviceAutoMaintenanceTime[#4]	When to start maintenance processing if device maintenance is enabled	00:00 to 23:59	23:00
AgentStartMenu_Display	Settings for the display of start menu items for an agent due to distribution of Agent Installer and agents	• ON: All start menu items for the agent are displayed. • OFF: None of the start menu items for the agent are displayed.[#2] • SELECT:*xxx*,*xxx*,... : Select the start menu items to be displayed. The following lists the menu items that can be specified for *xxx*. To specify multiple menu items, separate them by using commas (,). • IDR: **Register ID** • UINF: **End User Form** • PSM: **Package Setup Manager** • RCCHA: **Remote Control Agent - Taskbar appearance** • RCREQ: **Remote Control Agent - Requester Wizard** • RCAGT: **Remote Control Agent - Remote Control Agent** • ATAIT: **Administrator Tool - Automatic Installation Tool** • ATUSB: **Administrator Tool - Register USB Device** • ATSET: **Administrator Tool - Setup** • ATPACK: **Administrator Tool - Packager** • ATSEND: **Administrator Tool - Send Inventory** For example, if you want to display **Package Setup Manager** and **Register USB Device**, specify the following:	None

Property	Description	Setting values	Default value
AgentStartMenu_Display	Settings for the display of start menu items for an agent due to distribution of Agent Installer and agents	SELECT:PSM,ATUSB	None
SDM_Mapping_Name	Specifies whether to map the smart device name registered in JP1/IT Desktop Management 2 - Smart Device Manager as the host name, computer name, or device name displayed in the JP1/IT Desktop Management 2 operation window,	0: Do not map[#3] 1: Map	1
Mgrsrv_Patch_AutoPackageKind	Set whether to automatically acquire update program or not	0: Do not automatically acquire update program 1: Automatically acquire update program	1
ExcludeNetworkGroup[#5]	Settings to suppress the network group automatic generation	32 Other values cannot be specified.	None
AbortDeviceIdentify[#6]	Settings that do not perform identification when registering devices	Specify one or more MAC addresses The MAC address is specified by 17 characters, including separators. Alphabetic characters are not case sensitive. The separator for the MAC address specifies ":" or "-". If you specify more than one MAC address, separate the items by commas (,). For example, if you specify 00:05:9a:3c:7a:00 and 00:09:0f:fe:00:01, specify the following: 00:05:9a:3c:7a:00,00:09:0f:fe:00:01 The maximum number of MAC addresses that can be specified is 30.	None
DisableNCListUpdate[#7]	Settings to suppress automatic update of network control list	Specify one or more MAC addresses Specify one or a combination of the following: • Duplicate MAC addresses on multiple devices The MAC address is specified by 17 characters, including separators. • Random MAC Address Specifies a random MAC address and a forward match of up to 17 characters. Alphabetic characters are not case sensitive. The separator for the MAC address specifies ":" or "-". If you specify more than one MAC address, separate the items by commas (,). For example, if you specify 00:05:9a:3c:7a:00 and 00:09:0f:fe:00:01, specify the following: 00:05:9a:3c:7a:00,00:09:0f:fe:00:01 Forward matches are specified, including "$". For example, if you want the first "02:05:", to specify a matching MAC address, specify the following: 02:05:$ The maximum number of MAC addresses that can be specified is 100.	None

Property	Description	Setting values	Default value
NetworkControlListWarningThreshold	Alert threshold of the Network Control List	0 to 262140	162140
NetworkControlListNoticeOption	Set whether to notify notification items on the home screen when the number of network control list registrations reaches the warning threshold and the limit is reached	`ON`: Notify `OFF`: Not notify	ON

#1:

If the management server does not receive the uninstallation notification from the agent, its device information will remain unchanged in the system regardless of the option you specify. In this case, take action such as manually deleting the device information. For devices for which Network Monitor is enabled, the device inventory is not deleted. After disabling Network Monitor, you need to delete the device inventory manually.

#2:

In the case of the Citrix XenApp and Microsoft RDS server, displaying start menus of agents is not supported, and therefore all the start menus must be hidden from view.

#3:

If 0 is specified, the JP1/IT Desktop Management 2 operation window displays the following information as the host name, computer name, and device name: a combination of the user name, phone number, and model name in the smart-device information obtained from JP1/IT Desktop Management 2 - Smart Device Manager, separated with colons (for example, BobBrown:09012345678:iPhone).

#4:

When changing the time from the default value, in order to avoid increasing the load on the management server due to overlapping processing, please set each setting value shifted by the same time from the default. For example, when shifting by 8 hours, set the process being executed at the default of 23:00 to 7:00 and the function executed at default 00:00 to 8:00.

#5

Does not create a network group when the subnet mask information is signaled by 255.255.255.255, and prevents the state of increasing the number of network groups. If the device does not belong to any network group, it belongs to the "Unknown" group.

#6

Specify duplicate MAC addresses on multiple devices. If the MAC address notified by the device matches one of the MAC addresses specified in the setting value, the device will not be identified.

#7

If the MAC address notified by the device matches one of the MAC addresses specified in the setting value, the network control list will not be updated.

The following is an example of a configuration file setting:

```
#
# Configuration file
#
# Time for collecting revision history
ChangeHistory_GetTime=00:00
```

The settings in the configuration file are applied after the JP1/IT Desktop Management 2 service is restarted.

4.1.6 Procedure for changing agent monitoring items

You can use an inventory settings file (`jdng_inventory.conf`) to change the items that are subject to regular monitoring on computers with the agent software installed.

To change the monitored items for agents:

1. Using a text editor, create an inventory settings file (`jdng_inventory.conf`) with the content shown in the table below, and place it in the `%ALLUSERSPROFILE%\HITACHI\jp1itdma\conf` folder.

Section	Key name	Description	Setting values	Default setting
`SystemInventory`	`DHCPLeaseExpires`	You can specify whether to monitor for changes in the DHCP lease expiry time. If this section or key is omitted or the specified value is invalid, the system operates as if `0` were specified.	• `0`: Do not monitor • `1`: Monitor	`0`
	`DHCPLeaseObtained`	You can specify whether to monitor for changes in the time of obtaining the DHCP lease. If this section or key is omitted or the specified value is invalid, the system operates as if `0` were specified.	• `0`: Do not monitor • `1`: Monitor	`0`

The changes to the monitored items for agents take effect.

The following is an example of an inventory settings file that specifies the expiration and acquisition dates and times of DHCP leases as items to be monitored. The monitoring interval is the value specified in **Monitoring Interval (Others) (min)** in the **Timing of communication with the higher system** area on the **Basic Settings** page during agent setup.

```
[SystemInventory]
DHCPLeaseExpires=1
DHCPLeaseObtained=1
```

The content of the inventory settings file automatically takes effect when device information is next acquired from the agent.

4.1.7 Procedure for changing the settings for managing the software information of agents for UNIX or Mac

To collect UNIX or Mac software information and manage it in the JP1/IT Desktop Management 2 operation window, you must modify the configuration file (jdn_manager_config.conf). By modifying this file, you can display (in the Inventory module) the UNIX or Mac software information reported by the managed UNIX or Mac computers and collected by a job from agents for UNIX or Mac. Using the displayed information, you can also manage UNIX or Mac software licenses. However, depending on the OS, more than a thousand items might be displayed, making it difficult to understand the displayed information quickly.

To modify the configuration file (jdn_manager_config.conf):

1. Modify the settings in the configuration file.

The location of the configuration file (jdn_manager_config.conf) is as follows:
JP1/IT-Desktop-Management-2-installation-folder\mgr\conf

The following table describes the definition to be modified in the configuration file:

Property	Description	Setting values	Default
UNIX_Software_Manage	Specifies whether to manage UNIX or Mac software information.	• YES: Manages the information. • NO: Does not manage the information.	NO

The settings in the configuration file are applied after the JP1/IT Desktop Management 2 service is restarted.

For software / patch information#, it is possible to expand and acquire some information (such as version) of the software information.

#: For details of supported OS, see the description of Acquiring software information in the manual *JP1/IT Desktop Management 2 - Agent (For UNIX Systems)*.

The following table describes the definition to be modified in the configuration file.

Property	Description	Setting values	Default
Expand_LinuxSoftwareInformation	Specifies whether to expand and manage some information of Linux software information	• YES: Acquire • NO: Do not Acquire	NO

The settings of the configuration file are applied after restarting the service of JP1/IT Desktop Management 2. If you want to change the settings, delete the Linux device installation package information from the Remote Install Manager beforehand.

If you enable the settings, the software information is acquired as follows.

software name

The number of characters for software name is expanded from 50 characters to a maximum of 255 characters.

version

- The number of characters for the version is expanded from 6 characters to a maximum of 128 characters.
- Even if the version contains other than uppercase alphanumeric characters, the version will be acquired without omitting them.

4.1.8 Customizing conditions for weak passwords

The strength of a password is displayed in **Password Strength** under **Account Details** in **OS Security Details**. You can use the password definition file (jdng_security.xml) to customize conditions to determine whether a password is weak.

(1) Applying the definition to new agents to be installed

Create a password definition file (named jdng_security.xml) containing the code shown in (3) Settings in jdng_security.xml by using a text editor.

Click the **Create Agent Installer** button in the line of Agent Configuration Name which you want to apply a password definition file, under the **Windows Agent Configurations and Create Agent Installers** in the **Settings** module.

In the **Create Agent Installer** dialog box that appears, click the **Add** button in **Files to Be Deployed Settings** under **Agent Installer Configuration Items** and specify the following information:

File to Be Deployed: jdng_security.xml

Expand Folder: Select %ITDM2AGT%\conf from the drop-down list.

(2) Applying the definition to existing environments

For agent management:

Create a password definition file (named jdng_security.xml) containing the code shown in (3) Settings in jdng_security.xml by using a text editor. Place the definition file in the *JP1/IT-Desktop-Management-2-Agent-installation-folder*\jp1itdma\conf folder.

For agentless management:

Create a password definition file (named jdng_security.xml) containing the code shown in Settings in jdng_security.xml by using a text editor. Place the definition file in the *JP1/IT-Desktop-Management-2-Manager-installation-folder*\bin\miniagent folder.

Note that the definition file is not applied to agentless computers for which the search is already completed. You must place the definition file before the search is performed.

(3) Settings in jdng_security.xml

jdng_security.xml contains information in XML format. Installing an agent deploys the XML file containing the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<Security CreationDate="2009-04-03T00:00:00.000Z">
<PasswordCheck>
<NoPassword>1</NoPassword>
<UserAccount>15</UserAccount>
<ComputerName>7</ComputerName>
<Password>password</Password>
<Password>PASSWORD</Password>
<Password>Password</Password>
<Password>admin</Password>
<Password>ADMIN</Password>
<Password>Admin</Password>
<Password>administrator</Password>
<Password>ADMINISTRATOR</Password>
<Password>Administrator</Password>
</PasswordCheck>
</Security>
```

You can edit element contents in the <Security> and <PasswordCheck> elements to customize conditions to determine whether a password is weak.

Element	Description	Value	Default
NoPassword	Specify whether to check for a blank password. When any value other than 0 or 1 is specified, the system checks for a blank password.	0: Checks for a blank password. 1: Does not check for a blank password.	1
UserAccount	Specify how to determine whether a password includes the user account. Specify the sum (from 1 to 15) of the values of check items that you want. When a negative value, blank, or value exceeding the maximum value is specified, the system checks all items.	0: Does not check. 1: Checks if all characters are in lowercase. 2: Checks if all characters are in uppercase. 4: Checks if only the first character is in uppercase. 8: Checks for an exact match with the user account.	15
ComputerName	Specify how to determine whether a password includes the computer name. Specify the sum (from 1 to 7) of the values of check items that you want. When a negative value, blank, or value exceeding the maximum value is specified, the system checks all items.	0: Does not check. 1: Checks if all characters are in lowercase. 2: Checks if all characters are in uppercase. 4: Checks if only the first character is in uppercase.	7
Password	Specify keywords to check whether any of the keywords is used as a password.	Any keyword	password PASSWORD admin ADMIN Admin administrator ADMINISTRATOR Administrator

The following example disables the password check:

```
<?xml version="1.0" encoding="UTF-8"?>
<Security CreationDate="2009-04-03T00:00:00.000Z">
<PasswordCheck>
<NoPassword>0</NoPassword>
<UserAccount>0</UserAccount>
<ComputerName>0</ComputerName>
</PasswordCheck>
</Security>
```

4.2 Settings for building agentless configuration systems

4.2.1 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.

> **Tip**
>
> For Update interval set on **Agentless Management**, authentication is performed based on previous successful authentication information of the network discovery. Only changing the authentication information setting will not update previous successful authentication information of the network discovery.
>
> In this case, perform discovery from the **IP Address Range** view, and make sure the authentication is successful in order to update the authentication information. Please note that although new authentication information is used when performing **Update Device Details**, previous successful authentication information of the network discovery will not be updated even if the authentication succeeded.

4.3 Settings for building a support service linkage configuration system

4.3.1 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:

- 8.3 updatesupportinfo (uploading support service information)

4.4 Settings for building Active Directory linkage configuration systems

4.4.1 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:

- 4.4.4 Specifying search conditions (searching Active Directory)

4.4.2 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.

4.4.3 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:

- 4.4.4 Specifying search conditions (searching Active Directory)
- 1.7.3 Checking the device discovery status

4.4.4 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:

- 1.7.3 Checking the device discovery status

4.4.5 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.

4.5 Settings for building MDM linkage configuration systems

4.5.1 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 `changeit`.
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**.

Additional settings for using Microsoft Intune as MDM system:

When working with Microsoft Intune, you must register the following root CA certificate in Java keystore of PC where JP1/IT Desktop Management 2-Manager is installed:

- DigiCert Global Root CA

If this root CA certificates are not registered in Java keystore, download the root CA certificate file from the DigiCert website and run the following command at the command prompt:

JP1/IT Desktop Management 2 - Manager installation folder\mgr\uCPSB\jdk\jre\bin\keytool.exe -import -file DigiCertGlobalRootCA.crt -alias DigiCertGlobalRootCA -keystore *JP1/IT Desktop Management 2 - Manager installation folder*\mgr\uCPSB\jdk\jre\lib\security\cacerts

When the command is executed, you are asked to type a password to import the server certificate. Type the password. The default password is `changeit`.

Also, register the app using Microsoft Entra ID. Set the following items: Settings that are not listed can be left at their default values.

Authentication-Allow Public Client Flows

Yes

Certificate and secret

Select either Certificate or Client Secret.

API Accessibility

Specify "Microsoft Graph" as API to allow access.

Also, set the following items.

Types of Access Permissions Required for Applications

Application permissions

Name of the access permission

- DeviceManagement-ManagedDevices.Read.All
- DeviceManagement-ManagedDevices.PrivilegedOperations.

Important

When performing version up install from JP1/IT Desktop Management 2 - Manager 11-01 to JP1/IT Desktop Management 2 - Manager 12-50 or later, re-import the root certificate after the upgrade to JP1/IT Desktop Management 2 - Manager 12-50 or later.

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:

- 1.7.5 Checking the discovered devices
- 1.7.6 Checking the managed devices

4.6 Settings for building network monitoring configuration systems

4.6.1 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*.

4.6.2 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.

4.6.3 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.

4.6.4 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.

4.6.5 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.

4.6.6 Procedure for editing the network control settings file

You must edit the network control settings file (`jdn_networkcontrol.conf`) if, for example, you want to manage network connections by using the whitelist method when linkage with JP1/NETM/NM - Manager is being used. In this case, you can edit the file so that detected devices will be added to the network control list as devices that are not permitted to connect to the network.

The settings in the network control settings file are applied to all network segments managed by JP1/IT Desktop Management 2. Note that these settings are not applied to the network segments that are monitored by network monitors. Also note that these settings are not applied to the network connections of any devices that have already been registered in the network control list.

In a cluster configuration, edit the network control settings files on both the primary and secondary management servers.

To edit the network control settings file:

1. On the management server, execute the `stopservice` command.
   The services of the management server stop.
2. Open the network control settings file, and change the value of `NetworkControl_Default` to `1`.
   The location of the network control settings file is as follows:
   `\mgr\conf` in the JP1/IT Desktop Management 2 installation folder
   The following table describes the settings that can be specified in the network control settings file.

Property	Description	Specifiable value	Default
NetworkControl_Default	Specifies how the network connections of detected devices added to the network control list will be controlled.	• 0: Permitted • 1: Not permitted	0

3. On the management server, execute the `startservice` command.

   The services of the management server start.

Editing of the network control settings file is complete.

The following shows an example of setting the network control settings file to prohibit the network connections of detected devices.

```
[NetworkControl]
NetworkControl_Default=1
```

Tip

If you switch from the whitelist method to the blacklist method, edit the network control settings file to permit the network connections of detected devices.

4.6.7 Procedure for replacing a computer by a network control appliance when the network monitor on the computer is enabled

When you replace a computer by a network control appliance, if the network monitor on the computer is enabled, you must disable the network monitor and then install the network control appliance. The replacement procedure shown below assumes that JP1/NETM/NM - Manager has already been installed.

1. Disable the network monitor on the target computer.
2. Deploy and set up a network control appliance in the target network segment.
3. Register the target network segment and group in JP1/NETM/NM - Manager.
4. Specify the environment settings of the network control appliance in JP1/NETM/NM - Manager.

4.7 Settings for building JP1/IM linkage configuration systems

4.7.1 Procedure for setting the configuration file used for linkage with JP1/IM

You can enable the functionality for linking JP1/IT Desktop Management 2 with JP1/IM by changing the configuration file settings.

To set a configuration file (`jdn_manager_config.conf`):

1. Add a setting to the configuration file.
   The configuration file (`jdn_manager_config.conf`) is stored in the following location:
   JP1/IT Desktop Management 2-installation-folder\mgr\conf

The following table describes the relevant definition in the configuration file.

Property	Description	Specifiable values	Default value
JP1IM_EventOption	Specify whether to link with JP1/IM. If linkage is specified, events occurring in the system are monitored regularly, and the events output to the JP1/IM event console are reported to JP1/Base. During regular monitoring, events for output to the JP1/IM event console occurring within 24 hours after ON for this property is detected are obtained.	• `ON`: Link with JP1/IM. • `OFF`: Do not link with JP1/IM.	`OFF`

The following is a setting example for the JP1/IM linkage configuration file:

```
#
# configuration-file
#
# server-customize-option
JP1IM_EventOption=ON
```

The settings in the configuration file are applied after the JP1/IT Desktop Management 2 service is restarted.

If you no longer want to link with JP1/IM, delete the line `JP1IM_EventOption=ON` that you added to the configuration file or change it to `JP1IM_EventOption=OFF`. Then, restart the JP1/IT Desktop Management 2 service.

4.8 Settings for managing 30,000 to 50,000 computers

Use JP1/IT Desktop Management 2 11-10-02 or later.

4.8.1 Settings for collecting operation logs

Operation logs cannot be collected when 30,000 to 50,000 computers are managed. To manage operation logs, you must use a multi-server configuration. You must set up management relay servers so that they cannot notify a higher management server of operation log information collected from managed computers.

4.8.2 Procedure for setting the security judgment

Change the security judgment settings when 30,000 to 50,000 computers are managed. To change the settings:

> **Tip**
>
> Note that the security judgment settings of a management server must be changed when a single server directly manages agents and performs security judgment for more than 30,000 computers.

1. Edit the configuration file to include a statement.
   The configuration file (jdn_manager_config.conf) exists in the following location:
   JP1/IT Desktop Management 2-installation-folder\mgr\conf
   Edit the configuration file to include the following statement: Mgrsrv_jdnmssecurityctrl=10.
2. Restart the JP1/IT Desktop Management 2 service.

4.8.3 In case of 10-20 concurrent users to work with operation windows

> **Tip**
>
> Settings for using operation windows with 10-20 concurrent users are no longer required for versions up to version 12-10.

When you use operation windows with 10-20 concurrent users, consider the following items:

- Set the maximum number of displayed items per page on a list view to 100.
- Change the portlets displayed on the Home module and dashboard for each view to only those that are necessary.

5 Overwrite-installing the product and updating the components

This chapter describes overwrite installation of JP1/IT Desktop Management 2 - Manager and updating of the components (agent, relay system, and network monitor agent).

5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management 2 - Manager

To perform an overwrite installation of JP1/IT Desktop Management 2 - Manager, you must use a version that is no earlier than the currently installed version. In addition, an overwrite installation requires at least 2.5 gigabytes of free space on the hard disk drive.

Important

Before performing an overwrite installation, log out from JP1/IT Desktop Management 2 to close the operation window. If you perform an overwrite installation while the operation window is open, the operation window might not be displayed correctly after the installation.

Important

To perform an overwrite installation on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the permissions level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the program might not run correctly even if you install it again later.

Important

Before installation, make sure that all Windows applications have been closed. If you perform installation without terminating JP1/IT Desktop Management 2 - Manager, restart the OS regardless of whether installation was successful. If service `JP1_ITDM2_Service` does not start or JP1/IT Desktop Management 2 - Manager does not run when the OS is restarted, use the following procedure to perform installation again:

1. Close all Windows applications.
2. Stop the service (`JP1_ITDM2_Service`).
3. Perform overwrite installation again. (The service you stopped will start.)

To perform an overwrite installation of JP1/IT Desktop Management 2 - Manager:

1. Insert the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Manager**, and then click the **Install** button.
3. In the dialog box indicating the start of installation, click the **Next** button.
4. In the **License Agreement** dialog box, check the displayed information, select **I accept the terms in the license agreement**, and then click the **Next** button.
5. In the component selection dialog box, confirm the settings, then click the **Next** button.

6. In the **Type of Manager to Install** dialog box, confirm the Manager type, and then click the **Next** button.

   If **Management relay server** has been selected, go to step 7. If **The management server in a single-server configuration, or the primary management server in a multi-server configuration** has been selected, go to step 8.

7. In the **Agent Component Settings** dialog box, select the agent components to be included on the management relay server, and then click the **Next** button.

8. In the dialog box indicating that installation preparations are complete, check the displayed information, and then click the **Install** button.

   Installation starts. For a cluster configuration, a dialog box prompting for service stoppage if necessary opens. Perform the appropriate operation.

9. In the dialog box indicating that installation is complete, specify the settings for updating components, and then click the **Complete** button.

   For details about updating components, see 5.8 Updating components.

   Tip

   When a database needs to be upgraded, **Setup** appears in the dialog box indicating that the overwrite installation is complete. Select **Setup** or start setup from the **Start** menu to perform setup. In this case, component-related settings are displayed in the dialog box indicating that setup is complete.

The overwrite installation of JP1/IT Desktop Management 2 - Manager is complete. If a message asking you to restart the complete appears, restart it.

Note

When you upgrade this product (by installing it over the previous version of this product), the Import status that was displayed in the **Background Task** panel of the **Home** module is not inherited. The Import status will be updated when you perform an import after the upgrade.

Related Topics:

- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration

5.2 Procedure for performing an overwrite installation of an agent from the supplied media

To perform an overwrite installation of an agent, you must use a version that is not earlier than the currently installed version. In addition, you must log on to the OS as a user with administrator permissions.

Important

To install the agent on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the permissions level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the agent might not run correctly even if you install it again later.

Important

When performing an overwrite installation of JP1/IT Desktop Management 2 - Agent on a computer with JP1/IT Desktop Management - Agent installed, an installation error occurs if the path of the installation folder of JP1/IT Desktop Management - Agent is longer than 104 bytes. In this case, uninstall JP1/IT Desktop Management - Agent before installing JP1/IT Desktop Management 2 - Agent.

To perform an overwrite installation of an agent:

1. Insert the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Agent**, and then click the **Install** button.
3. In the dialog box indicating the start of installation, click the **Next** button.
4. In the **Types of components to be installed** dialog box, select **Agent** and then click the **Next** button.

   Tip

   You can change an agent to a relay system by selecting **Relay system**. However, you will be unable to change it back.

   Tip

   You cannot select **Relay system** unless the management server (or primary management server) is a management relay server. In this case, because you can install the agent only, **Agent** is selected and cannot be changed.

5. In the **Components to be installed** dialog box, select the component and subcomponents you want to install, and the installation method you want to use. Then, click the **Next** button.

   By default, the components selected during the initial installation are set.

6. In the dialog box indicating that installation preparations are complete, click the **Install** button.

Installation starts.

7. In the dialog box indicating that installation is complete, click the **Complete** button.

The overwrite installation of the agent is complete. If a message asking you to restart the computer appears, restart it.

5.3 Procedure for performing an overwrite installation of a relay system from supplied media

To perform an overwrite installation of a relay system, the version you are installing cannot be earlier than the currently installed version.

> **Important**
>
> When installing the software on a Windows computer that uses User Account Control (UAC), a dialog box might appear prompting you to elevate your permission level. In this case, give your permission to continue.

> **Important**
>
> Do not shut down the operating system during installation. If you shut down the operating system while installation is in progress, the program might not operate correctly even if you install it again.

> **Important**
>
> If you need to install a relay system on a computer that was being used as a JP1/IT Desktop Management site server (a computer with JP1/IT Desktop Management - Remote Site Server installed), uninstall JP1/IT Desktop Management - Remote Site Server from the computer before installing the relay system.

To perform an overwrite installation of a relay system:

1. Place the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box, select **JP1/IT Desktop Management 2 - Agent**, and then click the **Install** button.
3. In the dialog box indicating that installation will start, click the **Next** button.
4. In the **Components to be installed** dialog box, select the component and subcomponents you want to install, and the installation method you want to use. Then, click the **Next** button.
   By default, the components selected during the initial installation are set.

   > **Tip**
   >
   > When you want to change the installed components and subcomponents, or to change the installation method of the components, select the installation method from the pull-down menu displayed by clicking the icon to the left of the label.

5. In the dialog box indicating that the preparation for the installation is complete, click the **Install** button.
   The installation process begins.
6. When the installation process has finished, click the **Complete** button.

Overwrite installation of the relay system is complete. Restart the computer if requested to do so.

5.4 Procedure for performing an overwrite installation of a network access control agent from the supplied media

To perform an overwrite installation of a network access control agent, you must use a version that is no earlier than the currently installed version. In addition, you must log on to the OS as a user with administrator permissions.

Important

To install the agent on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the permissions level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the agent might not run correctly even if you install it again later.

To perform an overwrite installation of a network access control agent:

1. Insert the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Network Monitor**, and then click the **Install** button.
3. In the dialog box indicating the start of installation, click the **Next** button.
4. In the dialog box indicating that installation preparations are complete, click the **Install** button.
   Installation starts.
5. In the dialog box indicating that installation is complete, click the **Complete** button.

The overwrite installation of the network access control agent is complete. You do not need to restart the computer.

Important

If the network access control agent is performed overwrite installation on a device before the process of enabling Network Monitor has been completed, restart the device after the overwrite installation.

5.5 Procedure for performing an overwrite installation of an Internet gateway from supplied media

To perform an overwrite installation of an Internet gateway, you must use a version that is no earlier than the currently installed version. In addition, you must log on to the OS as a user with administrator permissions.

Important

To install the agent on a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the permissions level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS during installation. If you do so, the agent might not run correctly even if you install it again later.

Important

Before performing an overwrite installation of an Internet gateway, shut down all Windows applications.

To perform an overwrite installation of an Internet gateway:

1. Stop the World Wide Web Publishing Service.
2. Insert the supplied media in the CD/DVD drive.
3. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Internet Gateway**, and then click the **Install** button.
4. In the dialog box indicating the start of installation, click the **Next** button.
5. In the dialog box indicating that installation preparations are complete, click the **Install** button.
   Installation starts.

   Note

   If, after clicking the **Install** button, a window appears notifying you about the presence of files or services that cannot be updated with the setup, it means that the World Wide Web Publishing Service might still be running. Stop the installation process by using the **Cancel** button, and then start again from step 1.
6. In the dialog box indicating that installation is complete, click the **Complete** button.
   The overwrite installation of an Internet gateway is completed. If a message asking you to restart the computer appears, restart it.
7. Start the World Wide Web Publishing Service.

5.6 Overview of upgrading the entire JP1/IT Desktop Management 2 system

There are two ways to upgrade the entire JP1/IT Desktop Management 2 system, as described in this section. One way is to use the distribution functionality or supplied media, and the other is to update the system components by using the function that automatically updates programs registered on the management server.

To upgrade the system by using the distribution functionality or supplied media:

If you (administrator) want to upgrade the entire system at your convenience, disable the function that automatically upgrades programs registered on the management server beforehand.

1. Upgrade JP1/IT Desktop Management 2 - Manager by performing an overwrite installation of a newer version of the program on the management server.
2. Update the following components:
   - The relay system program on computers configured as relay systems
   - The agent and the network access control agent on the computer on which the network access control agent is installed
   - The controller for the remote control functionality that is installed on the administrator's computer
   - Remote Install Manager installed on the administrator's computer
3. Upgrade the agent on computers on which the network monitor agent is not installed.

To update the system components by using the function that automatically updates programs registered on the management server:

1. Upgrade JP1/IT Desktop Management 2 - Manager by performing an overwrite installation of a newer version of the program on the management server.
2. Register agent, and network access control components on the management server, and set them to be updated automatically.

   Important

   If you want to use the remote control functionality after JP1/IT Desktop Management 2 - Manager has been upgraded, you must first upgrade the controller.

Important

When performing an overwrite installation of JP1/IT Desktop Management 2 - Agent on a computer with JP1/IT Desktop Management - Agent installed, an installation error occurs if the path of the installation folder of JP1/IT Desktop Management - Agent is longer than 104 bytes. In this case, uninstall JP1/IT Desktop Management - Agent before installing JP1/IT Desktop Management 2 - Agent.

Important

You cannot upgrade to JP1/IT Desktop Management 2 from JP1/IT Desktop Management operating in a multi-server configuration system.

Important

Upgrading JP1/IT Desktop Management 2 via version 10-01 or version 10-02, causes the settings for the following items displayed in the management window and their display order to be reset to their default state:

- **Security** - **Computer Security Status** - **Device List**
- **Installed Software** tab in the **Assets** - **Managed Software** - **Managed Software List**
- **Inventory** - **Device Inventory** - **Device List**
- **Installed Software** tab in the **Inventory** - **Device Inventory** - **Device List**
- **Inventory** - **Software Inventory** - **Software List**
- **Settings** - **Discovery** - **Last Discovery Log** - **IP Address Range**

Tip

Linkage with the MDM system starts after the system's server certificate is validated. Specify the necessary settings as described in 4.5 Settings for building MDM linkage configuration systems. Also, confirm that the MDM server's host name is set correctly. For details, see the description of the MDM linkage parameters in the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

Related Topics:

- 5.7 Procedure for upgrading JP1/IT Desktop Management 2 - Manager
- 5.8 Updating components

5.7 Procedure for upgrading JP1/IT Desktop Management 2 - Manager

You can upgrade JP1/IT Desktop Management 2 - Manager by performing an overwrite installation with a new version of the program on the management server.

> **Important**
>
> Before starting the upgrade, log out from JP1/IT Desktop Management 2 to close the operation window. If you perform an upgrade while the operation window is open, the operation window might not operate correctly after the upgrade.

To upgrade JP1/IT Desktop Management 2 - Manager:

1. Back up the database.

   Create a backup of the database for use in the event of a failure.

   Use Database Manager to back up the database. Leave at least 20 gigabytes of free space on the drive containing the backup folder.

2. Perform an overwrite installation of **JP1/IT Desktop Management 2 - Manager** on the management server.

   During installation, at least 2.4 gigabytes of free space is required on the hard disk.

   > **Important**
   >
   > If the overwrite installation fails, restore the environment that existed before the overwrite installation, and then perform step 2 and the subsequent steps. To restore the environment that existed before the overwrite installation, install the old version of the program, register the license, and then restore the database you backed up in step 1. Use Database Manager to restore the database.

   > **Tip**
   >
   > If you set automatic updating of components during the overwrite installation, the agent and network monitor agent installed on the user's computer are updated automatically.

   > **Tip**
   >
   > When the agent and network monitor agent are updated automatically, data is sent to each computer from the management server. Approximately 80 megabytes of data is sent to each computer on which an agent is installed. An additional 5 megabytes of data is sent to computers on which the agent and network monitor agent are both installed.

3. Upgrade the database.

   Perform the setup to upgrade the database.

   > **Tip**
   >
   > When the database upgrade is complete, you can delete the database backup you created in step 1.

Upgrading JP1/IT Desktop Management 2 - Manager is complete.

Tip

Linkage with the MDM system starts after the system's server certificate is validated. Specify the necessary settings as described in 4.5 Settings for building MDM linkage configuration systems. Also, confirm that the MDM server's host name is set correctly. For details, see the description of the MDM linkage parameters in the *JP1/IT Desktop Management 2 Overview and System Design Guide*.

5.8 Updating components

Components include agents and network access control agents. You can upgrade these programs as follows:

> **Important**
>
> When performing an overwrite installation of JP1/IT Desktop Management 2 - Agent on a computer with JP1/IT Desktop Management - Agent installed, an installation error occurs if the path of the installation folder of JP1/IT Desktop Management - Agent is longer than 104 bytes. In this case, uninstall JP1/IT Desktop Management - Agent before installing JP1/IT Desktop Management 2 - Agent.

> **Important**
>
> If you need to install a relay system on a computer that was being used as a JP1/IT Desktop Management site server (a computer with JP1/IT Desktop Management - Remote Site Server installed), uninstall JP1/IT Desktop Management - Remote Site Server before installing the relay system.

Automatically updating components by using programs registered on the management server:

Register a new version of a program on the management server, and distribute it automatically to update the old version.

When you upgrade multiple programs, including JP1/IT Desktop Management 2 - Manager, as in an entire system upgrade, if you set automatic updating of components during the overwrite installation of JP1/IT Desktop Management 2 - Manager, new versions of the agent and network access control agent are registered on the management server and distributed automatically.

You can set the automatic updating of components and registration of each program on the management server in the dialog box indicating that overwrite installation of JP1/IT Desktop Management 2 - Manager is complete, or in the **Component Registration** dialog box that you can open from the **Start** menu on the management server.

Updating components by using ITDM-compatible distribution:

You can update components by registering a package on the management server and creating a task to distribute the package. This method is useful when you do not want to update components automatically because you want to control when the load is applied to the network. If you do not want to update components automatically, you need to disable the automatic updating of programs registered on the management server.

If you upgrade multiple programs, including JP1/IT Desktop Management 2 - Manager, as in an entire system upgrade, and you set components as a package during the overwrite installation of JP1/IT Desktop Management 2 - Manager, new versions of the agent and network access control agent are registered automatically as a package on the management server.

You can register components as a package and register each program on the management server in the dialog box indicating that the overwrite installation of JP1/IT Desktop Management 2 - Manager is complete, or in the **Component Registration** dialog box that you can open from the **Start** menu on the management server.

The name of the package that is registered automatically is [*program-format-name_version-number_program-name-of-each-component*] (for example, **[P-CC2642-7BA4_1050_JP1_IT Desktop Management 2 - Agent]**). Add and distribute a task that specifies this package. When adding a task, make sure the components are updated in the order described in 5.6 Overview of upgrading the entire JP1/IT Desktop Management 2 system.

> **Tip**
>
> When package registration of the component is completed, the name of the automatically registered package is displayed in the message. Even if the package of the same version is registered, the same message is displayed and overwrite registration is not done. To check whether package displayed on

the message is registered or not, check the Last Modified Date/Time of the package from **Packages** - **Package List** of the Distribution (ITDM-compatible) screen. If the Last Modified Date/Time is not updated, redistribution of package is not needed.

Updating components by using supplied media:

Update programs by performing an overwrite installation from the supplied media containing the new versions.

For an overwrite installation, make sure you update components in the order described in 5.6 Overview of upgrading the entire JP1/IT Desktop Management 2 system.

Updating the controller:

If the controller is updated when JP1/IT Desktop Management 2 is upgraded, an overwrite installation is performed automatically when Remote Controller is executed from the operation window.

If you execute Remote Controller from the **Start** menu, an overwrite installation of the controller is not performed. To execute Remote Controller from the **Start** menu, you must execute Remote Controller from the operation window to upgrade the controller first before you update the agent.

Important

An overwrite installation of the controller is not performed in the following cases:

- The proxy server Internet option is not set correctly in the environment to which you want to connect to JP1/IT Desktop Management 2 via the proxy server
- Internet Explorer is in offline mode

Important

If the network access control agent is upgraded on a device before the process of enabling Network Monitor has been completed, restart the device after the upgrade.

Related Topics:

- 5.9 Procedure for registering components

5.9 Procedure for registering components

Components include agents and network monitor agents.

When an updated component or a correction patch is released, it is useful to register the program on a management server and then set automatic updating for it.

If you do not want to update components automatically because you want to control the timing due to network load, you can register the package automatically by registering the updated version of the programs on the management server. In this case, specify the automatically registered package and create a task to distribute the programs.

Tip

When upgrading JP1/IT Desktop Management 2 - Manager, you can set automatic component updating or package registration during an overwrite installation of JP1/IT Desktop Management 2 - Manager. In this case, you do not need to perform any of the operations described here because updated components are registered on the management server and distributed or the package is registered automatically.

Tip

When the agent and network monitor agent are updated automatically, data is sent to each computer from the management server. Approximately 80 megabytes of data is sent to each computer on which an agent is installed. An additional 5 megabytes of data is sent to computers on which the agent and network monitor agent are both installed.

To register a component:

1. Obtain the updated component or correction patch.
2. On the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and **Component Registration**.
3. In the dialog box that opens, click the **Browse** button to specify the upgrade version of a component or a correction patch in the folder to which you downloaded these programs.
4. For the registered component, specify the settings related to automatic updating and package registration.
5. Click the **OK** button.

The upgrade version of a component or the correction patch is registered on the management server, and is distributed, or the package is registered according to the settings.

Tip

If the version of the component to be registered is the same as or older than the already registered version, "Package has already been registered. Please delete the registered package and then re-register the package." Error message will be output.

5.10 Overview of performing an overwrite installation in a cluster system

To perform an overwrite installation of JP1/IT Desktop Management 2 in a cluster system, perform an overwrite installation on the primary server first, and then on the standby server.

To perform overwrite installation in a cluster system:

1. Take the service resources of JP1/IT Desktop Management 2 on the primary server offline.
   For details about the service resources to be taken offline, see the JP1/IT Desktop Management 2 service resources (generic services) row in the table listing the resources that must be registered in groups. You can find the table in 2.10.2 Procedure for creating a resource group on the primary server. The Client access point, and the Storage (shared disk) resource remain online.
2. On the primary server, perform an overwrite installation of JP1/IT Desktop Management 2 - Manager.
3. Start setup on the primary server to upgrade the database.
   If you do not need to upgrade the database, you can skip this step.
4. Copy the file that is output when setup finishes on the primary server to the standby server.
5. Move the owner of the resource group to the standby server.
6. On the standby server, perform an overwrite installation of JP1/IT Desktop Management 2 - Manager.
7. Start setup on the standby server to upgrade the database.
   If you do not need to upgrade the database, you can skip this step.
8. Move the owner of the resource group to the primary server.
9. Bring online the service resource you took offline in step 1.

The process of performing the overwrite installation in a cluster system is complete.

Related Topics:

- 5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management 2 - Manager

5.11 Performing an overwrite installation from JP1/IT Desktop Management and other products to JP1/IT Desktop Management 2

You cannot run JP1/IT Desktop Management 2 on the same computer as its predecessor JP1/IT Desktop Management. However, you can perform an overwrite installation of JP1/IT Desktop Management 2 on a computer with JP1/IT Desktop Management installed.

Security policies in an overwrite installation from JP1/IT Desktop Management:

In JP1/IT Desktop Management 2 - Manager, for the setting values of **Restriction of Device Usage** of security polices, the setting values for JP1/IT Desktop Management 2 - Agent and for JP1/IT Desktop Management - Agent are retained. The settings that can be displayed and edited with the management window are only the settings for JP1/IT Desktop Management 2 - Agent.

- For the security policies migrated from JP1/IT Desktop Management - Manager:
  - For JP1/IT Desktop Management - Agent, the setting value that has been specified in JP1/IT Desktop Management - Manager is passed.
  - There is no setting value for JP1/IT Desktop Management 2 - Agent. It is controlled with the setting for JP1/IT Desktop Management - Agent.
- When you have edited the security policies migrated from JP1/IT Desktop Management - Manager:
  - For JP1/IT Desktop Management - Agent, the setting value specified in JP1/IT Desktop Management - Manager is retained.
  - For JP1/IT Desktop Management 2 - Agent, the setting value is changed to the value specified in the edit window of JP1/IT Desktop Management 2 - Manager.
- When you duplicate the security policies migrated from JP1/IT Desktop Management - Manager:
  - For JP1/IT Desktop Management - Agent, the setting value specified in JP1/IT Desktop Management - Manager from which the duplication is performed.
  - For JP1/IT Desktop Management 2 - Agent, the setting value of the environment from which the duplication is performed is retained.
- When you create security policies in JP1/IT Desktop Management 2 - Manager:
  - For JP1/IT Desktop Management - Agent, All the setting values of **Restriction of Device Usage** are disabled. Using devices is not suppressed.
  - For JP1/IT Desktop Management 2 - Agent, the setting value is the value specified in the edit window of JP1/IT Desktop Management 2 - Manager.

To use **Restriction of Device Usage** in JP1/IT Desktop Management 2 - Manager, install JP1/IT Desktop Management 2 - Agent. In JP1/IT Desktop Management 2 - Manager, the procedure to switch the control of **Restriction of Device Usage** for JP1/IT Desktop Management - Agent is shown as follows:

- To switch the assignment of security policies:

  By changing the assignment of security policies on which the setting of **Restriction of Device Usage** is different for JP1/IT Desktop Management - Agent, the control of **Restriction of Device Usage** is switched. Note that you can perform this procedure when you have created multiple security policies in which the setting of **Restriction of Device Usage** is different in JP1/IT Desktop Management - Manager and perform a migration to JP1/IT Desktop Management - Manager.

Running JP1/Software Distribution and JP1/IT Desktop Management 2 on the same computer

Although you can run JP1/Software Distribution and JP1/IT Desktop Management 2 on the same computer, you cannot perform an overwrite installation from JP1/Software Distribution to JP1/IT Desktop Management 2. The table below describes the specific components that can coexist on the same computer. Note that in environments where both products are present, they cannot connect with each other (that is, JP1/Software Distribution cannot manage the devices managed by JP1/IT Desktop Management 2 and vice versa).

JP1/NETM		JP1/IT Desktop Management 2						
		Management server	Agent	Relay system	Controller	Remote control agent	Network monitor	Asset Console
JP1/Software Distribution Manager (including remote control manager)	Manager	N	Y	Y	Y	Y	Y	Y
	Relay manager	N	Y	Y	Y	Y	Y	Y
JP1/Software Distribution Client (including remote control agent)	Relay system#	Y	Y	Y	Y	Y	Y	Y
	Client	Y	Y	Y	Y	Y	Y	Y
JP1/Software Distribution Manager (Asset Information Manager Limited)	Manager	N	Y	Y	Y	Y	Y	N
	Relay manager	N	Y	Y	Y	Y	Y	N
JP1/Asset Information Manager		N	Y	Y	Y	Y	Y	N
JP1/Client Security Control	Manager	N	Y	Y	Y	Y	Y	N
	Agent	Y	Y	Y	Y	Y	Y	Y
JP1/NM	Manager	Y	Y	Y	Y	Y	Y	Y
	Agent	Y	Y	Y	Y	Y	N	Y

Legend: Y: Can coexist. N: Cannot coexist.

#: Includes JP1/Software Distribution SubManager.

For details about how to perform an overwrite installation from JP1/IT Desktop Management to JP1/IT Desktop Management 2, see 5.6 Overview of upgrading the entire JP1/IT Desktop Management 2 system.

Automatically acquiring JP1/IT Desktop Management operation log data during overwrite installation

You can automatically acquire a maximum of 30 days of operation log data from the online area of the JP1/IT Desktop Management operation log database during an overwrite installation to JP1/IT Desktop Management 2. This data is imported into the JP1/IT Desktop Management 2 operation log database. In the window indicating that setup is complete, select the **Automatically import the operation logs of old products to the database** check box. The automatically acquired operation log data is automatically deleted when the period specified in **Storage period for operation logs to be automatically acquired** in the **Operation Log Settings** view of the Settings module has elapsed.

Important

- To automatically acquire operation log data from JP1/IT Desktop Management, you need to set a storage location in the setup of JP1/IT Desktop Management before performing the overwrite installation.
- The acquisition of operation log data from JP1/IT Desktop Management might take a day or longer.
- You can view the progress of operation log acquisition in the **Background Task** panel of the Home module, or the **Manual Acquisition of Stored Operation Logs** dialog box of the Security module.
- Because the acquisition of JP1/IT Desktop Management operation log data uses the manual acquisition function of JP1/IT Desktop Management 2, the associated events and messages will refer to manual acquisition.
- Because the management methods of operation logs differ between JP1/IT Desktop Management and JP1/IT Desktop Management 2, for operation logs of JP1/IT Desktop Management, on the time chart of the upper part of the Operations Log List view, the dates that are a day before and after the dates on which operation logs exist might be displayed as activated.

Tip

If there is no storage location specified for operation log data in the JP1/IT Desktop Management setup, the data in the online area of the JP1/IT Desktop Management database is output to the database backup folder during the overwrite installation of JP1/IT Desktop Management 2. The output destination for the data is displayed on the window indicating that setup is complete. To import the data into the JP1/IT Desktop Management 2 operation log database, you need to set the storage location for operation log data in the setup of the JP1/IT Desktop Management 2 management server. Then, import the data manually by copying the following files:

- OPR_CATALOG_*YYYYMMDD*.csv
- OPR_DATA_*YYYYMMDD*.zip
- OPR_OTHER.zip

A version upgrade of an environment where a site server is used

When you use a site server of JP1/IT Desktop Management (JP1/IT Desktop Management - Remote Site Server is installed.), perform the following operation before performing a version upgrade to JP1/IT Desktop Management 2 - Manager. If you do not perform it, you cannot perform ITDM-compatible distribution and collect operation logs.

- Before performing a version upgrade from JP1/IT Desktop Management - Manager to JP1/IT Desktop Management 2 - Manager, change the setting of **Package distribution relay site** and **Storage Location for Operation Logs** from the site server to the management server with the **Server Configuration Settings** window.

Important

If you need to install a relay system on a computer that was being used as a JP1/IT Desktop Management site server (a computer with JP1/IT Desktop Management - Remote Site Server installed), uninstall JP1/IT Desktop Management - Remote Site Server from the computer before installing the relay system.

Settings that cannot be inherited from JP1/IT Desktop Management

If you perform an overwrite installation of JP1/IT Desktop Management 2 on a computer that has JP1/IT Desktop Management installed, the following display items and display order settings are not inherited and are initialized:

- **Security - Computer Security Status - Device List**
- **Assets - Managed Software - Managed Software List - Installed Software**
- **Inventory - Device Inventory - Device List**
- **Inventory - Device Inventory - Device List - Installed Software Detail**
- **Inventory - Software Inventory - Software List**
- **Setting - Discovery - Last Discovery - IP Address Range**

6 Uninstalling products

This chapter describes how to uninstall JP1/IT Desktop Management 2 products.

6.1 Overview of uninstalling the entire system

1. If you are monitoring connection of devices to the network, disable network access control for each network segment.
2. Uninstall the agent on a computer on which an agent is installed.
3. Uninstall the relay system software from computers configured as a relay system.
4. Uninstall Remote Install Manager from the administrator's computer.
5. On the management server, uninstall JP1/IT Desktop Management 2 - Manager.

In addition, if you use the remote control functionality, you must uninstall the controller from the administrator's computer. You can uninstall the controller any time.

If you are using Asset Console to manage assets, you also need to uninstall Asset Console from the relevant computers. You can uninstall Asset Console at any time. For details about uninstalling, see the *JP1/IT Desktop Management 2 - Asset Console Configuration and Administration Guide*.

Furthermore, if you are using the Internet gateway, you also need to uninstall the Internet gateway from the relevant computer. You can uninstall the Internet gateway at any time.

Tip

The remote control agent is uninstalled automatically when the agent is uninstalled.

Tip

To perform uninstallation, use a user account with administrator privileges. After the uninstallation, restart your computer.

Related Topics:

- 6.6 Disabling the network monitor
- 6.4 Procedure for uninstalling the agent
- 6.2 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager
- 6.7 Uninstalling a controller

6.2 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager

If you want to reinstall JP1/IT Desktop Management 2 - Manager, or want to change the management server, uninstall JP1/IT Desktop Management 2 - Manager.

Important

Do not shut down the OS during uninstallation. If you do so, a program might not be uninstalled correctly if it is uninstalled again.

Important

Before installation, make sure that all Windows applications have been closed. If you perform installation without terminating JP1/IT Desktop Management 2 - Manager, restart the OS regardless of whether installation was successful.

To uninstall JP1/IT Desktop Management 2 - Manager:

1. In Windows Control Panel, start **Programs and Features**.
2. Select **JP1/IT Desktop Management 2 - Manager**, and then click the **Change** button.
3. In the wizard for installing **JP1/IT Desktop Management 2 - Manager**, click the **Next** button.
4. In the dialog box for confirming the uninstallation operation, click the **Delete** button.
5. In the dialog box indicating that installation is complete, click the **Complete** button.

JP1/IT Desktop Management 2 - Manager is uninstalled.

Tip

When you uninstall JP1/IT Desktop Management 2 - Manager, you do not need to uninstall the agent on each computer. However, because a computer has resident processes, we recommend that you uninstall the agent if you do not plan to use JP1/IT Desktop Management 2 any more.

Related Topics:

- 6.7 Uninstalling a controller
- 6.8 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager in a cluster system

6.3 Procedure for uninstalling Remote Install Manager

If you want to reinstall Remote Install Manager on the administrator's computer, or to change the computer on which Remote Install Manager is installed, you first need to uninstall Remote Install Manager.

Important

Do not shut down the OS during uninstallation. If you do so, the program might not be uninstalled correctly even if you repeat the uninstallation process.

Important

Before uninstallation, make sure that all Windows applications have been closed.

To uninstall Remote Install Manager:

1. In the Windows Control Panel, open **Programs and Features**.
2. Select JP1/IT Desktop Management 2 - Manager, and then click the **Change** button.
3. In the JP1/IT Desktop Management 2 - Manager installation wizard, click the **Next** button.
4. In the confirmation dialog box, click the **Delete** button.
5. In the window indicating that uninstallation is complete, click the **Complete** button.

This completes the process of uninstalling Remote Install Manager.

6.4 Procedure for uninstalling the agent

Uninstall the agent on a computer on which it is no longer necessary to manage detailed information by using JP1/IT Desktop Management 2. The computers managed online and from which an agent is uninstalled automatically become agentless computers.

To uninstall the agent:

1. In Windows Control Panel, start **Programs and Features**.
2. Select JP1/IT Desktop Management 2 **- Agent**, and then click the **Uninstall** button.
3. In the confirmation dialog box for uninstallation, click the **Yes** button.

The JP1/IT Desktop Management 2 agent is uninstalled.

Delete the device information on computers that are no longer managed by JP1/IT Desktop Management 2 if those computers will be disposed or will be returned due to expiration of the lease period.

Important

If a password is set for the agent, a dialog box for entering the password appears after step 3. Enter the password you set for the applicable agent configuration. The default password is *manager*.

Important

If you are unable to connect to a management server when uninstalling the agent for online management, a dialog box for making sure that you want to continue uninstallation appears. You can specify whether to connect to the management server again, or to continue uninstallation without checking the connection. If you uninstall the agent without connecting to the management server, the management server treats the computer as a computer on which an agent is installed. To manage the computer as an agentless computer, delete the device information, and run device discovery. After running discovery, register the computer again.

If you are uninstalling the agent for offline management, this dialog box does not appear.

6.5 Procedure for uninstalling a relay system

If you no longer need to use a particular system as a relay system, or you want the role to be performed by a different computer, you first need to uninstall the relay system program.

Important

You cannot uninstall the relay system if the network monitor is enabled on the computer. Disable the network monitor on the computer before uninstalling the relay system.

To uninstall a relay system:

1. In the Windows Control Panel, open **Programs and Features**.
2. Select JP1/IT Desktop Management 2 - Agent, and then click the **Uninstall** button.
3. In the confirmation dialog box, click the **Yes** button.
   The relay system program is uninstalled.
4. Restart the computer.

   Important

   If you do not restart the computer after uninstalling the relay system, other applications might lose the ability to access the network.

If the computer will no longer be managed by JP1/IT Desktop Management 2, delete its device information from the management server. This might apply if the computer is being disposed of or will be returned because its lease period has expired.

Important

If the relay system is password-protected, a dialog box prompting you to enter a password appears after step 3. Enter the password set for the agent configuration assigned to the relay system. The default password is `manager`.

Important

If you are unable to connect to the management server while uninstalling the relay system, a confirmation dialog box appears asking if you want to continue the uninstallation process. You can specify whether to try to connect to the management server again, or to continue uninstallation without checking the connection. If you uninstall the relay system without connecting to the management server, the management server will continue to treat the computer as a computer on which an agent is installed. To manage the computer as an agentless computer, delete the associated device information and run device discovery. After running discovery, register the computer again.

Related Topics:

- 6.6 Disabling the network monitor

6.6 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:

- 2.6.2 Enabling the network monitor

6.7 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.

6.8 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager in a cluster system

To uninstall JP1/IT Desktop Management 2 - Manager in a cluster system, uninstall it from the primary server first, and then the standby server.

To uninstall JP1/IT Desktop Management 2 - Manager in a cluster system:

1. Take the service resources of JP1/IT Desktop Management 2 - Manager on the primary server offline.

   For details about the service resources to be taken offline, see the JP1/IT Desktop Management 2 service resource (generic service) row of the table listing the resources that must be registered in groups. You can find the table in 2.10.2 Procedure for creating a resource group on the primary server. The Client access point, and the Storage (shared disk) remain online.

2. On the primary server, uninstall JP1/IT Desktop Management 2 - Manager.

3. Move the owner of the resource group to the standby server.

4. On the standby server, uninstall JP1/IT Desktop Management 2.

This completes the process of uninstallation in a cluster system.

Related Topics:

- 6.2 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager

6.9 Procedure for uninstalling an Internet gateway

To uninstall an Internet gateway from computers, you have to log on to the OS as a user having administrator permissions.

Important

If you uninstall an Internet gateway from a Windows computer that supports User Account Control (UAC), a dialog box requesting elevation of the user permission level might appear. If this dialog box appears, agree to the request.

Important

Do not shut down the OS while during uninstallation. If you do so, the Internet gateway might not be uninstalled properly even if you re-execute the uninstallation process.

Important

Before uninstalling the Internet gateway, shut down all Windows applications.

To uninstall the Internet gateway:

1. Stop the World Wide Web Publishing Service.
2. On the Windows Control Panel, start **Programs and Features**.
3. Select **JP1/IT Desktop Management 2 - Internet Gateway** and then click the **Uninstall** button.
4. In the dialog box asking for your confirmation to uninstall the program, click the **Yes** button.
   The Internet gateway is uninstalled. If a message asking you to restart the computer appears, restart it.

   Note

   If, after clicking the **Yes** button, a window appears notifying you about the presence of files or services that cannot be updated with the setup, it means that the World Wide Web Publishing Service might still be running. Stop the installation process by using the **Cancel** button, and then start again from step 1.
5. Delete the Microsoft Internet Information Services configuration that you have created in (4) Setting up Microsoft Internet Information Services.
6. Cancel the setting that you have specified for the firewall in 2.11.2 Setting up firewalls.

7 Migrating environments

This chapter describes how to migrate the JP1/IT Desktop Management 2 environment.

7.1 Replacing a management server

Replacement of a management server means to use a computer on which JP1/IT Desktop Management 2 - Manager is not installed as the new management server.

The following provides notes on replacing a management server:

Important

The version information of JP1/IT Desktop Management 2 - Manager that will be installed on the new computer and the version information of the product on the old computer must match.

Important

You cannot upgrade JP1/IT Desktop Management 2 - Manager while replacing a management server. Accordingly, install the upgrade before or after replacement.

Important

On a computer running Windows Server 2019, Windows Server 2016 or Windows Server 2012, do not specify the following folders during setup:

- Folders under *system-drive*`:\program files\WindowsApps`
- Folders in storage areas created by virtual provisioning

Important

If the IP address of the new computer is no longer the same as that of the old computer, and you want to change the connection destination of the agent, you need a network configuration in which the new management server and the agent can directly access each other. A network in which direct access is possible means a network in which a host name or an IP address is used for access, and in which the server and the agent can communicate with each other directly via ICMP. In addition, you must be able to pass the TCP protocol port that is used by the management server and the agent.

Important

If you want the management server to inherit the system configuration on the old computer, the IP address of the managed device must match before and after replacement.

For example, if the IP address of the managed computer changes due to a change in the installation location during management server replacement, that computer is not connected to the new management server. If this happens, create an installation set on the new management server to reinstall the agent on the computer. This action connects the computer to the management server.

Important

Manage the database backup on the old computer by using a user ID and password to prevent access by personnel other than the administrator. If an unintended user obtains the backup improperly and then restores it, that user can use the managed devices from the user's management server just as you protect the management server.

Important

If you want to manage devices that were managed on the old management server on the new management server, restore the database you backed up on the old computer on the new computer. If the database is not restored, the agent installed on the managed devices will not be able to connect to the new management server.

If you want to manage new devices on the new management server, you do not need to back up and restore the database. However, if you want to manage the same devices that were managed before replacement, take either of the following actions after replacement:

- For computers on which an agent is installed: Use the installation set you created on the management server after replacement to reinstall the agent.
- For agentless devices: Run discovery to include the devices as managed devices.

Important

If you connect the old management server to a network without uninstalling JP1/IT Desktop Management 2 - Manager, the agent on the new management server cannot be managed correctly.

This is because both of the servers can connect to the agent, and the agent might enter a state that the administrator did not intend because the management servers have given different instructions. In addition, information reported from the agent by connecting to the old management server is not reported to the new management server. As a result, there might be differences in the information managed by the two servers.

7.1.1 Procedure for replacing a management server in a single-server configuration

This subsection describes the procedure for replacing a management server in a single-server configuration. In the procedure described here, you replace a management server by installing JP1/IT Desktop Management 2 - Manager on the replacement-destination computer and by migrating the data from the replacement-source computer. For notes on replacement, see 7.1 Replacing a management server.

To replace a management server in a single-server configuration:

1. Stop the services of JP1/IT Desktop Management 2.

   You must stop the services so that new operation log data reported by the agent after the database is backed up will not be stored.

   From the Windows **Start** menu, select **Administrative Tools**, and then **Services**. In the dialog box that appears, right-click the name of a service, and then select **Stop**. The service will be stopped. Repeat this operation to stop the following services:

- JP1_ITDM2_Agent Control
- JP1_ITDM2_Service
- JP1_ITDM2_Web Container

2. Back up the database.

   On the replacement-source computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Then, start the database manager of JP1/IT Desktop Management 2 - Manager, and back up the database. At least about 20 GB of free space is required on the drive on which the backup folder exists.

3. Save the backup data of the operation log.

   If the system is set to store operation log data, save the backup data that is contained in the *Operation log backup folder* specified during setup.

   To check whether the system is set to store operation log data, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Then, start the setup of JP1/IT Desktop Management 2 - Manager, and then, in the **Operation Log Settings** window, check whether the **Store the operation logs** check box is selected. If the check box is selected, the system is set to store operation log data.

4. Save the backup data of the revision history.

   If the system is set to output revision history archives, save the backup data that is contained in the *Output folder for the revision history* specified during setup.

   To check whether the system is set to store revision history archives, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Then, start the setup of JP1/IT Desktop Management 2 - Manager, and then, in the **Output Settings for Saving the Revision History** window, check whether the **Regularly output and save the revision history** check box is selected. If the check box is selected, the system is set to output revision history archives.

5. On the replacement-destination computer, store the backup data of the operation log.

   If you saved the backup data of the operation log in step 3, before you start installation, store the backup data in the folder that will be specified as the *Operation log backup folder* on the replacement-destination computer. Note that this folder must not contain data other than the backup data of the operation log.

6. On the replacement-destination computer, store the backup data of the revision history.

   If you saved the backup data of the revision history in step 4, before you started installation, store the backup data in the folder that will be specified as the *Output folder for the revision history* on the replacement-destination computer. Note that this folder must not contain data other than the backup data of the revision history.

7. If the IP address and host name of the management server do not change after replacement, disconnect the replacement-source computer from the network.

8. On the replacement-destination computer, install JP1/IT Desktop Management 2 - Manager.

9. Set up JP1/IT Desktop Management 2 - Manager.

   On the replacement-destination computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and perform the setup procedures.

   If the system is set to store operation log data, for the *Operation log backup folder* in the **Automatic Backup Setting for Operation Logs** window, specify the folder in which you stored backup data in step 5.

   If the system is set to output revision history archives, for the *Output folder for the revision history* in the **Output Settings for Saving the Revision History** window, specify the folder in which you stored backup data in step 6.

10. Restore the database by using the data that you backed up in step 2.

On the replacement-destination computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Start the database manager of JP1/IT Desktop Management 2 - Manager, and restore the database.

11. Register the license.

    In the login window of JP1/IT Desktop Management 2 - Manager that has been installed on the replacement-destination computer, click the **License** button. In the dialog box that appears, click the **Register License** button to register the licence.

12. If the IP address or host name of the management server changes after replacement, specify the necessary settings by referring to the following procedures:

    - 7.9.1 Procedure for changing the management server host name
    - 7.9.2 Procedure for changing the management server IP address

13. Confirm that the system operates correctly.

    In the JP1/IT Desktop Management 2 - Manager that has been installed on the replacement-destination computer, check whether the agent is connected to the management server. To do so, in the Inventory module, in the **Device List** window, confirm that the **Last Alive Confirmation Date/Time** value has been updated.

    If **Last Alive Confirmation Date/Time**, which is an item that is not displayed initially, is not displayed, right-click an item in the list of the **Device List** window, and select **Select Columns**. In the dialog box that appears, confirm that the value has been updated. If the **Last Alive Confirmation Date/Time** value has not been updated, on the user's computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Administrator Tool**, and then **Setup**. Then, start the setup of the agent, and check whether the replacement-destination management server has been set as the connection destination.

14. On the replacement-source computer, uninstall JP1/IT Desktop Management 2 - Manager.

Now you have completed replacement of the management server.

Tip

If the backup created on the replacement-source computer becomes unnecessary after replacement, delete the backup.

Tip

If the agent is connected to the management server after replacement, the **Last Alive Confirmation Date/Time** value in the **Device List** window of the Inventory module is updated. If the agent is not connected, on the user's computer, check whether the connection destination has been set correctly by starting the setup of the agent.

Related Topics:

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration
- 2.10.1 Overview of building a cluster system
- 7.1 Replacing a management server

7.1.2 Procedure for replacing a management server in a multi-server configuration

This subsection describes the procedure for replacing a management server in a multi-server configuration. In the procedure described here, you replace a management server by installing JP1/IT Desktop Management 2 - Manager on the replacement-destination computer and by migrating the data from the replacement-source computer. For notes on replacement, see 7.1 Replacing a management server.

Note that the procedure described here can be applied to both replacement of the primary management server and replacement of a management relay server.

To replace a management server in a multi-server configuration:

1. Stop the services of JP1/IT Desktop Management 2.

   You must stop the services so that new operation log data reported from the agent after the database is backed up will not be stored.

   From the Windows **Start** menu, select **Administrative Tools**, and then **Services**. In the dialog box that appears, right-click the name of a service, and then select **Stop**. The service will be stopped. Repeat this operation to stop the following services:

   - JP1_ITDM2_Agent Control
   - JP1_ITDM2_Service
   - JP1_ITDM2_Web Container
   - JP1_ITDM2_Relay Manager Service

2. Back up the database.

   On the replacement-source computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Then, start the database manager of JP1/IT Desktop Management 2 - Manager, and back up the database. At least 20 GB of free space is required on the drive where the backup folder exists.

3. Save the backup data of the operation log.

   If the system is set to store operation log data, save the backup data that is contained in the *Operation log backup folder* specified during setup.

   To check whether the system is set to store operation log data, from the Windows **Start**menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and then, in the **Operation Log Settings** window, check whether the **Store the operation logs** check box is selected. If the check box is selected, the system is set to store operation log data.

4. Save the backup data of the revision history.

   If the system is set to output revision history archives, save the backup data that is contained in the *Output folder for the revision history* specified during setup.

   To check whether the system is set to store revision history archives, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and then, in the **Output Settings for Saving the Revision History** window, check whether the **Regularly output and save the revision history** check box is selected. If the check box is selected, the system is set to output revision history archives.

5. Back up the following file:

   Windows-installation-folder\jdnagent.nid

6. On the replacement-destination computer, store the backup data of the operation log.

If you saved the backup data of the operation log in step 3, before you start installation, store the backup data in the folder that will be specified as the *Operation log backup folder* on the replacement-destination computer. Note that this folder must not contain data other than the backup data of the operation log.

7. On the replacement-destination computer, store the backup data of the revision history.

   If you saved the backup data of the revision history in step 4, before you start installation, store the backup data in the folder that will be specified as the *Output folder for the revision history* on the replacement-destination computer. Note that this folder must not contain data other than the backup data of the revision history.

8. If the IP address and host name of the management server do not change after replacement, disconnect the replacement-source computer from the network.

9. On the replacement-destination computer, install JP1/IT Desktop Management 2 - Manager as a custom installation.

10. Store the jdnagent.nid file that you backed up in step 5 in *Windows-installation-folder* on the replacement-destination computer.

11. Use a text editor to create the inventory configuration file (jdng_inventory.conf) that contains the following entries, and place the file in the %ALLUSERSPROFILE%\HITACHI\jp1itdma\conf folder:

    ```
    [NodeID]
    ReproductionLimit=0
    ```

12. Set up JP1/IT Desktop Management 2 - Manager.

    On the replacement-destination computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and perform the setup procedure.

    If you are replacing a management relay server with a new one, make sure that the new management relay server connects to the same upper management server to which the current management relay server connects.

    If the system is set to store operation log data, for the *Operation log backup folder* in the **Automatic Backup Setting for Operation Logs** window, specify the folder in which you stored backup data in step 6.

    If the system is set to output revision history archives, for the *Output folder for the revision history* in the **Output Settings for Saving the Revision History** window, specify the folder in which you stored backup data in step 7.

13. Restore the database by using the data that you backed up in step 2.

    On the replacement-destination computer, from the Windows **Start**menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Start the database manager of JP1/IT Desktop Management 2 - Manager, and perform restoration of the database.

14. If the product licenses are managed on the individual management servers, execute the `distributelicense` command on the primary management server to set the product license information on the management relay servers.

15. If the server you are replacing is the primary management server or a management relay server that is allowed to register licenses, register the license on the new (replacement-destination) management server.

    In the login window of JP1/IT Desktop Management 2 - Manager that has been installed on the replacement-destination computer, click the **License** button. In the dialog box that appears, click the **Register License** button to register the licence.

16. If the IP address or host name of the management server changes after replacement, specify the necessary settings by referring to the following procedures

    - 7.9.1 Procedure for changing the management server host name
    - 7.9.2 Procedure for changing the management server IP address

17. Confirm that the system operates correctly.

    In JP1/IT Desktop Management 2 - Manager that has been installed on the replacement-destination computer, check whether the agent is connected to the management server. To do so, in the Inventory module, in the **Device List** window, confirm that the **Last Alive Confirmation Date/Time** value has been updated.

    If **Last Alive Confirmation Date/Time**, which is an item that is not displayed initially, is not displayed, right-click an item in the list of the **Device List** window, and select **Select Columns**. In the dialog box that appears, confirm that the value has been updated. If the **Last Alive Confirmation Date/Time** value has not been updated, on the user's computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Administrator Tool**, and then **Setup**. Start setup of the agent, and check whether the replacement-destination management server has been set as the connection destination.

18. On the replacement-source computer, uninstall JP1/IT Desktop Management 2 - Manager.

Now you have completed replacement of the management server.

Tip

If the backup created on the replacement-source computer becomes unnecessary after replacement, delete the backup.

Tip

If the agent is connected to the management server after replacement, the **Last Alive Confirmation Date/Time** value in the **Device List** window of the Inventory module is updated. If the agent is not connected, on the user's computer, check whether the connection destination has been set correctly by starting the setup of the agent.

Related Topics:

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration
- 7.1 Replacing a management server
- 8.11 distributelicense (distributing licenses)

7.2 Procedure for changing the server role from management server in a single-server configuration to primary management server in a multi-server configuration

To change the server role from management server in a single-server configuration to primary management server in a multi-server configuration, start **Setup**, and then, in the **Select the Server Configuration** window, select **Multi-server configuration**.

To change the server role from management server in a single-server configuration to primary management server in a multi-server configuration:

1. Log on 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 **Setup**.
3. In the setup window that appears, click the **Next** button.
4. In the **Select a Setup** window, select **Modify settings**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Select the Server Configuration** window appears.
6. From **Server Configuration**, select **Multi-server configuration**.
7. Continue to click the **Next** button until the **Confirm Setup Settings** window appears.
8. In the **Confirm Setup Settings** window, confirm the specified settings, and then click the **Next** button.
9. In the **Setup for Distribution by Using Remote Install Manager** window that appears, click the **OK** button.
   Setup starts, and a dialog box indicating that processing is in progress appears. When setup ends, the **Setup has Completed** window appears.
   If there is a need to stop services, a dialog box to confirm that services will be stopped appears. Click the **OK** button to stop the services.
10. In the **Setup has Completed** window, click the **OK** button.

Now you have changed the server role from management server in a single-server system to primary management server in a multi-server system.

> **Tip**
>
> If you want to upgrade the version of JP1/IT Desktop Management 2 - Manager when changing the role of the management server, upgrade the version, and then change the server configuration.

Related Topics:

- 5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management 2 - Manager

7.3 Procedure for changing the server role from management server to management relay server

You can change the server role from either management server in a single-server system or primary management server in a multi-server system to management relay server in a multi-server system. To do so, overwrite-install JP1/IT Desktop Management 2 - Manager by selecting **Management relay server** as the **Type of Manager to Install**. Then, specify the upper management server to which the management relay server is to be connected.

> **Tip**
>
> You cannot change the management server in a cluster environment or a computer on which JP1/IT Desktop Management 2 - Agent is installed, to a management relay server.
>
> Note that you cannot change the Manager type when overwrite-installing a management relay server.

To change the server role from management server to management relay server:

1. On the management server that you want to change to a management relay server in a multi-server system, overwrite-install JP1/IT Desktop Management 2 - Manager. At this time, make sure that you install the same version of JP1/IT Desktop Management 2 - Manager that has already been installed on each server in the multi-server system.
   Also make sure that you select **Management relay server** as the **Type of Manager to Install** when performing overwrite installation.
2. Specify the upper management server to which the management relay server is to be connected.

Now you have changed the server role from either the management server in a single-server system or the primary management server in a multi-server system to a management relay server in a multi-server system.

> **Tip**
>
> If you want to upgrade the version of JP1/IT Desktop Management 2 - Manager when changing the role of the management server, upgrade the version, and then change the type of Manager.

> **Tip**
>
> This tip applies when you change the management server in a single-server system to a management relay server in a multi-server system. In this case, on the primary management server in the multi-server system, you can register the product licenses that were registered on the management server in the single-server system. Note that if you want to manage product licenses on individual management relay servers in a multi-server system, execute the `distributelicense` command on the primary management server to set the product license information on each management relay server.

Related Topics:

- 1.3.3 Procedure for setting product license information for a management relay server
- 5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management 2 - Manager
- 3.6 Procedure for changing the higher connection destination settings of a management relay server
- 5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management 2 - Manager

7.4 Replacing a computer with only Remote Install Manager installed

To replace a computer with Remote Install Manager installed:

1. If needed, uninstall Remote Install Manager from the computer being replaced.
2. Replace the computer.
3. On the new computer, install Remote Install Manager.
   Select **Custom installation** as the installation type, and **Remote Install Manager** as the component to install. Because you do not need to install the Manager, select **This feature will not be available.** from the pull-down menu for **Manager**.

This completes the process of replacing a computer with Remote Install Manager installed.

Related Topics:

- 1.9.1 Procedure for installing Remote Install Manager only

7.5 Procedure for replacing computers on which an agent is installed

To replace a computer on which an agent is installed:

1. Uninstall the agent from the computer.
2. Replace the computer.
3. Install the agent on the replaced computer.

Replacement of the computer on which an agent is installed is complete.

7.6 Procedure for replacing relay systems

Replacing a relay system means to migrate the functionality of an existing computer that is functioning as a relay system to another computer.

To replace a relay system, you need to back up the information on the computer being replaced, and restore it to the new computer.

To back up information on the computer being replaced:

1. On the relay system you are replacing, stop the relay system service.

   In **Control Panel** - **Administrative Tools** - **Services**, stop the Agent service (JP1_ITDM2_Agent Service). Note that the Agent service can be stopped only for the relay system.

2. Make sure that the processes below have stopped.

   When you stop the agent service, the following processes stop. Using Task Manager or similar tools, make sure that the following processes are not displayed. If any process is still displayed, then the process is still running, so wait until the process ends and the display disappears.

   - `jdngdmpsetup.exe`
   - `jdngwinst.exe`
   - `jdngsite.exe`
   - `jdngschserv.exe`
   - `jdngsrvmain.exe`

3. On the relay system being replaced, back up the following registry entries:

   The back up of the registry can be performed by launching the OS feature Registry Editor and exporting the registry entries.

   For 32-bit operating systems:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\JP1/IT Desktop Management - Agent\DMP
   ```

   For 64-bit operating systems:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\JP1/IT Desktop Management
   - Agent\DMP
   ```

4. Back up the following files:

   Manually back up the files and folders under the following path.

   - Files under *relay-system-installation-folder*`\MASTER\DB`
   - Files under *relay-system-installation-folder*`\SCHEDULE`
   - Files under *relay-system-installation-folder*`\SERVER`
   - Files under *relay-system-installation-folder*`\SITESRV`
   - Files under *relay-system-installation-folder*`\DMPSITE\\COLLECTION`
   - *Windows-installation-folder*`\jdnagent.nid`

The information on the relay system being replaced is backed up.

To restore the backed-up information to the new computer:

1. Install the relay system program on the new computer.

When the installation process is complete, the Setup window appears.

2. In the Setup window, click the **Cancel** button.

3. Stop the relay system service on the new computer.

   In **Control Panel** - **Administrative Tools** - **Services**, stop the Agent service (JP1_ITDM2_Agent Service). Note that the Agent service can be stopped only for the relay system.

4. Make sure that the processes below have stopped.

   When you stop the agent service, the following processes stop. Using Task Manager or similar tools, make sure that the following processes are not displayed. If any process is still displayed, then the process is still running, so wait until the process ends and the display disappears.

   - `jdngdmpsetup.exe`
   - `jdngwinst.exe`
   - `jdngsite.exe`
   - `jdngschserv.exe`
   - `jdngsrvmain.exe`

5. Restore the backup information to the new computer.

   Restore file information and registry backed up before replacement. The file information is restored to the same location as the backed up folder. You can restore the registry by starting up the OS feature Registry Editor and importing the backup file.

6. Using a text editor, create an inventory settings file (`jdng_inventory.conf`) with the following content, and place it in the `%ALLUSERSPROFILE%\HITACHI\jp1itdma\conf` folder.

   ```
   [NodeID]
   ReproductionLimit=0
   ```

7. Set up the relay system on the new computer.

   For setup, start setup from **JP1_IT Desktop Management 2 - Agent - Administrator Tool** in the start menu. After setup starts, enter **Host Name or IP Address** and **Port Number** of **Management Server**, and click the **OK** button.

8. Log off from the relay system computer, and then log in again.

This completes the process of replacing the relay system.

> **Important**
>
> On agents for which the old computer is specified as the higher system, you will need to change the higher system to the new relay system in the **Basic Settings** view of the agent configuration.

Related Topics:

- 1.8.1 Installing a relay system
- 1.8.2 Procedure for installing a relay system from supplied media
- 1.8.3 Procedure for setting up a relay system
- 6.5 Procedure for uninstalling a relay system

7.7 Procedure for replacing computers for which network access control is enabled

Before replacing a computer for which network access control is enabled, you must disable network access control first. For details about how to disable and enable network access control, see 6.6 Disabling the network monitor, and 2.6.2 Enabling the network monitor.

To replace a computer for which network access control is enabled:

1. Disable network access control on the old computer.
2. Uninstall the agent from the old computer.
3. Replace the computer.
4. Install the agent on the new computer.
5. Enable network access control on the new computer.

The replacement of a computer for which network access control is enabled is complete.

7.8 Replacing the Internet gateway

To replace the Internet gateway:

> **Important**
>
> The IP address and host name of the Internet gateway must be the same before and after replacement.

1. Stop the World Wide Web Publishing Service.
2. Uninstall the agent from the computer.
3. If a relay system has been installed on the Internet gateway, back up computer information before replacement.
   For details, see 7.6 Procedure for replacing relay systems.
4. Build an Internet gateway on the new computer.
   For details, see 2.11.1 Building an Internet gateway.
5. If you are installing a relay system on the Internet gateway after replacement, restore the computer information you have backed up in step 3.
   For details, see 7.6 Procedure for replacing relay systems.

The replacement of the Internet gateway is now completed.

7.9 Changing host names and IP addresses in the system configuration

7.9.1 Procedure for changing the management server host name

If you change the host name of the management server, you will need to set the following items again:

- Connection destination of a management relay server under the local server (if the host name is specified as the connection destination in a multi-server configuration)
- Agent connection destinations (when specified by host name)
- Connection destination in the login window of Remote Install Manager (when specified by host name)
- The Asset Console data source

> **Important**
>
> If you changed the host name of the management relay server, restart the computer, start Remote Install Manager, and then make sure that the host name in the system configuration information of the relevant PC has been changed. If the host name has not been changed, delete the system configuration information of the PC, wait a while, and then make sure that the system configuration information is registered by the changed host name.

Connection destination of a management relay server under the local server (if the host name is specified as the connection destination in a multi-server configuration)

On the target management relay server under the local server, start the setup, and then, in **Management Relay Server Settings**, set the new host name for **Host name or IP address**. For details about the procedure, see 3.6 Procedure for changing the higher connection destination settings of a management relay server.

The connection-destination host name of the management relay server under the local server is changed.

Agent connection destinations (when specified by host name)

1. Change the setting according to the method the agent uses to connect to the higher system.

   If you use a file for connection destinations (`itdmhost.conf`) to define connections to higher systems, edit the file for connection destinations (`itdmhost.conf`) on the agent.

   If you use an information file for higher connection destinations (`dmhost.txt`) to define connections to higher systems, edit the information file for higher connection destinations on the agents.

   If you use a file for higher system addresses (`SERVERIP.ini`), edit the file for higher system addresses on the agents.

   > **Tip**
   >
   > For details about changing the setting files, see the following:
   >
   > The file for connection destinations (`itdmhost.conf`)
   >
   > *(2) Creating the file for connection destinations (itdmhost.conf)*
   >
   > The information file for higher connection destinations (`dmhost.txt`)
   >
   > The description of creating an information file for higher connection destinations (`dmhost.txt`) in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

The file for higher system addresses (`SERVERIP.ini`)

The description of format of file for higher system addresses in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

2. Under **Management Server** in the **Basic Settings** area of the agent configuration, specify the new host name in **Host name or IP address**.

   If a computer is not running when you change the agent configuration, you will need to change the setting for that agent individually in the Setup window.

The connection destination of the agent is changed.

Connection destination in the login window of Remote Install Manager (when specified by host name)

If a host name is specified in the **Management server** field of the login window of Remote Install Manager, change it to the new host name.

Asset Console data source

In the Setup window for Asset Console, use the following procedure to re-create the data source:

1. Start server setup.
2. Click **Create Data Source**.
3. In the **Products for connection** area, select **JP1/Desktop Management 2 - Manager** and then click the **Next** button.
4. If a host name is set in the **Server** field, replace it with the new host name.
5. Click the **OK** button.

The Asset Console data source is re-created.

7.9.2 Procedure for changing the management server IP address

If you change the IP address of the management server, you will need to set the following items again:

- Connection destination of a management relay server under the local server (if the IP address is specified as the connection destination in a multi-server configuration)
- Agent connection destinations (when specified by IP address)
- Exception connection for devices denied network access
- Connection destination in the login window of Remote Install Manager (when specified by IP address)
- The Asset Console data source

Important

If you changed the IP address of the management relay server, restart the computer, start Remote Install Manager, and then make sure that the IP address in the system configuration information of the relevant PC has been changed. If the IP address has not been changed, delete the system configuration information of the PC, wait a while, and then make sure that the system configuration information is registered by the changed IP address.

To change the IP address of the management server:

1. Stop any processing in progress in the Asset Console and Remote Install Manager.
2. On the management server, execute the `stopservice` command to stop services.#

   #: When changing to an IP address that was already valid when the management server service started, stopping the management server service is not needed.
3. Start JP1/IT Desktop Management 2 - Manager setup, and in the **Database Settings** view, replace the IP address used for database access with the new IP address. Then, perform the setup process.

The IP address for the management server is changed. Next, set the items as follows:

Connection destination of a management relay server under the local server (if the IP address is specified as the connection destination in a multi-server configuration)

On the target management relay server under the local server, start the setup, and then, in **Management Relay Server Settings**, set the new IP address for **Host name or IP address**. For details about the procedure, see 3.6 Procedure for changing the higher connection destination settings of a management relay server.

The connection-destination IP address of the management relay server under the local server is changed.

Agent connection destinations (when specified by IP address)

1. Change the setting according to the method the agent uses to connect to the higher system.

   If you use a file for connection destinations (`itdmhost.conf`) to define connections to higher systems, edit the file for connection destinations (`itdmhost.conf`) on the agent.

   If you use an information file for higher connection destinations (`dmhost.txt`) to define connections to higher systems, edit the information file for higher connection destinations on the agents.

   If you use a file for higher system addresses (`SERVERIP.ini`), edit the file for higher system addresses on the agents.

   Tip

   For details about changing the setting files, see the following:

   The file for connection destinations (`itdmhost.conf`)

   (2) Creating the file for connection destinations (itdmhost.conf)

   The information file for higher connection destinations (`dmhost.txt`)

   The description of creating an information file for higher connection destinations (`dmhost.txt`) in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

   The file for higher system addresses (`SERVERIP.ini`)

   The description of format of file for higher system addresses in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*
2. Under **Management server** in the **Basic Settings** area of the agent configuration, specify the new IP address in **Host name or IP address**.

   If a computer is off when you change the agent configuration, you will need to change the setting for that agent individually in the Setup window.

The connection destination of the agent is changed.

Exception connection for devices denied network access

In the **Network Access Control Settings** view, remove the old IP address of the management server from the **Exclusive Communication Destination for Access-Denied Devices** area, and add the new IP address.

Connection destination in the login window of Remote Install Manager (when specified by IP address)

If an IP address is specified in the **Management server** field of the login window of Remote Install Manager, change it to the new IP address.

Asset Console data source

In the Setup window for Asset Console, use the following procedure to re-create the data source:

1. Start server setup.
2. Click **Create Data Source**.
3. In the **Products for connection** area, select **JP1/Desktop Management 2 - Manager** and then click the **Next** button.
4. If an IP address is set in the **Server** field, replace it with the new IP address.
5. Click the **OK** button.

The Asset Console data source is re-created.

7.9.3 Procedure for changing the host name or IP address of a relay system

To change the host name or IP address of a relay system:

1. Delete any jobs that are in progress in Remote Install Manager.
   Delete all jobs that pass through the relay system whose host name or IP address you are changing.
2. Change the host name or IP address of the relay system.
3. In the **Device List** view and in the **System Configuration** window of Remote Install Manager, make sure that the host name or IP address has changed.
4. Change the connection destinations of agent devices that connect to the relay system whose host name or IP address you changed.
   In the Settings module, select **Windows Agent Configurations and Create Agent Installers**, and click the **Edit** button for the agent configuration applied to agents that connect to the relay system whose host name or IP address you changed.
   In the displayed agent configuration, in the **Higher System for Distribution that Uses Remote Install Manager** area under **Basic settings**, specify the new host name or IP address in **Host name or IP address**.

This completes the process of changing the host name or IP address of the relay system.

7.9.4 Procedure for changing logical host names in a cluster system

To change the logical host name of a cluster system, change the host name in the Setup window and then set the following items again:

- Agent connection destinations (when specified by host name)
- Connection destination in the login window of Remote Install Manager (when specified by host name)
- The Asset Console data source

To change the logical host name of a cluster system:

1. Stop any processing in progress in the Asset Console and Remote Install Manager.
2. Take the resources listed in 2.10.2 Procedure for creating a resource group on the primary server offline.
3. In the setup for the primary server, replace the logical host name in the **Cluster Environment** view with the new host name. Then, perform the setup process.
4. Copy the following setup file output during the setup process to the standby server:
   JP1/IT-Desktop-Management-2-Manager-installation-folder`\mgr\conf\jdn_manager_setup.conf`
5. Transfer the ownership of the resource group to the standby server.
6. Initiate the setup process on the standby server, and perform the setup process specifying the setup file you copied in step 4.
7. Transfer the ownership of the resource group back to the primary server.
8. Place the resources listed in 2.10.2 Procedure for creating a resource group on the primary server online.

The logical host name of the cluster system is changed. Next, set the following items again:

Agent connection destinations (when specified by host name)

1. Change the setting according to the method the agent uses to connect to the higher system.
   If you use a file for connection destinations (`itdmhost.conf`) to define connections to higher systems, edit the file for connection destinations (`itdmhost.conf`) on the agent.
   If you use an information file for higher connection destinations (`dmhost.txt`) to define connections to higher systems, edit the information file for higher connection destinations on the agent.
   If you use a file for higher system addresses (`SERVERIP.ini`), edit the file for higher system addresses on the agent.

> **Tip**
>
> For details about changing the setting files, see the following:
>
> The file for connection destinations (`itdmhost.conf`)
>
> *(2) Creating the file for connection destinations (itdmhost.conf)*
>
> The information file for higher connection destinations (`dmhost.txt`)
>
> The description of creating an information file for higher connection destinations (`dmhost.txt`) in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

The file for higher system addresses (`SERVERIP.ini`)

The description of format of file for higher system addresses in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

2. Under **Management server** in the **Basic Settings** area of the agent configuration, specify the new host name in **Host name or IP address**.

   If a computer is off when you change the agent configuration, you will need to change the setting for that agent individually in the Setup window.

The connection destination of the agent is changed.

Connection destination in the login window of Remote Install Manager (when specified by host name)

If a host name is specified in the **Management server** field of the login window of Remote Install Manager, change it to the new host name.

The Asset Console data source

In the Setup window for Asset Console, use the following procedure to re-create the data source:

1. Start server setup.
2. Click **Create Data Source**.
3. In the **Products for connection** area, select**JP1/Desktop Management 2 - Manager** and then click the **Next** button.
4. If a host name is set in the **Server** field, replace it with the new host name.
5. Click the **OK** button.

The Asset Console data source is re-created.

7.9.5 Procedure for changing logical IP addresses in a cluster system

To change the logical IP address of a cluster system, change the host name in the Setup window and then set the following items again:

- Agent connection destinations (when specified by IP address)
- Exception connection for devices denied network access
- Connection destination in the login window of Remote Install Manager (when specified by IP address)
- The Asset Console data source

To change the logical IP address of a cluster system:

1. Stop any processing in progress in the Asset Console and Remote Install Manager.
2. Take the resources listed in 2.10.2 Procedure for creating a resource group on the primary server offline.
3. In the setup for the primary server, replace the logical IP address in the **Cluster Environment** view with the new IP address. Then, perform the setup process.
4. Copy the following setup file output during the setup process to the standby server:

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

5. Transfer the ownership of the resource group to the standby server.
6. Initiate the setup process on the standby server, and perform the setup process specifying the setup file you copied in step 4.
7. Transfer the ownership of the resource group back to the primary server.
8. Place the resources listed in 2.10.2 Procedure for creating a resource group on the primary server online.

The logical IP address of the cluster system is changed. Next, set the following items again:

Agent connection destinations (when specified by IP address)

1. Change the setting according to the method the agent uses to connect to the higher system.

   If you use a file for connection destinations (itdmhost.conf) to define connections to higher systems, edit the file for connection destinations (itdmhost.conf) on the agent.

   If you use an information file for higher connection destinations (dmhost.txt) to define connections to higher systems, edit the information file for higher connection destinations on the agent.

   If you use a file for higher system addresses (SERVERIP.ini), edit the file for higher system addresses on the agent.

   Tip

   For details about changing the setting files, see the following:

   The file for connection destinations (itdmhost.conf)

   (2) Creating the file for connection destinations (itdmhost.conf)

   The information file for higher connection destinations (dmhost.txt)

   The description of creating an information file for higher connection destinations (dmhost.txt) in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

   The file for higher system addresses (SERVERIP.ini)

   The description of format of file for higher system addresses in the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*

2. Under **Management server** in the **Basic Settings** area of the agent configuration, specify the new IP address in **Host name or IP address**.

   If a computer is off when you change the agent configuration, you will need to change the setting for that agent individually in the Setup window.

The connection destination of the agent is changed.

Exception connections for devices denied network access

In the **Network Access Control Settings** view, remove the old IP address of the management server from the **Exclusive Communication Destination for Access-Denied Devices** area, and add the new IP address.

Connection destination in the login window of Remote Install Manager (when specified by IP address)

If an IP address is specified in the **Management server** field of the login window of Remote Install Manager, change it to the new IP address.

The Asset Console data source

In the Setup window for Asset Console, use the following procedure to re-create the data source:

1. Start server setup.
2. Click **Create Data Source**.
3. In the **Products for connection** area, select **JP1/Desktop Management 2 - Manager** and then click the **Next** button.
4. If an IP address is set in the **Server** field, replace it with the new IP address.
5. Click the **OK** button.

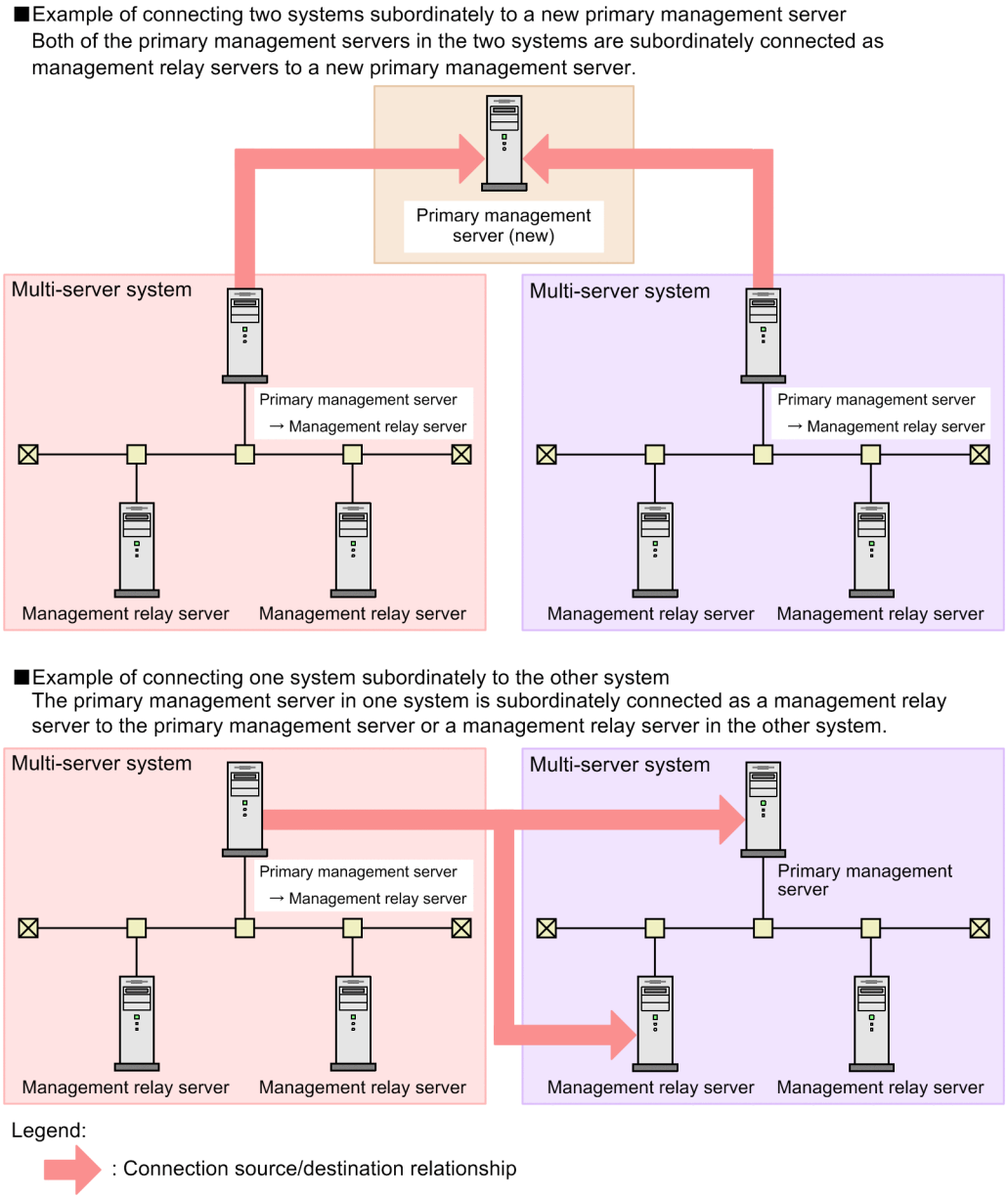
The Asset Console data source is re-created.

7.10 Procedure for merging multi-server systems

The following shows the methods you can use to merge two multi-server systems:

- Add a new primary management server, and connect the existing two multi-server systems subordinately to it, changing the primary management servers of both systems to management relay servers.
- Connect one multi-server system subordinately to the other system, changing the primary management server of the subordinate system to a management relay server.

The following figure shows examples of merging multi-server systems.



The following describes the procedure for merging multi-server systems.

To merge multi-server systems:

1. If you choose to add a new primary management server, on the computer on which you want to use as that server, install JP1/IT Desktop Management 2.

2. On the management relay server or servers (former primary management server or servers), overwrite-install JP1/IT Desktop Management 2.

3. On the new primary management server, register the product licenses that have been registered on the management relay server or servers (former primary management server or servers).

4. On the management relay server or servers (former primary management server or servers), set the higher connection destination.

   On the management relay server or servers (former primary management server or servers), from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and then perform setup.

5. Confirm that the management relay server or servers (former primary management server or servers) are connected subordinately to the higher connection destination set in step 4.

   You can check the hierarchical structure of the multi-server system by using the **Status of management servers under the local server** tab in the Home module of the higher connection destination set in step 4.

6. If you want to manage the product licenses on individual management servers in the new (merged) multi-server system, on the primary management server of the system, execute the `distributelicense` command to set the product license information on each management relay server.

7. If you want to use Remote-Installation-Manager-based distribution in the new (merged) multi-server system, on the server that was set as the higher connection destination in step 4 and its higher management servers, use Remote Install Manager to execute the *Get system configuration information* job for the management relay server or servers (former primary management server).

   For details about job creation and execution by using Remote Install Manager, see the description of job creation in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

8. From the management relay server or servers (former primary management server or servers), report all device information to the higher management server.

   To report all device information to the higher management server, in the Inventory module, select **Device Inventory**, and then **Device List**. In the window that appears, from **Action**, select **Report all Device Details to the Higher Management Server**.

   > **Important**
   >
   > Do not update the device information on a management relay server (former primary management server) by using the operation window or commands while device information is being reported to the higher management server. If you do so, the device information between the servers becomes inconsistent. You can check whether all device information has been reported from an event that will be output in the Events module of the management relay server (former primary management server).

9. If the destination of the device information in step 8 is a management relay server, use the procedure in step 8 to report the device information to each higher management server until it reaches the primary management server.

10. If necessary, on the server specified as the higher connection destination in step 4, review the settings of JP1/IT Desktop Management 2.

Related Topics:

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 1.2.3 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management relay server)

- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration
- 1.2.5 Procedure for setting up a management relay server
- 1.3.3 Procedure for setting product license information for a management relay server
- 8.7 startservice (starting services)
- 8.11 distributelicense (distributing licenses)

7.11 Procedure for switching the higher connection destination of a management relay server

To switch the higher connection destination of a management relay server to another management server in a multi-server configuration, perform setup again. The following shows the procedure for switching the higher connection destination of a management relay server.

To switch the higher connection destination of a management relay server:

1. On the target management relay server, start setup to switch the higher connection destination.

   On the target management relay server, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and then perform the setup procedure.

2. Make sure that the target management relay server is connected subordinately to the new higher connection destination setup in step 1.

   On the server that you set as the higher connection destination in step 1, you can check the hierarchical structure of the multi-server system in the **Status of management servers under the local server** tab of the Home module.

3. If the product licenses are managed on individual management servers, on the primary management server, execute the `distributelicense` command to set the product license information for each management relay server.

4. If you want to use Remote-Installation-Manager-based distribution, on the server that was set as the higher connection destination in step 1 and its higher management servers, use Remote Install Manager to execute the *Get system configuration information* job for the target management relay server.

   For details about job creation and execution by using Remote Install Manager, see the description of job creation in the *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

5. On the target management server and its lower management servers, if the added management items and software search conditions that were applied from the previous higher management server remain, delete those items and conditions.

   To delete added management items of hardware asset information, in the Settings module, select **Assets**, and then **Asset Field Definitions**. In the window that appears, select the items that you want to delete, and then click the **Remove** button.

   To delete software search conditions, in the Settings module, select **Inventory**, and then **Software Search Conditions**. In the window that appears, select the conditions that you want to delete, and then click the **Remove** button.

6. From the target management server, report all device information to the higher management server.

   To report all device information to the higher management server, in the Inventory module, select **Device Inventory**, and then **Device List**. Then, in the window that appears, from **Action**, select **Report all Device Details to the Higher Management Server**.

   > **Important**
   >
   > Do not update the device information on the target management server by using the operation window or commands while device information is being reported to the higher management server. If you do so, the device information between the servers will be inconsistent. You can check whether all device information has been reported from an event that will be output in the Events module of the target management server.

7. If the destination of the device information in step 6 is a management relay server, use the procedure in step 6 to report the device information to each higher management server until it reaches the primary management server.

8. If necessary, on the server specified as the higher connection destination in step 1, review the settings of JP1/IT Desktop Management 2.

Related Topics:

- 1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management server in a single-server configuration or on a primary management server in a multi-server configuration)
- 1.2.3 Procedure for installing JP1/IT Desktop Management 2 - Manager (on a management relay server)
- 1.2.4 Procedure for setting up a management server in a single-server configuration or the primary management server in a multi-server configuration
- 1.2.5 Procedure for setting up a management relay server
- 1.3.3 Procedure for setting product license information for a management relay server
- 8.7 startservice (starting services)
- 8.11 distributelicense (distributing licenses)

7.12 Procedure for switching the management server to which an agent connects

To switch the management server to which an agent connects:

1. On the management server that you want to switch, in the operation window, 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 for the agent configurations that are assigned to the agent whose connection destination you want to switch.
4. Under **Management server** in the **Basic Settings** area of the **Edit Agent Configuration** dialog box, specify the host name or IP address of the new management server in **Host name or IP address**.

   The value you specify in **Host name or IP address** depends on the item selected in **Settings for Address Resolution** during setup.

   When **Host name** is selected in **Settings for Address Resolution**:

   - Specify a host name.
   - In an environment that uses a DNS server, specify a fully qualified domain name (consisting of the host name followed by a period and then the domain name).
   - If the management server incorporates multiple network adapters that connect to the same segment, specify the name of the host with the highest priority in the binding order in the OS of the management server.

   When **IP address** is selected in **Settings for Address Resolution**:

   - Specify an IP address.

The management server to which the agent connects is changed.

Note that if the network connection information has been set on the previously-connected management server, import that network connection information to the currently-connected management server. For details, see the description of the procedure for importing network connection information in the *JP1/IT Desktop Management 2 Administration Guide*.

> **Important**
>
> Immediately after the management server is changed, the agent configuration that is indirectly assigned to the group is used. Before switching the connection destination, make sure that the appropriate agent configuration is assigned to the group. If necessary, create a group, and then assign the agent configuration. However, device type groups and network groups cannot be created in an operation window. If you want to use such groups, connect the devices that belong to the target groups in advance. Then, after groups are created, assign the agent configuration to each group.

> **Tip**
>
> In operation that uses a connection-destination configuration file (`itdmhost.conf`) for agents, distribute the connection-destination configuration file (`itdmhost.conf`) that you changed, to the connection-destination management server. After the file is distributed, the connection destination server will change when the agent restarts or when agent polling is executed.

7.13 Procedure for switching the connection-destination management server of a specific agent in a multi-server configuration

The agent configurations specified on a managing device include the setting of the connection-destination management server for all agents to which the agent configurations are assigned. Therefore, you can change the connection-destination management server of those agents all at one time by modifying the agent configurations. However, to change the connection-destination management server of only a specific agent, you must perform the agent setup procedure. The following shows the procedure for switching the connection-destination management server of a specific agent (switch-source) to another management server (switch-destination) in a multi-server configuration.

To switch the connection-destination management server of a specific agent in a multi-server configuration:

1. On the switch-destination management server, check the default agent configuration to confirm that the server itself is set as a connection destination of agents.

   To check the default agent configuration, in the Settings module, select **Agent**, and then **Windows Agent Configurations and Create Agent Installers**. Then, in the list box of the window that appears, click the **Edit** button displayed in the default agent configuration column.

2. Log on as an OS user with administrator permissions, to the computer whose connection-destination management server you want to change. Then, start the setup, and change the connection-destination management server of the agent.

   On the target computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Administrator Tool**, and then **Setup** to start the setup of JP1/IT Desktop Management 2 - Agent. Then, specify the necessary settings.

   If the agent is password-protected, a password entry window appears. Enter the appropriate password for the relevant agent configurations. The default password is `manager`.

3. On the switch-destination management server, assign the agent configurations to the agent whose connection-destination management server you switched.

   To assign the agent configurations, in the Settings module, select **Agent**, and then **Windows Agent Configurations Assignment**. Then, in the window that appears, select the computer on which the agent whose connection-destination management server has been switched is installed, and then click the **Assign** button. In the dialog box that appears, select the agent configurations to be assigned.

Note that if the network connection information has been set on the switch-source management server, import that network connection information to the switch-destination management server. Note that if the network connection information has been set on the previously-connected management server, import that network connection information to the currently-connected management server. For details, see the description of the procedure for importing network connection information in the *JP1/IT Desktop Management 2 Administration Guide*.

Related Topics:

- 1.6.10 Procedure for setting up the agent
- 7.12 Procedure for switching the management server to which an agent connects

7.14 Procedure for switching the relay system to which an agent connects

The procedure differs depending on whether you are changing the connection destination for every agent that connects to a relay system, or only for specific agents.

To change the connection destination for every agent that connects to a particular relay system:

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 for the agent configuration whose relay system you want to switch.
4. Under **Higher System for Distribution that Uses Remote Install Manager** in the **Basic Settings** area of the **Edit Agent Configuration** dialog box, specify the host name or IP address of the new relay system in **Host name or IP address**.

   The value you specify in **Host name or IP address** depends on the item selected in **Settings for Address Resolution** during setup.

   When **Host name** is selected in **Settings for Address Resolution**:

   - Specify a host name.
   - In an environment that uses a DNS server, specify a fully qualified domain name (consisting of the host name followed by a period and then the domain name).
   - If the management server incorporates multiple network adapters that connect to the same segment, specify the name of the host with the highest priority in the binding order in the OS of the relay system.

   When **IP address** is selected in **Settings for Address Resolution**:

   - Specify an IP address.

The connection destination is changed for every agent that connects to the relay system.

> **Important**
>
> When you unassign an agent configuration, the default agent configuration is automatically assigned to the device. If you are using ID groups to distribute jobs, assigning the default agent configuration might result in ID group jobs being executed from the management server. When you later assign the appropriate agent configuration to the agent, ID group jobs might also be distributed to the agent from the new relay system.

7.15 Procedure for switching the relay system to which a specific agent connects

To switch the connection destination of only a specific agent that connects to the relay system that is to be switched:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Windows Agent Configurations Assignment**.
3. Select the computer on which the agent whose connection destination is to be switched is located, and then click the **Cancel** button.

   The agent configurations that are assigned to the selected computer are cleared, and the default agent configuration is assigned to the computer, instead.
4. Click the **Assign** button to display the **Windows Agent Configurations Assignment** dialog box, and then assign the agent configurations that include the setting for connecting to the switch-destination relay system.

The relay system to which the selected computer is connected (switch-source) is switched to the new relay system (switch-destination).

> **Important**
>
> When the agent configurations of a computer are cleared, the default agent configuration is automatically assigned to the computer. In an environment in which distribution by ID group is performed, when the default agent configuration is assigned to a computer, the management server of the computer might execute an ID group job. In this case, when the agent configurations are re-assigned, the new connection-destination relay system might also execute an ID group job.

7.16 Procedure for switching the management server to which an Internet gateway

To change the management server to which the Internet gateway is connected:

1. Stop the World Wide Web Publishing Service.
2. From the Window's **Start** menu, select **All programs**, **JP1_IT Desktop Management 2 - Internet Gateway**, and then **Internet Gateway Setup**.
3. In the **IT Desktop Management 2 - Internet Gateway Setup** dialog box, set a higher system for the Internet gateway.
4. Click the **OK** button.
5. Start the World Wide Web Publishing Service.

The management server to which the Internet gateway is connected changes.

7.17 Procedure for switching the large-scale management option

The large-scale management option is to be set when installing JP1/IT Desktop Management 2 - Manager. This subsection describes the procedure for switching the large-scale management option from disabled to enabled.

> **Tip**
>
> The same procedure is also used for switching the large-scale management option from enabled to disabled.
>
> However, if you manage 50,000 devices or more, do not switch the large-scale management option from enabled to disabled.

To switch the large-scale management option from disabled to enabled:

1. Stop the services of JP1/IT Desktop Management 2.

   You must stop the services so that new operation log data reported by the agent after the database is backed up will not be stored.

   From the Windows **Start** menu, select **Administrative Tools**, and then **Services**. In the dialog box that appears, right-click the name of a service, and then select **Stop**. The service will be stopped. Repeat this operation to stop the following services:

   - JP1_ITDM2_Agent Control
   - JP1_ITDM2_Service
   - JP1_ITDM2_Web Container

2. Back up the database for the management server before migration.

   On the computer working as *the management server before migration*, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Then, start the database manager of JP1/IT Desktop Management 2 - Manager, and back up the database. At least about 20 GB of free space is required on the drive on which the backup folder exists.

3. Save the backup data of the operation log.

   If the system is set to store operation log data, save the backup data that is contained in the Operation log backup folder specified during setup.

   To check whether the system is set to store operation log data, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Then, start the setup of JP1/IT Desktop Management 2 - Manager, and then, in the **Operation Log Settings** window, check whether the **Store the operation logs** check box is selected. If the check box is selected, the system is set to store operation log data.

4. Save the backup data of the revision history.

   If the system is set to output revision history archives, save the backup data that is contained in the Output folder for the revision history specified during setup.

   To check whether the system is set to store revision history archives, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Then, start the setup of JP1/IT Desktop Management 2 - Manager, and then, in the **Output Settings for Saving the Revision History** window, check whether the **Regularly output and save the revision history** check box is selected. If the check box is selected, the system is set to output revision history archives.

5. Uninstall JP1/IT Desktop Management 2 - Manager from the computer working as *the management server before migration*.

6. Install JP1/IT Desktop Management 2 - Manager. In the Type of Manager to Install dialog box, select the **For large-scale management**

7. Set up JP1/IT Desktop Management 2 - Manager.

   On the computer working as *the management server after migration*, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**. Start the setup of JP1/IT Desktop Management 2 - Manager, and perform the setup procedures.

   If the system is set to store operation log data, specify the Operation log backup folder before the migration as the Operation log backup folder in the **Automatic Backup Setting for Operation Logs** window.

   If the system is set to output revision history archives, specify the Output folder for the revision history before the migration as the Output folder for the revision history in the **Output Settings for Saving the Revision History** window.

8. Restore the database by using the data that you backed up in step 2.

   On the computer where the management server after migration, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Database manager**. Start the database manager of JP1/IT Desktop Management 2 - Manager, and restore the database.

9. Confirm that the system operates correctly.

   Check whether the agent is connected to the management server after migration. To do so, in the Inventory module, in the **Device List** window, confirm that the **Last Alive Confirmation Date/Time** value has been updated.

   If **Last Alive Confirmation Date/Time**, which is an item that is not displayed initially, is not displayed, right-click an item in the list of the **Device List** window, and select **Select Columns**. In the dialog box that appears, confirm that the value has been updated. If the **Last Alive Confirmation Date/Time** value has not been updated, on the user's computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Agent**, **Administrator Tool**, and then **Setup**. Then, start the setup of the agent, and check whether the management server after migration has been set as the connection destination.

10. Specify the parameters.

    After all the steps here are finished, specify the parameters.

    For details, see the descriptions on the operation method in the large-scale environment in the manual *JP1/IT Desktop Management 2 Administration Guide*.

11. Remove the backup of the database as well as the backup data of the operation log and revision history as necessary.

Tip

- When JP1/IT Desktop Management 2 is upgraded from a version earlier than 12-60, the large-scale management option is disabled.
- When you migrate from JP1/NETM/DM to JP1/IT Desktop Management 2, and if you want to enable the large-scale management option, first migrate your server to a management server with the large-scale management option disabled, and then enable the large-scale management option.

Tip

Settings for the overview of the operation window and the layout of lists are maintained for each login user. Even after switching the large-scale management option, the display settings for the management server before migration will be inherited as they are. If the following display settings do not work in the operation of the management server after migration, you need to modify them manually.

- Layout of panels in the Home module and their settings
- Layout of panels in the dashboard of the Security module and their settings
- Layout of panels in the dashboard of the Assets module and their settings
- Layout of panels in the dashboard of the Inventory module and their settings
- Layout of panels in the dashboard of the Distribution module and their settings
- Maximum number of displayed items per page, items to be displayed in a list, and the display order of list items in various lists

8 Commands used for building-related operations

This chapter describes JP1/IT Desktop Management 2 commands that are used to build a system, change settings, and replace devices.

8.1 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`

8.2 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.

8.3 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:

- 8.1 Executing commands

8.4 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:

- 8.1 Executing commands

8.5 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:

- 8.1 Executing commands

8.6 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:

- 8.1 Executing commands

8.7 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:

- 8.1 Executing commands

8.8 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

  However, when using task scheduler, if the folders or files described above exist, `getlogs` command execution will fail. Therefore, perform the execution after deleting the troubleshooting information.

- 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:

- 8.1 Executing commands

8.9 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:

- 8.1 Executing commands

8.10 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:

- 8.1 Executing commands

8.11 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:

- 8.1 Executing commands

8.12 dmpclint.exe (resetting the information generated by the distribution function that uses Remote Install Manager)

This section describes the `dmpclint.exe` command that resets the information generated by the distribution function that uses Remote Install Manager.

Functionality

When the distribution function that uses Remote Install Manager is executed, information such as the job being executed and distribution history is generated. You can use the `dmpclint.exe` command to reset this information. For example, when you deploy an agent by copying a disk, you can prevent the generated information from being copied to the copy-destination computer by executing the command on the copy-source computer,

Format

```
dmpclint.exe△/ALL
```

Argument

/ALL

This is a required argument. If you omit specifying this argument, the command will not be executed.

Storage location

agent-installation-folder\bin\

Return value

The following table lists the return values of the `dmpclint.exe` command:

Return value	Description
0	The command finished normally.
1	Initialization failed.
2	An invalid argument was specified for the command.
3	The information could not be reset.

Example

The following example shows how to use this command to reset the generated information if the agent installation folder is C:\Program Files\Hitachi\jp1itdma:

```
cd "C:\Program Files\Hitachi\jp1itdma\bin"

start /wait dmpclint.exe /ALL

echo %errorlevel%
```

8.13 checkitdmhost (checking the format of the file for connection destinations)

This section describes the `checkitdmhost` command, which checks whether the file for connection destinations (`itdmhost.conf`) used for automatically setting connection destinations of agents conforms to the required file format.

Functionality

This command checks whether the file format requirements of the file for connection destinations (`itdmhost.conf`) are satisfied.

When you execute this command, the file for connection destinations specified in the argument is checked line by line. The line number of a line with invalid syntax is output in a message. Even if invalid syntax is found, the command continues to check the next line. The command stops checking after the last line. However, if the number of lines with invalid syntax exceeds 100, the command displays a syntax error and stops checking. Note that if another error occurs during the check, the command stops checking to display the error.

In the file for connection destinations, the syntax of a line is determined to be invalid in the following cases:

- A required item is omitted.
- An invalid IP address is specified.
- The value specified for *connection-destination* exceeds the maximum number of characters that can be entered.
- A value other than `netmdm` or `netmdmw` is specified for *connection-type* in the DM section.
- An invalid value is specified for *multicast-distribution-address* in the DM section.
- An item other than the items that can be specified for the line is specified.
- An invalid value is specified for the section name.
- The same section is specified more than once.
  In this case, the items in the duplicate sections are still checked.
- No section is specified.
- Either the ITDM section or the DM section is specified, but not both.

A line specified as follows is not handled as invalid, but all or part of the line is ignored:

- Any text following a semicolon
  Such text is handled as a comment.
- A line containing only a line break
- Single-byte spaces at the beginning or end of an item

Execute this command on the management server.

Format

```
checkitdmhostΔ-iΔinput-file-name
```

Argument

-i

Use an absolute path of 200 bytes or less to specify the file for connection destinations (`itdmhost.conf`) whose format you want to check.

Storage location

JP1/IT Desktop Management 2-installation-folder\mgr\bin\

If you use the command prompt provided by JP1/IT Desktop Management 2, you can execute this command without having to specify where the executable file is stored.

Return values

The following table shows the return values of the `checkitdmhost` command.

Return value	Description
0	The command finished normally.
11	The command argument syntax is invalid.
12	An access error for the specified file for connection destinations occurred.
13	The name of the specified file for connection destinations is invalid.
80	The format of the specified file for connection destinations is invalid.
101	Command execution failed due to insufficient memory.
150	Command execution was interrupted due to some other error.

Example

In the following example, the command is being used to check the format of the file for connection destinations in `C:\work1\`.

```
checkitdmhost -i C:\work1\itdmhost.conf
```

9 Troubleshooting

This chapter describes how to deal with the problems that might occur when building a JP1/IT Desktop Management 2 system.

9.1 Overview of troubleshooting during building of an environment

Use the following procedure when a problem occurs while you are building server and agent environments:

1. Check the error message.
   Check the error message output to the log file.

   Tip

   You can also check the error message from the dialog box reporting the error.

2. Check the cause of the problem and the suggested action, and then take corrective action.
   In the message output to the log file, check the cause of the problem and the action to take, and then correct the problem.

You will be able to resolve the problem that has occurred.

Message output format

The following are the formats of the messages that are output:

- KDEX*nnnn-Zmessage-text*
- KFPH*nnnnn-Zmessage-text*

The message ID indicates the following:

K
: This is the system identifier.

DEX
: Indicates that the message is a JP1/IT Desktop Management 2 message (databases excepted).

FPH
: Indicates that the message is related to JP1/IT Desktop Management 2 databases.

nnnn
: Indicates a serial number identifying the message. The serial numbers of messages related to JP1/IT Desktop Management 2 databases have five digits.

Z
: Indicates the following message type as follows:

  - E: Error message
  - W: Warning message
  - I: Informational message
  - Q: Message that requires a user response

Related Topics:

- 9.2 Troubleshooting when building a minimal configuration system
- 9.2.1 Troubleshooting during building of a management server
- 9.2.2 Troubleshooting during agent installation
- 9.4 Troubleshooting during building of an agentless configuration system

9.2 Troubleshooting when building a minimal configuration system

You cannot find any devices even when you run discovery.

If you cannot find any devices connected to the network even when you run discovery, select **Discovery** and then **Configurations** in the Settings module to make sure the IP address range and authentication information settings are correct.

Communication between managed devices and the management server is not possible.

If you install an agent on a managed device by using supplied media, agent setup information is not set automatically. Make sure the setup information has been set. If it has been set, check the following:

- In the setup information of the agent that is installed on the managed device, make sure that the connection destination management server name and the port number settings are correct.
- In the management server setup information, make sure that the port number setting is correct.

9.2.1 Troubleshooting during building of a management server

If you cannot install JP1/IT Desktop Management 2 - Manager on the management server, make sure of the following:

- The OS supports JP1/IT Desktop Management 2 - Manager.
- You have logged on to Windows as a user account with Administrative privileges.

If necessary, you can obtain troubleshooting information during installation by using the `getinstlogs` command. For details about the `getinstlogs` command, see 8.9 getinstlogs (collecting troubleshooting information about installation).

Log type you can obtain

Log type	Output destination	File name	Description
Installer trace log file	• When JP1/IT Desktop Management 2 - Manager is installed correctly: *JP1/IT Desktop Management 2 - Managerinstallation-folder*\log • When JP1/IT Desktop Management 2 - Manager is not installed correctly: %WINDIR%\Temp\JDNINST	JDNINS01.log	The trace log file for the installer. It is output when JP1/IT Desktop Management 2 - Manager is installed.

9.2.2 Troubleshooting during agent installation

If you cannot install an agent on a computer, make sure of the following:

- The OS is a prerequisite OS for the computer on which the agent is to be installed.
- You have logged on to Windows as a user account with Administrative privileges.
- You are not trying to install an agent that is older than the agent that is already installed.

If necessary, obtain troubleshooting information for the agent.

To collect troubleshooting information for an agent:

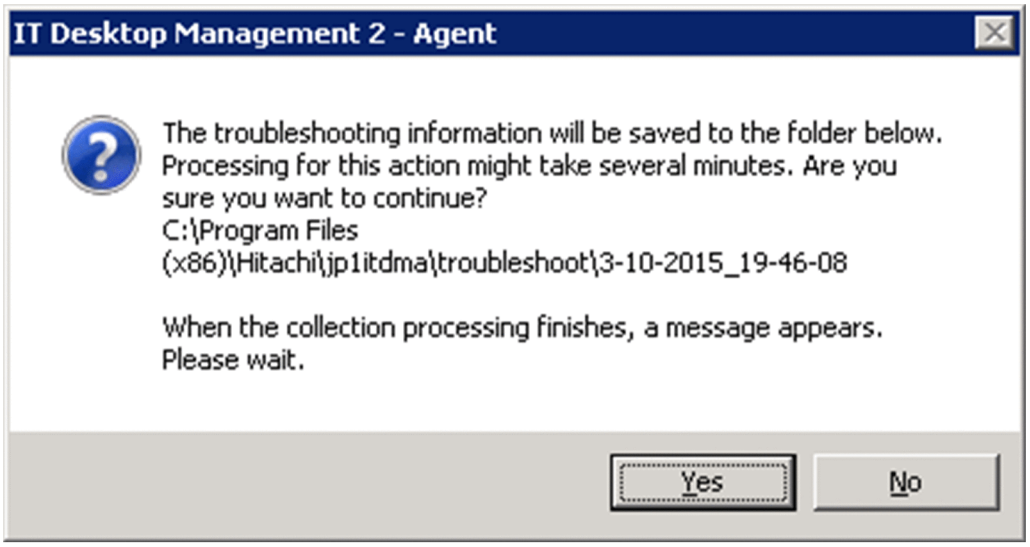
Collect troubleshooting information on the computer on which the problem occurred. Perform this operation as a user with administrator permissions.

1. Double-click `getlogs.vbs`.

   The location of `getlogs.vbs` is as follows:

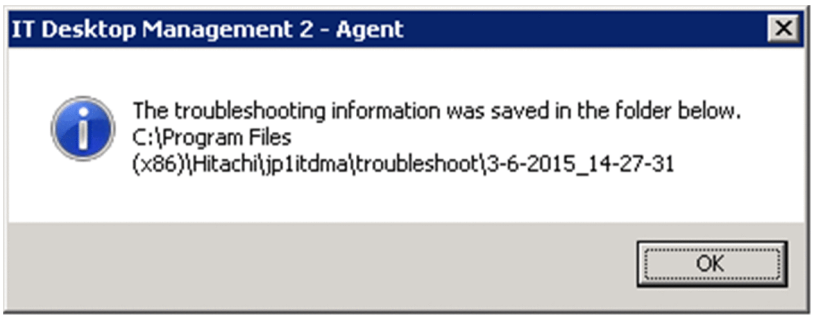
   JP1/IT-Desktop-Management-2-Agent-installation-folder`\bin`

   The dialog box asking you whether you want to continue with the collection of troubleshooting information appears.



2. Click the **Yes** button.

   The collection of troubleshooting information starts. When the troubleshooting information has been collected, a dialog box that shows the storage location of the troubleshooting information appears.



   The collected troubleshooting information is stored in the following location:

   JP1/IT-Desktop-Management-2-Agent-installation-folder`\troubleshoot\`*YYYY-MM-DD_hh-mm-ss*[#]

   #:*YYYY* is the year, *MM* is the month, *DD* is the day, *hh* is the hour, *mm* is the minute, and *ss* is the second.

3. Click the **OK** button.

   The dialog box showing the storage location of the troubleshooting information closes.

The following table shows the troubleshooting information that can be collected by using this method.

Troubleshooting information	Information collected
Agent log	*JP1/IT Desktop Management 2 - Agent-installation-folder*`\log`
System information	• System information Result of `msinfo32/nfo` execution

Troubleshooting information	Information collected

System information	• Environment variable
	Result of `SET` command execution
	• Registry information
	  • Registry information under `HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi`
	  • Registry information under `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices`
	• Device information
	Status and properties of devices
	• File information
	A list of subfolders and files under the *JP1/IT Desktop Management 2 - Agent-installation-folder*
	• Event log
	Application, system, and security information

In case of background execution using task scheduler:

Set the `/s` option to turn off confirmation message on the start and end of troubleshooting information acquisition, and then set the program name and arguments.

Example: command line setting when using task scheduler to execute command

cscript.exe //B "*JP1/IT-Desktop-Management-2-Agent-installation-folder*\bin\getlog.vbs" /s

9.2.3 Troubleshooting when two sets of device information appear for one computer

If two host IDs are registered for one computer, it appears in the user interface of JP1/IT Desktop Management 2 as if the computer has two sets of device information.

In this case, you can make sure that only the latest device information is displayed for the computer by deleting both sets of device information in the **Managed Nodes** area of the **Discovery** view of the Settings module.

9.3 Troubleshooting during building of an offline management configuration system

In the following cases, change the management status. For details about how to do this, see 9.3.1 Switching from offline management to online management or 9.3.2 Switching from online management to offline management.

- The agent for online management was mistakenly installed on a computer you want to manage offline.
- The agent for offline management was mistakenly installed on a computer you want to manage online.

To determine whether you installed the wrong agent, check the agent setup.

Also, if you assigned the wrong agent configuration to a computer on which you want to enable the network monitor, take action as follows according to the settings:

To take action when the agent configuration that clears Communicate with the higher system is assigned:

1. Switch the management status from offline management to online management.
2. Manually start the network monitor service.

To take action when the agent configuration that clears Periodically notify the higher system of the information collected from the computer is assigned:

1. In the agent configuration, select **Basic Settings**, and select the **Periodically notify the higher system of the information collected from the computer** check box.

9.3.1 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.

9.3.2 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.

9.4 Troubleshooting during building of an agentless configuration system

If you cannot authenticate an agentless computer, make sure of the following:

On a management server

- The community name used to connect to a device when SNMP is used correct.
- The user ID or password for Windows management shares is correct.

On a computer

- The SNMP agent service is operating correctly.
- The conditions necessary for agentless management have been met.

9.5 Troubleshooting during building of a support service linkage configuration system

If you are unable to connect to the support service site when obtaining updated program information and anti-virus product information, in the Settings module, select **General**, and then **Product Update**. In the window that appears, check whether the URL, Download User ID, password, and other items that are set in this window are correct. If you change the settings, click the **Test** button to ensure that a connection can be established.

9.6 Troubleshooting during building of an Active Directory linkage configuration system

If you cannot connect to Active Directory, make sure that the settings you specified in the **Active Directory** view that opens when you select **General** in the Settings module are correct.

9.7 Troubleshooting during building of an MDM linkage configuration system

This subsection describes the action to take if a problem occurs during the building of an MDM linkage configuration system.

Smart device information is not collected.

If authentication on the MDM system being connected to fails, smart device information cannot be obtain.

Action

Check whether a message for the 1118 event or the KDEX5427-E message is output. If either is output, the password you set in the **MDM Linkage Settings** view of the Settings module might be incorrect. Set the correct password.

9.8 Troubleshooting during building of a network monitoring configuration system

When you enable network access control, if none of the devices installed in the applicable network segment can connect to the network, make sure network connection for the network devices, such as routers, is permitted. If connection is not permitted, permit network connection for the network devices, including routers.

9.9 Troubleshooting during building of a cluster system

If a problem occurs on a running management server, and operation cannot be switched to a backup server automatically, verify the settings you specified during setup.

Settings specified in the Cluster Environment view

- **Use cluster configuration to operate IT Desktop Management 2 - Manager** is selected.
- **Primary** is selected on the management server, and **Secondary** is selected on the other server.
- The specified logical host name and logical IP address are correct.

Settings specified in the Folder Settings view

- The folder for the shared disk is specified.
- The specified folder path is correct.

9.10 Troubleshooting during linkage with JP1/NETM/NM - Manager

If a problem occurs during linkage with JP1/NETM/NM - Manager, collect error information for JP1/NETM/NM - Manager. Then, contact the support service and submit the collected information together with JP1/IT Desktop Management 2 troubleshooting information.

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 Recognition procedure when an agent environment is changed

A unique ID used to identify a device (host identifier) is generated for a computer on which an agent is installed.

If you change the computer environment, whether a host identifier is generated depends on how the changes are made. When a host identifier is regenerated, the device is recognized as a different device from the device recognized before the environment was changed.

A host identifier is regenerated in the following cases:

- The OS is reinstalled.
- The hard disk drive on which the OS is installed was changed.
- The motherboard is changed.#
- The agent is installed on another computer from a disk copy.#
- The `resetnid.vbs` command is executed.
- The host ID management file becomes invalid, and the file is recreated.

#: If the host identifier has already been regenerated, the device is recognized as the same device as the device recognized before the environment was changed.

In all other cases, the host identifier is not regenerated. For example, the host identifier is not regenerated for the following cases:

- The agent is uninstalled.
- The agent is reinstalled after being uninstalled.
- An overwrite installation of the agent is performed.
- The CPU, memory, or a network card is replaced.
- The OS is upgraded.
- The hard disk drive size is increased.

Tip

If a device is recognized as a different device, device information and hardware resource information before the change to the environment remain on the management server. If necessary, delete this information.

A.3 The procedure for creating a server environment of Citrix XenApp and Microsoft RDS

The following describes the procedure necessary to manage the Citrix XenApp and Microsoft RDS server with JP1/IT Desktop Management 2.

- Create Agent installers
- Installing agents
- Assigning security policies
- Creating policies of destination groups

(1) Create agent installers

The followining describes the procedure for creating agent installers to perform an installation to the Citrix XenApp and Microsoft RDS server. The agent installers must be created by an administrator.

In addition, agents must be registered to the management server. For details on procedure for registering agents to the management server, see *5.9 Procedure for registering components*.

This section describes the procedure to manage the Citrix XenApp and Microsoft RDS server. For information on other necessary settings, see *1.6 Manually installing agents on computers*.

1. Stop the services of the management server.
   To stop the services, execute the `stopservice` command (stopping services).
2. Edit the configuration file (`jdn_manager_config.conf`).
   Set the value of `AgentStartMenu_Display` to `OFF`. (If the execution of setup is necessary, for example, when you change the connection destination of agents, execute *Agent-installation-folder*\bin\jdngsetup.exe.)
   For details on the configuration file (`jdn_manager_config.conf`), refer to the property list in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.
3. Start the services of the management server.

To start services, execute the `startservice` command (Starting services).

4. Log in to the management window of JP1/IT Desktop Management 2.

5. Add agent settings.

   Select **Windows Agent Configurations and Create Agent Installers** on the menu area of the **Settings** module, then click **Add Agent Configuration** button in the **Windows Agent Configurations and Create Agent Installers** window. In the **Add Agent Configuration** dialog box, add agent settings for the Citrix XenApp and Microsoft RDS server. For the agent settings we recommend, refer to the the parameter list in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

6. Specify the setting items for agent installers.

   From the **Windows Agent Configurations and Create Agent Installers** window, select the agent settings you created and then click **Create Agent Installer**. In the **Create Agent Installer** dialog box, specify the setting items for agent installers.

   In **Settings for the component to be installed**, select **JP1/IT Desktop Management 2 - Agent (Agent)**, and set the check of **Remote Control Agent** off.

7. Create agent installers.

(2) Installing agents

The following describes the procedure for installing agents to the Citrix XenApp and Microsoft RDS server. In this procedure, an administrator creates agent installers and a master image in which the agents are installed.

This section describes the procedure to manage the Citrix XenApp and Microsoft RDS server. For information on other necessary settings, see *1.6 Manually installing agents on computers*.

1. Log on to the Citrix XenApp and Microsoft RDS server to which agents are installed with administrator privileges.

2. Install the agents with the agent installers.

   Perform the installation with administrator privileges.

3. Specify the settings to distinguish the Citrix XenApp and Microsoft RDS server from general Windows computers.

   With a registry editor etc., add the registry information to the Citrix XenApp and Microsoft RDS server. Example of registry information to be specified:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\JP1/IT Desktop Management - Agent
Value name	RdsServerType
Type	REG_SZ
Value	XenApp_RDS_Server

4. From a command prompt launched with administrator privileges, execute the following command.

```
Agent-installation-folder\bin\jdngsetrdsconf.bat LOGSETTING
```

   This command is for setting the size expansion of internal logs of agents. After executing, confirm the following message is displayed.#

```
The operation completed successfully.
```

   # The following describes the errors that might occur when executing the command and how to deal with them.

Inputted parameter is invalid.

Workaround: Conform that the `LOGSETTING` option when executing the command is specified correctly.

Access to the registry is denied.

Workaround: Confirm that the command is executed with administrator privileges.

Failed to create an INI file.

Workaround 1: Confirm that the command is executed with administrator privileges.

Workaround 2: Confirm that there is the access privilege to the *Agent-installation-folder*\conf folder.

5. Register the exception of the ports for communication of agents to Windows Firewall.

   From a command prompt, execute the following command.

   ```
   netsh advfirewall firewall add rule name="JP1/IT Desktop Management 2 - Ag
   ent Service" dir=in action=allow protocol=TCP localport=Port-number-for-re
   quest-forstarting-agents
   ```

   The following shows an execution example:

   ```
   netsh advfirewall firewall add rule name="JP1/IT Desktop Management 2 - Ag
   ent Service" dir=in action=allow protocol=TCP localport=31001
   ```

   Note that in the management server, when you change **Agent startup port number** of setup from the default value (31001), also change the port number for the request for starting agents of the execution commands.

6. Execute the `resetnid.vbs` command (Re-setting host id).

   From a command prompt, execute the following command.

   ```
   cscript.exe Agent-installation-folder\bin\resetnid.vbs /nodeid /i
   ```

   For details on the `resetnid.vbs` command (Re-setting host id), refer to the explanation about re-setting host id (resetnid.vbs) in the manual *JP1/IT Desktop Management 2 Administration Guide*.

7. Create a master image with a tool etc.

8. Reboot the OS after copying the master image to the Citrix XenApp and Microsoft RDS server.

9. Log in.

   Agent is started.

(3) Assigning security policies

The following describes the procedure to create and assign security policies for the Citrix XenApp and Microsoft RDS server. For information on other necessary settings, see *1.6 Manually installing agents on computers*.

1. Log in to the management window of JP1/IT Desktop Management 2.

2. Specify additional management items.

   In **Custom Fields (Hardware Assets)** in the **Asset Field Definitions** window of the setting window, add the items to acquire the registry information specified in *(2) Installing agents*.

   Example of an additional management item:

Item name	The Citrix XenApp and Microsoft RDS server identification information
Input method	Acquire from registries

Data type		Text
Registry path	Root key	HKEY_LOCAL_MACHINE
	Path	SOFTWARE\Wow6432Node\Hitachi\JP1/IT Desktop Management - Agent
	Registry	RdsServerType

3. Add groups of user definitions.

   From **Device List (User-Defined)**] in the menu area of the security window and device window, add groups of user definitions in which additional management items are specified as a condition.

   Example of a user definition group:

Group name		The Citrix XenApp and Microsoft RDS server
Condition	Targeted item	The Citrix XenApp and Microsoft RDS server identification information
	Condition to be determined	Equal to determined value
	Determined value	XenApp_RDS_Server

4. Create security policies.

   Select **Security Policy List** in the menu area in the **Security** module, click **Add** button in **Security Policy List** window, and then create security policies in the **Add Security Policy** dialog box. For the security policies we recommend, refer to the items that can be specified in security policies in the manual *JP1/IT Desktop Management 2 Overview and System Design Guide*.

5. Assign the security policies.

   Select the created groups of user definitions from **Device List (User-Defined)** in the menu area of the security window. After the list of the Citrix XenApp and Microsoft RDS servers is displayed, select all the items and click **Action** - **Assign Policy**, and then display the **Assign Policy** dialog box. Select and assign the created security policies of the Citrix XenApp and Microsoft RDS server.

(4) Creating policies of destination groups

To perform distribution with Remote Install Manager, by creating policies of destination groups, you can create the destination groups for the Citrix XenApp and Microsoft RDS server.

This section describes the procedure for creating policies to create destination groups for the Citrix XenApp and Microsoft RDS server. For information on other necessary settings, refer to the manual *JP1/IT Desktop Management 2 Distribution Function Administration Guide*.

1. Log in to Remote Install Manager of JP1/IT Desktop Management 2.

2. Display the **Group by custom fields of hardware asset information** dialog box.

   Display the **Policy Setup** dialog box by selecting **File** - **Create Host Group** - **Create the policy for a host group** from the menu of the **Destination** window. The **Group by custom fields of hardware asset information** dialog box is displayed by Clicking **Add**, selecting **Automatic maintenance of destination group**, and then selecting **Group by custom fields of hardware asset information**.

3. Add the policies in which additional management items to distinguish the Citrix XenApp and Microsoft RDS server are specified.

   Example of the policy of destination groups:

Policy type	Group by custom fields of hardware asset information

Custom fields of hardware asset information	1st level	The Citrix XenApp and Microsoft RDS server identification information
	2nd level	(Not specified)
	3rd level	(Not specified)
	4th level	(Not specified)
	5th level	(Not specified)
	6th level	(Not specified)
Route	(Not specified)	

A.4 Building an environment for shared VDI

This section describes the procedure you must follow to manage shared VDI-based virtual computers with JP1/IT Desktop Management 2.

Creating an installation set and installing agents

Follow the procedure described below to install agents on shared VDI-based virtual computers. In this procedure, an administrator creates an installation set as well as a master image of the master PC on which an agent has been installed.

This section focuses on the procedure you must follow to manage virtual computers provided by VMware Horizon View and Citrix Virtual Desktops. For details on other necessary settings, see *1.6 Manually installing agents on computers*.

1. Log in to the operation window of JP1/IT Desktop Management 2.

2. Add an agent configuration.

   In the menu area of the Settings module, select **Windows Agent Configurations and Create Agent Installers**, and then in the **Windows Agent Configurations and Create Agent Installers** view that appears, click the **Add Agent Configuration** button. In the Add Agent Configuration dialog box that appears, add an agent configuration for shared VDI-based virtual computers.

   Select **User Notification Settings**, and then **Display Settings on User Computers**. For **When a user input window is displayed**, set **Hidden**.

   For details about agent configurations, see the Lists of Parameters in the JP1/IT Desktop Management 2 Overview and System Design Guide.

3. Specify the setting items for the installation set.

   From the **Windows Agent Configurations and Create Agent Installers** view, select the created agent configuration, and then click the **Create Agent Installer** button. In the **Create Agent Installer** dialog box, specify the setting items for the installation set.

   Select **Installation Folder Settings**, **Settings when generating the host ID**, and then the **Generate the host ID based on information about the virtual computer** check box. Furthermore, select the device information to be used, which should be appropriate to the technology used to create the virtual computers to be managed.

   When VMware Horizon View is used, or when the Machine Creation Services (MCS) technology provided by Citrix Virtual Desktops is used:

   Computer Name or **IP Address**

   When the Provisioning Services (PVS) technology provided by Citrix Virtual Desktops is used:

   Account Name

   For details about the setting items for the installation set, see the lists of parameters in the JP1/IT Desktop Management 2 Overview and System Design Guide.

4. Create an installation set.

5. Log in to the master PC on which to install an agent with administrator privileges.

6. Install an agent on the master PC by using the installation set.
   You have to install an agent on the master PC with administrator privileges.

Registering a logoff script

To manage the operation logs of virtual computers, register a command in the logoff script on the master PC.

1. **Select Local Group Policy**, **Windows Settings**, **Scripts (Logon/Logoff)**, and then **Logoff**.
   The **Logoff Properties** dialog box appears.

2. Add a script.
   Register the `upldoplog` command as the script.

   Script name

   agent-installation-folder`\bin\upldoplog.exe`

   Script parameter

   `/upload`

   For details about the `upldoplog` command, see upldoplog (uploading operation logs) in the JP1/IT Desktop Management 2 Administration Guide.

> **Important**
>
> Logging off from a shared VDI-based virtual computer causes the virtual computer to be initialized. You must therefore upload the agent's operation logs to the management server by using the `upldoplog` command prior to logging off from the virtual computer. Keep the following in mind when uploading an operation log:
>
> - If any operation is performed while operation logs are being uploaded, the log of that operation will not be uploaded, and the remaining operation log is deleted once the user logs off from the computer.
> - If occurrence of a failure while operation logs are being uploaded causes the upload process to end in failure, the operation logs are deleted.

Setting the master PC

1. Create a security policy to be assigned to virtual computers and assign it to the master PC.
   For details about how to use security policies, see *Using security policies* in the JP1/IT Desktop Management 2 Administration Guide.

   > **Note**
   >
   > When there are multiple master PCs, we recommend that you create a filter by using a host name or the like for ease of checking. For details about filters, see *Using filters* in the JP1/IT Desktop Management 2 Overview and System Design Guide.

2. If the software, updates, and other programs to be used by virtual computers are to be installed on the master PC, distribute them to the master PC.

For details about the distribution of software, see *Software and File Distribution* in the JP1/IT Desktop Management 2 Administration Guide.

3. In the Inventory module, confirm that a host ID has been generated from device information.

   If **Host ID** is not displayed in the Inventory module, right-click an item name in the list and select **Select Columns**. In the displayed dialog box, select the **Host ID** check box and click the OK button. The **Host ID** column shows up.

Generalizing an agent and creating a master image

To create a master image, delete program-specific information from an agent to generalize it. Execute the following commands:

```
upldoplog /upload
prepagt.bat /prep
```

For details about the commands, see the JP1/IT Desktop Management 2 Administration Guide.

> **Note**
>
> The `prepagt.bat` command deletes the operation logs that have not been uploaded yet. Therefore, if you want to manage the operation logs on the master PC, you have to execute the `upldoplog` command to upload them to the management server prior to executing the prepagt.bat command.

After generalizing the agent, create a master image from the master PC. For details about how to create a master image, see the manual of the applicable virtualization product.

Creating virtual computers

Create virtual computers from the master image. For details about how to create virtual computers, see the manual of the applicable virtualization product.

> **Important**
>
> When creating virtual computers with instant clone, restart the create virtual computers.

Checking the usage status of virtual computers

You can check the usage status of virtual computers by using the Inventory module. In the Inventory module, select **Host ID (Partial Match)** as the filtering condition, and then specify the following starting strings.

- Computer Name: `#GII`
- Account Name: `#GIO`
- IP Address: `#GIY`

> **Note**
>
> The filtered device list contains the master PC as well. To exclude the master PC from the filtered device list, set a filtering condition that can exclude the host name of the master PC.

You can check the operation logs of virtual computer users by selecting **Operations Logs**, and then **Operations Log List** in the Security module.

A.5 Building an environment for using HTTPS with the external system linkage configuration

This section describes how to build an environment for using HTTPS connection with the external system linkage configuration and presents the commands to be used for this purpose.

(1) Building an environment

You have to take the following steps to use HTTPS connection with the external system linkage configuration.

Obtaining certificates for SSL communication for the management server

From a Certificate Authority, obtain certificates (root certificate and SSL server certificate) for SSL communication for the management server.

The flow of obtaining certificates for SSL communication for the management server is as follows:

1. Create a private key for the Web server (`openssl.bat genrsa` command).
2. Create a Certificate Signing Request (CSR) (`openssl.bat req` command).
3. Display the contents of a Certificate Signing Request (CSR) (`openssl.bat req` command).
   If necessary, check the contents of the Certificate Signing Request (CSR).
4. Send the CSR to the CA.
5. Acquire a certificate from the CA.

> **Tip**
>
> You can use the `openssl.bat x509` command to check the contents of the certificate you obtained.

> **Tip**
>
> In the certificate you obtained, save the part from `-----BEGINCERTIFICATE-----` to `-----END CERTIFICATE----` in another file (httpsd.pem file defined in httpsd.conf provided as standard).

Related Topics:

- (a) Creating a private key for the Web server (openssl.bat genrsa command)
- (b) Creating a Certificate Signing Request (CSR) (openssl.bat req command)
- (c) Displaying the contents of a Certificate Signing Request (CSR) (openssl.bat req command)
- (d) Displaying certificate contents (openssl.bat x509 command)
- (e) Converting the certificate format (openssl.bat x509 command)

Setting up the management server

1. Log on to the OS as a member of the Administrators group.
2. Stop the JP1/IT Desktop Management 2 services on the management server
   Execute the following command:

   ```
   stopservice
   ```

   For details about the commands, see the JP1/IT Desktop Management 2 Administration Guide.
3. Store an SSL server certificate and a private key in the following folder on the management server:

   ```
   JP1/IT Desktop Management 2 - Manager-installation-folder\mgr\uCPSB\httpsd
   \conf\ssl\server
   ```

   You have to store the following files in the above folder:

   - The SSL server certificate file: `httpsd.pem`
   - The private key file: `httpsdkey.pem`

   > **Note**
   >
   > When you change the connection setting from HTTPS to HTTP, delete SSL server certificate and private key.

4. Edit the configuration file to include a statement.
   The configuration file (jdn_manager_config.conf) exists in the following location:

   ```
   JP1/IT Desktop Management 2 - Manager-installation-folder\mgr\conf
   ```

   Edit the configuration file to include the following statement: `RestAPIProtocol=1`

   > **Note**
   >
   > When you change the connection setting from HTTPS to HTTP, change the statement of the configuration file `RestAPIProtocol=1` to `RestAPIProtocol=0`. Do not delete the row of RestAPIProtocol that you added.

5. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
6. In the Setup window, click the **Next** button.
7. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
8. Click the **Next** button until the **API settings** view appears.
9. Select the **Use the API** check box.
10. Click the **Next** button.
11. Click the **Next** button until the **Confirm Setup Settings** view appears.
12. In the **Confirm Setup Settings** view, confirm that the specified settings are correct, and then click the **Next** button.

A dialog to confirm that Remote Install Manager and JP1/IT Desktop Management 2 - Asset Console have been stopped is displayed. After confirming, click the **OK** button. In the cluster system, make the cluster resources associated with the services displayed in the dialog offline, and then click the **OK** button.

13. In the **Setup for Distribution by Using Remote Install Manager** view, click the **OK** button.
    The setup process begins, and a dialog box appears indicating that setup is in progress. When setup has finished, the **Setup Complete** view appears.

    Important

    When the dialog box that says "Could not start the service. Service name=JP1_ITDM2_Web Server." appears, complete the setup by clicking the **OK** button to close the dialog box. Then, review the SSL server certificate file and the private key file in step 3, and then directly start the service of `JP1_ITDM2_Web Server`. When the dialog box of "An error occurred during Setup." appears, review the `RestAPIProtocol` value which is set in step 4 is correct.

14. In the **Setup Complete** view, click the **OK** button.

Note

In case of a cluster system, setup the primary server and the standby server.

(2) Commands used to acquire certificates for SSL communication

The following describes the commands used to acquire certificates for SSL communication.

The commands are stored in the following folders:

```
JP1/IT Desktop Management 2 - Manager-installation-folder\mgr\uCPSB\httpsd\s
bin
```

(a) Creating a private key for the Web server (openssl.bat genrsa command)

Functionality

This section describes the `openssl.bat genrsa` command, which creates a private key for the Web server.

Format

```
openssl.batΔgenrsaΔ-randΔfile-name[:file-name...]Δ-outΔkey-fileΔ[512|1024|20
48|4096]
```

Operand

-randΔ*file-name*[:*file-name...*]
Specify any file to be used for random number generation.

-outΔ*key-file*
Specify the file to which the Web server private key is output.

512|1024|2048|4096
Specify the bit length of the Web server private key. If this operand is omitted, `2048` is assumed.

Notes

If you enter a password that is 3 characters long or less, there will be a message prompting you to enter at least 4 characters and no more than 1,023 characters. In this version, enter a password of 4 characters to a maximum of 64 characters. Please note that even if you enter a password of 65 characters or longer, it will not be an error.

Example

To create the `httpsdkey.pem` Web server private key:

```
openssl.bat genrsa -rand C:\WINNT\NOTEPAD.EXE -out httpsdkey.pem 2048
```

Related Topics:

- (b) Creating a Certificate Signing Request (CSR) (openssl.bat req command)

(b) Creating a Certificate Signing Request (CSR) (openssl.bat req command)

Functionality

This section describes the `openssl.bat req` command, which creates a Certificate Signing Request (CSR). The created CSR file is submitted to the CA, which then issues the signed certificate. The CSR is created in the format conforming to PKCS #10.

Format

```
openssl.batΔreqΔ-newΔ-sha256Δ-keyΔkey-fileΔ-outΔCSR-file
```

Operand

-sha256
: Specify the signature algorithm `sha256WithRSAEncryption` is used when the CSR is created.

-key*Δkey-file*
: Specify the Web server private key file.

-out*ΔCSR-file*
: Specify the file to which the created CSR is output.

Example

To create a Certificate Signing Request (CSR) by using the Web server private key file `httpsdkey.pem`, specify as follows:

```
openssl.bat req -new -sha256 -key httpsdkey.pem -out httpsd.csr
```

If you have set a password when creating the private key for the Web server, you are prompted to enter the password. For the items to be set, follow the instructions from the CA to which you submit the Certificate Signing Request (CSR).

(c) Displaying the contents of a Certificate Signing Request (CSR) (openssl.bat req command)

Functionality

This section describes the `openssl.bat req` command, which displays the contents of a Certificate Signing Request (CSR).

Format

```
openssl.bat△req△-in△CSR-file△-text
```

Operand

-in△*CSR-file*

Specify the CSR file to be displayed.

Example

To display the CSR file `httpsd.csr`, specify as follows:

```
openssl.bat req -in httpsd.csr -text
```

(d) Displaying certificate contents (openssl.bat x509 command)

Functionality

This section describes the `openssl.bat x509` command, which displays the contents of a certificate file. The following command displays the part of the certificate file that begins with `-----BEGIN CERTIFICATE-----` and ends with `-----END CERTIFICATE----`.

Format

```
openssl.bat△x509△-in△certificate-file△-text
```

Operand

-in△*certificate-file*

Specify the certificate file to be displayed.

Example

To display the certificate file `httpsd.pem`, specify as follows:

```
openssl.bat x509 -in httpsd.pem -text
```

(e) Converting the certificate format (openssl.bat x509 command)

Functionality

This section describes the `openssl.bat x509` command, which converts the certificate format. Use this functionality as necessary.

Format

```
openssl.bat△x509△-inform△input-format△-outform△output-format△-in△input-file△
-out△output-file
```

Operand

-inform△*input-format*

Specify the input format of the certificate file before conversion. The following input formats can be specified:

- DER
- PEM

-outform△*output-format*

Specify the input format of the certificate file after conversion. The following input formats can be specified:

- DER
- PEM

-in△*input-file*

Specify the certificate file before conversion.

-out△*output-file*

Specify the certificate file after conversion.

A.6 Version changes

(1) Changes in 13-01

(a) Changes in the manual (3021-3-L73-10(E))

- The flow rate control can be performed with relay system.
- Added Microsoft Intune to MDM system to work with.

(2) Changes in 13-00

(a) Changes in the manual (3021-3-L73(E))

- Windows Server 2022 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
- Windows 11 was added as an applicable operating system for the following products:
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
- Windows Server 2012 was removed from applicable OSs for the following products:

- JP1/IT Desktop Management 2 - Manager
- JP1/IT Desktop Management 2 - Asset Console
- JP1/IT Desktop Management 2 - Internet Gateway

- Add the following properties that can be set by the configuration file:
  - Settings to suppress the network group automatic generation
  - Settings that do not perform identification when registering devices
  - Settings to suppress automatic update of network control list
  - Alert threshold of the Network Control List
  - Set whether to notify notification items on the home screen when the number of network control list registrations reaches the warning threshold and the limit is reached

(3) Changes in 12-60

(a) Changes in the manual (3021-3-E13-30(E))

- Maximum of 300,000 devices can be managed.
- **Operation Date/Time (UTC)** was added to the information items to be collected in the operation log.

(4) Changes in 12-50

(a) Changes in the manual (3021-3-E13-20(E))

- A procedure for setting API usage was added.
- The explanation for using operation windows with 10-20 concurrent users was changed.

(5) Changes in 12-10

(a) Changes in the manual (3021-3-E13-10(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
- Devices can now be managed from an external system via the API.
- Shared VDI-based virtual computers can now be managed.

(6) Changes in 12-00

(a) Changes in the manual (3021-3-E13(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

- The connection destination of a higher system can now be automatically switched for distribution of files.
- Computers can now be managed via the Internet.

(7) Changes in 11-51

(a) Changes in the manual (3021-3-B53-40(E))

- A security policy can now be set for offline-managed devices.

(8) Changes in 11-50

(a) Changes in the manual (3021-3-B53-30(E))

- 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.
- 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.

(9) Changes in 11-10

(a) Changes in the manual (3021-3-B53-20(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
- By linking with JP1/Base, you can now log in to JP1/IT Desktop Management 2 by using JP1 authentication.
- 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
- As files that are to be executed automatically during installation, ZIP files for installers of related products, such as Hibun, can now be set.
- A maximum of 50,000 devices can now be managed.

(10) Changes in 11-01

(a) Changes in the manual (3021-3-B53-10(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.
- You can now use the file for connection destinations (`itdmhost.conf`) to specify the connection destination of an agent.
- In the description of the Procedure for installing Remote Install Manager only, the following information was amended:
    - The description of the dialog box where you select a component to install
    - The description of the information needed when starting Remote Install Manager after installation
- To perform distribution by using Remote Install Manager, you can now select whether to enable flow control (by specifying the maximum transfer rate for sending packages).
- 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.
- You can now select which menu items are to be displayed in the start menu of an agent.
- The procedure for switching the higher connection destination of a management relay server now mentions that device information needs to be manually reported all the way from the lower management relay server to the primary management server.
- A description of the port numbers used on the administrator's computer (Remote Install Manager) and relay systems was added.

(11) Changes in 11-00

(a) Changes in the manual (3021-3-B53(E))

- Operating JP1/IT Desktop Management 2 in a multi-server configuration enables both location-by-location management and integrated management.
- The procedure for installing JP1/IT Desktop Management 2 - Manager was changed.
- The procedure for setting up a management server was changed.
- The procedure for overwrite-installing JP1/IT Desktop Management 2 - Manager was changed.
- You can now import and export network connection information.
- The following products now support Windows 10:
    - 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 OSs for the following products:

  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
  - JP1/IT Desktop Management 2 - RC Manager
- Anti-virus product information can now be acquired from the support service site.
- You can now install and manage an agent on a computer whose OS is UNIX.
- As an argument for the resetnid.vbs (resetting host identifiers) command, /s was added.
- (Changes from only this manual (3021-3-369(E))) The software, purchasing status, product ID, GUID, and software type for some software can now be managed.

(12) Changes in 10-50

(a) Changes in the manuals (3021-3-275 and 3021-3-369(E))

- A description of a method of displaying the return code of the `resetnid.vbs` (reset a host ID) command was added, and the accompanying usage example was amended.
- Systems can no longer be deployed in a site server configuration, and a host called a *relay system* was added as an essential component of distribution using Remote Installation Manager.
- When distributing software using Remote Installation Manager, the conditions for managed computers and the installation behavior can now be specified in more detail.
- Hardware information (including networking equipment), software information, and contract information can now be centrally managed in the database.
- Files stored on managed computers can now be collected as a batch.
- In the **Getting Started** wizard, you can now manage devices by installing the agent software.
- Systems can no longer be deployed in a multi-server configuration, and a single management server can now manage a maximum of 30,000 devices.
- You can now specify how many times the user can enter the wrong password before his or her account is locked, and set a valid period for passwords.
- The settings associated with installation, setup, and agent setup were changed to reflect the new product structure.
- Windows 8.1 and Windows Server 2012 R2 were added as supported OSs for the following products:
  - JP1/IT Desktop Management 2 - Manager
  - JP1/IT Desktop Management 2 - Agent
  - JP1/IT Desktop Management 2 - Network Monitor
- Windows 8 and Windows 7 are no longer supported OSs of the following product:
  - JP1/IT Desktop Management 2 - Manager
- The following product no longer supports Windows 2000:
  - JP1/IT Desktop Management 2 - Agent
- The supported versions of Internet Explorer were changed.
- Microsoft Cluster Service was removed from the list of supported cluster software.
- Some port numbers were changed.
- The folder structure created under JP1/IT Desktop Management 2 - Manager was changed to reflect the new product structure.

(13) Changes in 10-10

(a) Changes in the manual (3021-3-153-30)

- Cautionary notes regarding installation, overwrite installation, and uninstallation were added.
- A description was added stating that if the discovery of network-connected devices is concentrated within a specified time period, the discovery range must be set so that the number of IP addresses does not exceed 50,000.
- By linking with JP1/NM - Manager, network connections that are monitored by the appliance products on which JP1/NM is installed can now be monitored from JP1/IT Desktop Management.
- A description was added about changing the server certificate of the MDM system after the server certificate is imported to the management server. The description of the versions of Internet Explorer that can be used to obtain the server certificate was deleted. A description of the settings to use when linking with the JP1 smart device management service was also added.
- You can now specify whether to enable automatic updates for all items in the network control list or only for additional items.
- The description of performing an overwrite installation of the product and updating the components was amended.
- A description of the procedure for upgrading the entire JP1/IT Desktop Management system and the procedure for upgrading JP1/IT Desktop Management -Manager was added.
- The procedure for changing the site server's connection destination was added to the procedure for replacing the management server in a single-server configuration system.
- All descriptions relating to command execution permissions were consolidated under the description of the procedure for executing commands. A description was also added regarding situations in which UAC is enabled in the OS when executing commands other than `getinv.vbs`.
- Cautionary notes regarding command execution were added.
- The `/i` option was added to the `resetnid.vbs` command, and dialog boxes in which the user can select whether to execute the command and display the execution result now appear on the user's computer.
- The description of port number settings was amended. A description of the network between JP1/IT Desktop Management - Remote Site Server and agentless computers was also added.

(b) Changes in the manual (3021-3-338-10(E))

- The following products now support Windows 8 and Windows Server 2012:
  - Job Management Partner 1/IT Desktop Management - Manager
  - Job Management Partner 1/IT Desktop Management - Remote Site Server
  - Job Management Partner 1/IT Desktop Management - Network Monitor
- Notes on installation, overwrite installation, and uninstallation were added.
- You can now obtain the revision history of device information.
- 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 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. In addition, the descriptions of the Internet Explorer version available for obtaining a server certificate were deleted.

- For automatic update of the network control list, you can now specify whether to enable all automatic updates or automatic updates only for add operations.
- Descriptions of overwrite-installing the product and updating components were corrected.
- Descriptions were added to the procedures for updating the version of the entire JP1/IT Desktop Management system and JP1/IT Desktop Management - Manager.
- The procedure for changing the connection destination of a site server was added to the procedure for replacing a management server in a single-server system.
- Descriptions about permissions required to execute commands were collected in *8.1 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. In addition, notes on command execution were added.
- You can now export and import definitions of shared management items and added management items in CSV format.
- A description was added about the characters that can be used for folder names specified in the following commands:
  - exportdb command
  - getlogs command
  - getinstlogs command
  - importdb 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. In addition, the following topics were added:
  - A procedure of resetting a host ID on a computer on which a site server is installed
  - Notes on executing the resetnid.vbs command on a device on which the network monitor is installed
- 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.

(14) Changes in 10-02

(a) Changes in the manual (3021-3-153-20)

- The following products now support Windows 8 and Windows Server 2012:
  - JP1/IT Desktop Management - Manager
  - JP1/IT Desktop Management - Remote Site Server
  - JP1/IT Desktop Management - Network Monitor
- You can now obtain the revision history of device information.
- A procedure of executing commands on a computer with an agent installed was added.
- You can now export and import definitions of shared management items and added management items in CSV format.
- A description was added about the characters that can be used for folder names specified in the following commands:
  - `exportdb` command
  - `getlogs` command

- `getinstlogs` command
- `importdb` command

- A procedure of resetting a host ID on a computer on which a site server is installed.
- Notes on executing the `resetnid.vbs` command on a device on which the network monitor is installed.

(15) Changes in 10-01

(a) Changes in the manual (3021-3-153-10)

- A description stating that the default file name of the installation set is ITDMAgt.exe was added.
- A 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.
- JP1/IT Desktop Management information can now be updated by obtaining the support service information, including information about anti-virus software.
- The notes that apply when JP1/IM and JP1/Base are not connected in a JP1/IM linkage system were improved.
- The notes on deleting the search range or authentication information of devices managed without using agents, or on unregistering the devices from the Active Directory settings, were collected in the JP1/IT Desktop Management 2 Overview and System Design Guide.
- You can now update the JP1/IT Desktop Management information by obtaining anti-virus product information from the support service site.
- The procedure for setting the information required to link with the MDM system was corrected.
- A general procedure for updating the version of the entire JP1/IT Desktop Management system was added.
- The procedure for updating the version of JP1/IT Desktop Management - Manager was corrected.
- The description of how to update components was corrected.
- A general procedure for overwrite-installing JP1/IT Desktop Management - Manager in a multi-server system was added.
- A general procedure for updating the version of JP1/IT Desktop Management - Manager in a multi-server system was added.
- The procedure for replacing a site server and the notes on the `recreatelogdb` command used to replace a site server were corrected.
- A procedure for replacing a computer on which the network monitor is enabled was added.
- You can now update the JP1/IT Desktop Management information by obtaining the SAMAC software dictionary file for offline updates from the support service site.
- The note on the `recreatelogdb` command executed with an argument other than -node was corrected.
- A description of the `stopservice` (stopping services) command as a configuration-related command was added.
- A description stating that the `getlogs` command uses the folder set in the TEMP user environment variable as a temporary folder was added.
- The description of the case in which an agent is installed by copying a disk without executing the `resetnid.vbs` command in the reference material section was improved.
- The port numbers used by JP1/IT Desktop Management - Manager were described separately for a single-server configuration and for a multi-server configuration.

(b) Changes in the manual (3021-3-338(E))

- The following information was combined into the Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management Overview and System Design Guide:
  - A description of Microsoft products
  - Icons and formats used in the manual
  - Online Help
  - Related manuals
  - Related documents
  - Notations used in the manual
  - Abbreviations used in the manual
  - Conventions, for example, kilobyte (KB)
  - Glossary
- A description stating that the default file name of the installation set is ITDMAgt.exe was added.
- A 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
- You can now update the JP1/IT Desktop Management information by obtaining information from the support service.
- The notes applying if JP1/IM and JP1/Base are not connected in a JP1/IM linkage system were improved.
- The procedure for setting the information required to link with the MDM system was corrected.
- A general procedure for updating the version of the entire JP1/IT Desktop Management system was added.
- The procedure for updating the version of JP1/IT Desktop Management - Manager was corrected.
- The description of how to update components was corrected.
- A general procedure for overwrite-installing JP1/IT Desktop Management - Manager in a multi-server system was added.
- A general procedure for updating the version of JP1/IT Desktop Management - Manager in a multi-server system was added.
- The procedure for replacing a site server and the notes on the `recreatelogdb` command used to replace a site server were corrected.
- A procedure for replacing a computer on which the network monitor is enabled was added.
- The note on the `recreatelogdb` command executed with an argument other than -node was corrected.
- A description of the `stopservice` (stopping services) command as a configuration-related command was added.
- A description stating that the `getlogs` command uses the folder set in the TEMP user environment variable as a temporary folder was added.
- A description of the case in which an agent is installed by copying a disk without executing the `resetnid.vbs` command in the reference material section was improved.
- The port numbers used by JP1/IT Desktop Management - Manager were described separately for a single-server configuration and for a multi-server configuration.
- You can now manage a maximum of 50,000 devices when operating a system in a multi-server configuration.
- You can now link with JP1/IM to send notifications concerning JP1 events.

- The URL of the login window for JP1/IT Desktop Management was added.
- The following description was added: The **Set the account to install Agent** setting in the **Create Agent Installer** dialog box takes effect only if you install an agent in Windows 2000, Windows XP, or Windows Server 2003.
- The following description was added: You can schedule the time to obtain the latest updated program information from the support service site by using **Edit Import Schedule**, which is displayed by selecting **General**, and then **Product Update** in the Settings module.
- A solution for the following was added: When installing an agent by copying a disk, multiple devices are recognized as a single device.
- The following was added: The time required to generate a new host name after the `resetnid.vbs` is executed.
- The port numbers of the controller and remote control agent were modified.
- The timing at which the host ID is regenerated was added.
- 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 within 180 days of setting it.
- A procedure for releasing a user account lock was added.
- You can now link with an MDM product to manage smart devices.
- 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 detailed procedure for replacing a management server was added.
- The action to be taken in the following case was added: The file for recording the execution status (`deletelog_lasttime.txt`) exists in the work folder when the `deletelog` command that deletes the site server operation log data is executed.
- Port number 31000 was added to the list of port numbers for site servers.

(16) Changes in 10-00

(a) Changes in the manual (3021-3-153)

- You can now manage a maximum of 50,000 devices when operating a system in a multi-server configuration.
- You can now link with JP1/IM to send notifications concerning JP1 events.
- The URL of the login window for JP1/IT Desktop Management was added.
- The following description was added: The **Set the account to install Agent** setting in the **Create Agent Installer** dialog box takes effect only if you install an agent in Windows 2000, Windows XP, or Windows Server 2003.
- The following description was added: You can schedule the time to obtain the latest updated program information from the support service site by using **Edit Import Schedule** that is displayed by selecting **General**, and then **Product Update** in the Settings module.
- A solution for the following was added: When installing an agent by copying a disk, multiple devices are recognized as a single device.
- The following was added: The time required to generate a new host name after the `resetnid.vbs` is executed.
- The port numbers of the controller and remote control agent were modified.
- The timing at which the host ID is regenerated was added.
- 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

(17) Changes in 09-51

(a) Changes in the manual (3020-3-S94-10)

- 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 within 180 days of setting it.
- A procedure for releasing a user account lock was added.
- You can now link with an MDM product to manage smart devices.
- 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 detailed procedure for replacing a management server was added.
- The action to be taken in the following case was added: The file for recording the execution status (`deletelog_lasttime.txt`) exists in the work folder when the `deletelog` command that deletes site server operation log data is executed.
- Port number 31000 was added to the list of port numbers for site servers.

Index

A

B

C

D

E

G

H

I

J

L

M

N

O

P

R

S

T

U

Hitachi, Ltd.
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan