

Job Management Partner 1 Version 10

**Job Management Partner 1/IT Desktop
Management 2 Configuration Guide**

3021-3-369(E)

Notices

■ Relevant program products

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

The above product includes the following:

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

■ Trademarks

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

Firefox is a registered trademark of the Mozilla Foundation.

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

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

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

Mac OS is a trademark of Apple Inc.

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

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

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

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

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

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

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

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

SOAP is an XML-based protocol for sending messages and making remote procedure calls in a distributed environment.

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

HITACHI
Inspire the Next

Hitachi, Ltd.



Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

■ Restrictions

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

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

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

■ Issued

Apr. 2015: 3021-3-369(E)

■ Copyright

All Rights Reserved. Copyright (C) 2015, Hitachi, Ltd.

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

Preface

This manual describes how to build a Job Management Partner 1/IT Desktop Management 2 - Manager (abbreviated hereafter to JP1/IT Desktop Management 2) system.

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

■ 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 a minimal configuration system (management servers and agents)
This chapter describes how to build a minimal configuration system (consisting of 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, please see the *Job Management Partner 1/IT Desktop Management 2 Overview and System Design Guide*.

Contents

Notices	2
Preface	5

1	Building a minimal configuration system (management servers and agents)	12
1.1	Overview of building a minimal configuration system	13
1.2	Creating a management server environment	14
1.2.1	Types of JP1/IT Desktop Management 2 - Manager installation	14
1.2.2	Procedure for installing JP1/IT Desktop Management 2 - Manager	14
1.2.3	Procedure for setting up a management server	16
1.3	Registering a Product License	20
1.3.1	Registering a product license	20
1.3.2	Adding a product license	20
1.4	Logging in to the Operation Window	21
1.4.1	Logging in	21
1.4.2	Changing the default password	22
1.4.3	Setting user account information	22
1.4.4	Unlocking a user account	23
1.5	Identifying all devices used in your organization	24
1.5.1	Searching for devices connected to the network	24
1.5.2	Planning the installation of agents	25
1.6	Manually installing agents on computers	27
1.6.1	Creating an installation set	27
1.6.2	Installing agents on computers	29
1.6.3	Uploading an agent to a Web server	30
1.6.4	Uploading an agent to a file server	31
1.6.5	Distributing the agent installation media (CD-R or USB memory) to users	32
1.6.6	Distributing agents to users as a file attached to an email	33
1.6.7	Installing an agent on the computer by using a logon script	33
1.6.8	Installing an agent on the computer by using the disk copy feature	35
1.6.9	Procedure for installing the agent from supplied media	36
1.6.10	Procedure for setting up the agent	37
1.7	Automatically installing agents on computers	39
1.7.1	General procedure for checking the agent installation status	39
1.7.2	Automatically deploying an agent to every computer discovered during the search (network search)	40
1.7.3	Checking the device discovery status	40
1.7.4	Checking the latest discovery status	41

- 1.7.5 Checking the discovered devices 41
- 1.7.6 Checking the managed devices 42
- 1.7.7 Checking the excluded devices 43
- 1.7.8 Deploying agents to selected groups of computers on which agents have not yet been installed 43

2 Building system configurations 45

- 2.1 Building a basic configuration system (relay system) 46
 - 2.1.1 Overview of building a basic configuration system 46
 - 2.1.2 Installing a relay system 46
 - 2.1.3 Procedure for installing a relay system from supplied media 47
 - 2.1.4 Procedure for installing a relay system by deploying from the management server 49
 - 2.1.5 Procedure for setting up a relay system 49
 - 2.1.6 Procedure for installing Remote Installation Manager only 50
- 2.2 Building offline management configuration systems 53
 - 2.2.1 Overview of building an offline management configuration system 53
- 2.3 Building agentless configuration systems 54
 - 2.3.1 Overview of building an agentless configuration system 54
- 2.4 Building support service linkage configuration systems 55
 - 2.4.1 Overview of building a support service linkage configuration system 55
- 2.5 Building Active Directory linkage configuration systems 56
 - 2.5.1 Overview of building an Active Directory linkage configuration system 56
- 2.6 Building MDM linkage configuration systems 57
 - 2.6.1 Overview of building a MDM linkage configuration system 57
- 2.7 Building network monitoring configuration systems 58
 - 2.7.1 Overview of building a network monitoring configuration system 58
 - 2.7.2 Enabling the network monitor 58
- 2.8 Building JP1/NETM/NM - Manager linkage configuration systems 61
 - 2.8.1 Overview of building a JP1/NETM/NM - Manager linkage configuration system 61
- 2.9 Building JP1/IM linkage configuration systems 62
 - 2.9.1 Overview of building a JP1/IM linkage configuration system 62
- 2.10 Building a cluster system 64
 - 2.10.1 Overview of building a cluster system 64
 - 2.10.2 Procedure for creating a group resource on the primary server 64
 - 2.10.3 Setting up JP1/IT Desktop Management 2 on the primary server 68
 - 2.10.4 Setting up JP1/IT Desktop Management 2 on the standby server 71

3 Changing settings 72

- 3.1 Procedure for changing the setting for connection to the database 73
- 3.2 Procedure for changing the folders that are used 77
- 3.3 Procedure for configuring operation log acquisition 78
- 3.4 Procedure for setting up the output folder for the revision history 82
- 3.5 Procedure for changing a port number 84

3.6	Procedure for changing the currency unit	86
3.7	Procedure for controlling the network bandwidth used for distribution	88
3.8	Procedure for changing login restrictions	90
3.9	Procedure for suppressing asset information registration and modification	92
3.10	Procedure for upgrading a database	94
3.11	Procedure for initializing a database	95
4	Customizing the settings specified when building a system	96
4.1	Settings for building a minimal configuration system	97
4.1.1	Specifying search conditions (discovery from IP address)	97
4.1.2	Credentials used in discovery from IP address	97
4.1.3	Adding agent configurations	99
4.1.4	Procedure for adding relay system configurations	99
4.1.5	Procedure for using configuration files to configure processing	99
4.1.6	Procedure for changing agent monitoring items	100
4.2	Settings for building agentless configuration systems	102
4.2.1	Regularly updating agentless device information	102
4.3	Settings for building a support service linkage configuration system	103
4.3.1	Setting information for connecting to the support service	103
4.4	Settings for building Active Directory linkage configuration systems	105
4.4.1	Setting information for connecting to Active Directory	105
4.4.2	Setting the information acquired from Active Directory as an additional management item	105
4.4.3	Searching for devices registered in Active Directory	106
4.4.4	Specifying search conditions (searching Active Directory)	106
4.4.5	Setting a device as a management target	107
4.5	Settings for building MDM linkage configuration systems	109
4.5.1	Specifying settings to link with an MDM system	109
4.6	Settings for building network monitoring configuration systems	111
4.6.1	Editing devices in the network control list	111
4.6.2	Editing the automatic update of the network filter list	111
4.6.3	Adding network monitor settings	111
4.6.4	Changing assignment of network monitor settings	112
4.6.5	Enabling the JP1/NETM/NM - Manager linkage settings	112
4.6.6	Procedure for editing the network control settings file	113
4.6.7	Procedure for replacing a computer by a network control appliance when the network monitor on the computer is enabled	114
4.7	Settings for building JP1/IM linkage configuration systems	115
4.7.1	Procedure for setting the configuration file used for linkage with JP1/IM	115
5	Overwrite-installing the product and updating the components	116
5.1	Procedure for performing an overwrite installation of JP1/IT Desktop Management 2 - Manager	117
5.2	Procedure for performing an overwrite installation of an agent from the supplied media	119

- 5.3 Procedure for performing an overwrite installation of a relay system from supplied media 120
- 5.4 Procedure for performing an overwrite installation of a network access control agent from the supplied media 121
- 5.5 Overview of upgrading the entire JP1/IT Desktop Management 2 system 122
- 5.6 Procedure for upgrading JP1/IT Desktop Management 2 - Manager 124
- 5.7 Updating components 126
- 5.8 Procedure for registering components 128
- 5.9 Overview of performing an overwrite installation in a cluster system 129
- 5.10 Performing an overwrite installation from JP1/IT Desktop Management and other products to JP1/IT Desktop Management 2 130

6 Uninstalling products 132

- 6.1 Overview of uninstalling the entire system 133
- 6.2 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager 134
- 6.3 Procedure for uninstalling Remote Installation Manager 135
- 6.4 Procedure for uninstalling the agent 136
- 6.5 Procedure for uninstalling a relay system 137
- 6.6 Disabling the network monitor 138
- 6.7 Uninstalling a controller 140
- 6.8 Procedure for uninstalling JP1/IT Desktop Management 2 - Manager in a cluster system 141

7 Migrating environments 142

- 7.1 Procedure for replacing a management server 143
- 7.2 Replacing a computer with only Remote Installation Manager installed 147
- 7.3 Procedure for replacing computers on which an agent is installed 148
- 7.4 Procedure for replacing relay systems 149
- 7.5 Procedure for replacing computers for which network access control is enabled 151
- 7.6 Changing host names and IP addresses in the system configuration 152
 - 7.6.1 Procedure for changing the management server host name 152
 - 7.6.2 Procedure for changing the management server IP address 152
 - 7.6.3 Procedure for changing the host name or IP address of a relay system 154
 - 7.6.4 Procedure for changing logical host names in a cluster system 154
 - 7.6.5 Procedure for changing logical IP addresses in a cluster system 155
- 7.7 Procedure for switching the management server to which an agent connects 158
- 7.8 Procedure for switching the relay system to which an agent connects 159

8 Commands used for building-related operations 160

- 8.1 Executing commands 161
- 8.2 Command description format 163
- 8.3 updatesupportinfo (uploading support service information) 164
- 8.4 exportdb (acquiring backup data) 166
- 8.5 importdb (restoring backup data) 169
- 8.6 stopservice (stopping services) 173

- 8.7 getlogs (collecting troubleshooting information) 175
- 8.8 getinstlogs (collecting troubleshooting information about installation) 177
- 8.9 resetnid.vbs (resetting the host ID) 179

9 Troubleshooting 181

- 9.1 Overview of troubleshooting during building of an environment 182
- 9.2 Troubleshooting when building a minimal configuration system 184
 - 9.2.1 Troubleshooting during building of a management server 184
 - 9.2.2 Troubleshooting during agent installation 184
 - 9.2.3 Troubleshooting when two sets of device information appear for one computer 186
- 9.3 Troubleshooting during building of an offline management configuration system 187
 - 9.3.1 Switching from offline management to online management 187
 - 9.3.2 Switching from online management to offline management 188
- 9.4 Troubleshooting during building of an agentless configuration system 189
- 9.5 Troubleshooting during building of a support service linkage configuration system 190
- 9.6 Troubleshooting during building of an Active Directory linkage configuration system 191
- 9.7 Troubleshooting during building of an MDM linkage configuration system 192
- 9.8 Troubleshooting during building of a network monitoring configuration system 193
- 9.9 Troubleshooting during building of a cluster system 194
- 9.10 Troubleshooting during linkage with JP1/NETM/NM - Manager 195

Appendix 196

- A Miscellaneous Information 197
 - A.1 Port number list 197
 - A.2 Recognition procedure when an agent environment is changed 201
 - A.3 Summary of amendments 201

Index 205

1

Building a minimal configuration system (management servers and agents)

This chapter describes how to build a minimal configuration system (consisting of management servers and agents).

After building a minimal configuration system, you can change its settings or install other components to tailor the system to your objectives. If you intend to build a system other than a minimal configuration system, see [2. Building system configurations](#) first.

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](#)

1.2 Creating a management server environment

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

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.

1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager

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

Important note

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 note

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 note

On a computer running 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 note

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.)

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 **Permission Agreement** dialog box, check the displayed information, select **I accept the terms in 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.
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.

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 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.

11. 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.

1.2.3 Procedure for setting up a management server

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.
If you selected **Secondary** in the settings for using a cluster system, skip step 6, step 7, and steps 9 to 17.

6. 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.

7. 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.
The setting that controls the cache size when accessing the database only appears when the computer on which JP1/IT Desktop Management 2 - Manager is installed is running a 64-bit operating system.
8. 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.
9. 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 13.
10. In the view that appears, set whether to retain operation log data, and then click the **Next** button.
11. 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.
12. 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.
This view only appears when the computer on which JP1/IT Desktop Management 2 - Manager is installed is running a 64-bit operating system.
13. 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.
14. 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.
15. 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*.
16. 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.
17. 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.
18. In the **Confirm Setup Settings** view, make sure the setup is correct, and then click the **Next** button.

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

19. In the **Setup for Distribution by Using Remote Install Manager** view, enter the settings related to distribution using Remote Installation Manager, and then click the **Next** 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 *Job Management Partner 1 Version 10 Job Management Partner 1/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 Installation 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.

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.

20. In the view indicating that setup is complete, click the **OK** button.

If **Register components** appears, specify whether to register components after setup, and then click the **OK** button. Components include agents and network monitor agents. By registering these programs on the management server, you can deploy the agent software and install the network monitor agent from the user interface.

When you register a component, the **Component Registration** dialog box opens. In the dialog box, specify the settings related to component registration and update.

Tip

If you start setup after installation, you can specify the settings for updating a component in the window that indicates that setup is complete.

For details about updating components, see [5.7 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.

1.3 Registering a Product License

This chapter describes how to register 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.

To register a product license:

1. Display the Login window.
2. Click the **License** button.
3. In the displayed dialog box, click the **Register License** button.
4. In the displayed dialog box, select a license key file, and then click the **Open** button.

License registration is complete.

Tip

If you are not registering a license for the first time, you can also register a license from the **License Details** view, which is displayed by selecting **Product Licenses** in the Settings module and then **License Details**. Click the **Register License** button. In the displayed dialog box, select a license key file, and then click the **Open** button to complete license registration.

Tip

If you are not registering a license for the first time, you can also register a license from the **About** dialog box, which is displayed by selecting **Help** in the top left corner of the view and then selecting **About**. Click the **Register License** button. In the displayed dialog box, select a license key file, and then click the **Open** button to complete license registration.

Related Topics:

- [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. Building a minimal configuration system (management servers and agents)

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#/jplitdm/
```

#: This is the port number that was specified in the **Port Number Settings** view during setup. The default value of 31080 is specified for a simple installation.

2. Enter the user ID and password.
3. Click the **Log In** button.

The Home module is displayed if the user account is successfully authenticated.

The default user ID is `system`. The default password is `manager`. When you use the default user ID and password to log in, the **Change Password** dialog box is displayed. Change the password in the dialog box. Note that the **Change Password** dialog box is also displayed if you use a newly created user account to log in for the first time.

Tip

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 note

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**.

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 note

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

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 note

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

1. Building a minimal configuration system (management servers and agents)

Important note

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

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 note

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.

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.

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.

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 dialog box, click the **Next** button.

1. Building a minimal configuration system (management servers and agents)

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

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

Enter information for the following items according to the instructions of the wizard, and then click the **Next** button:

Installation folder settings

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

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

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.

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.

A dialog box for downloading the installation set appears.

5. In this dialog box, click the **Save** button.

The default file name is `ITDM2Agt.exe`.

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

Tip

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

Tip

You can create the information file for higher connection destinations (`dmhost.txt`) and store it in the JP1/IT Desktop Management 2 - Manager data folder. Then this file is imported into the installation set when the installation set is created. For details about the information file for higher connection destinations, see the description of automatic change of connection destinations for agents in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Distribution Function Administration Guide*.

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. 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.

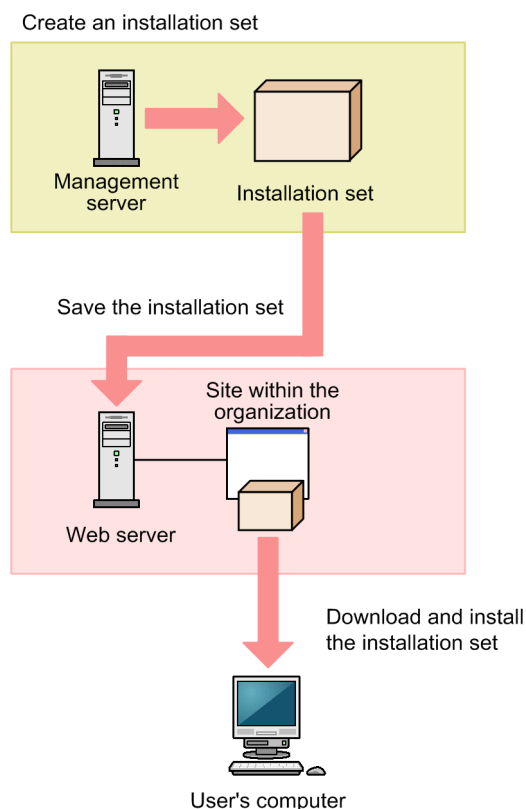
Advantage:

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.

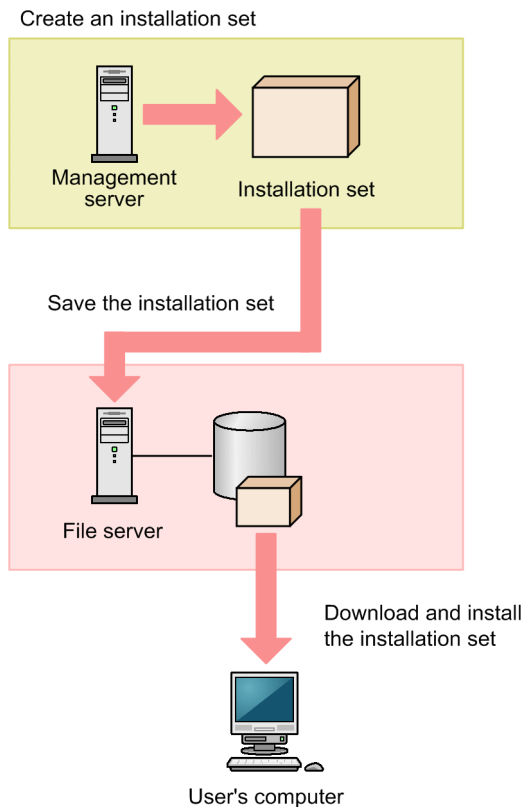
Advantage:

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:



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.

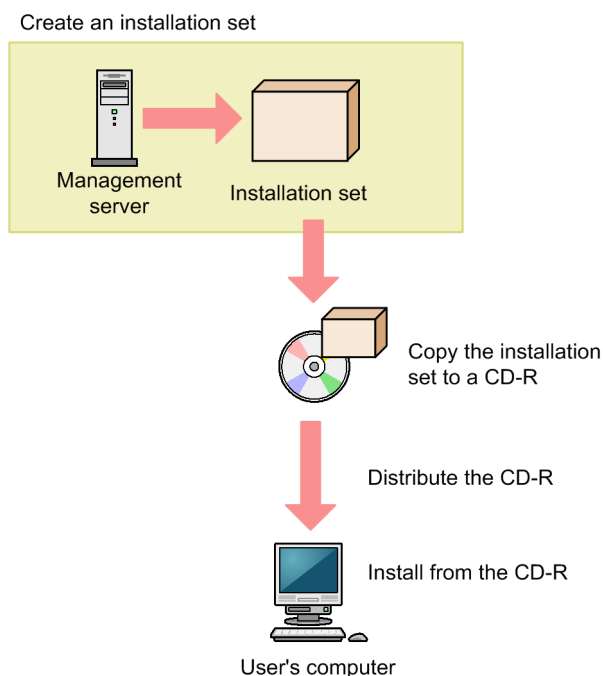
Advantage:

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.

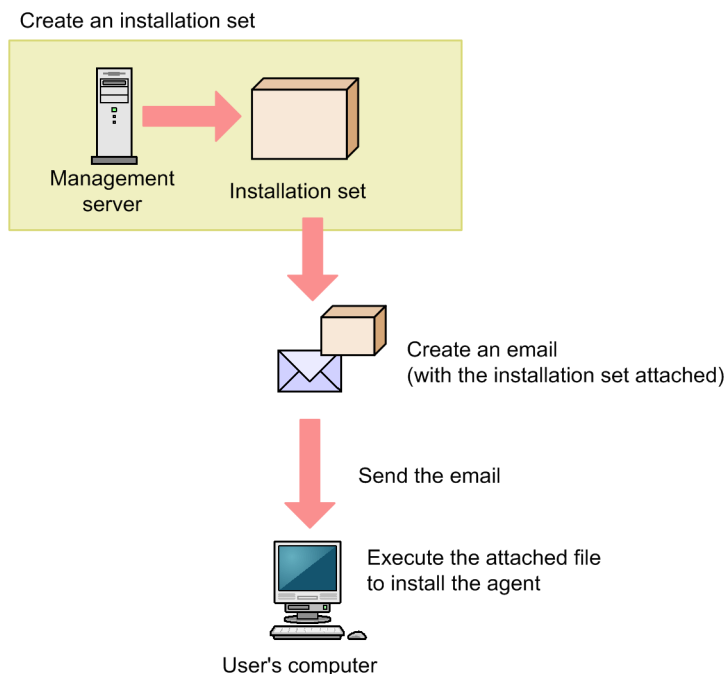
Advantage:

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\jplitdma\bin\jdnglogon.exe" (
start /w \\server-name\shared-folder-name\ITDM2Agt.exe
)
) else (
if not exist "%ProgramFiles%\Hitachi\jplitdma\bin\jdnglogon.exe" (
start /w \\server-name\shared-folder-name\ITDM2Agt.exe
)
)

```

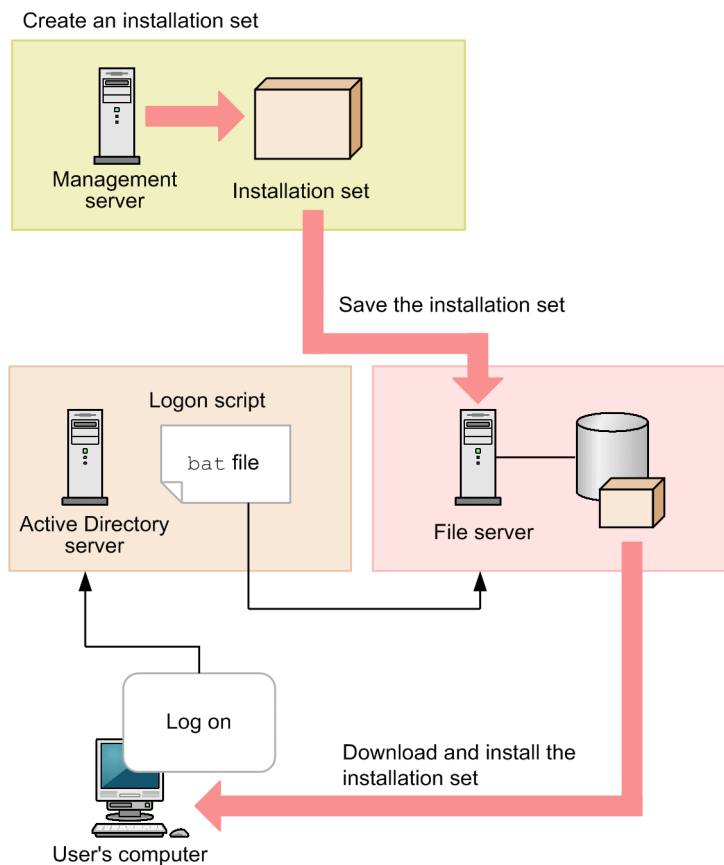
Advantage:

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 note

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

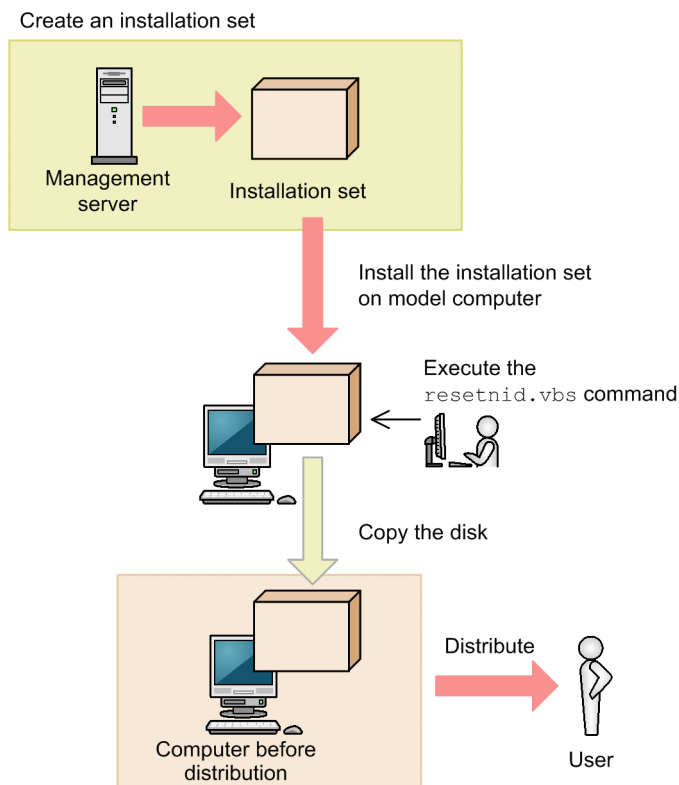
Advantage:

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

Disadvantage:

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

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



Related Topics:

- [1.6.1 Creating an installation set](#)
- [1.7.1 General procedure for checking the agent installation status](#)
- [8.9 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 note

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 note

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 note

On a computer that runs Windows 8.1, Windows 8, 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 note

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.

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\jplitdma. 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\jplitdma\ when the OS is installed on the C drive).

Important note

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

Important note

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.

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.

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 an information file for higher connection destinations (`dmhost.txt`) to set the connection destination. 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 *Job Management Partner 1 Version 10 Job Management Partner 1/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, 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 (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 **OK** 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.

1.7 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.

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 Device module.

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

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

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

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

Tip

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

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

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

2. Export device information.

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

3. Check the agent installation status.

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

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

1.7.2 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.
5. Click the **Start Discovery** button.
6. In the displayed dialog box, click the **OK** button.

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

1.7.3 Checking the device discovery status

In JPI/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.

1. Building a minimal configuration system (management servers and agents)

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

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

Tip

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

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 how to install and set up JP1/IT Desktop Management 2 - Asset Console, see the JP1 Version 10 JP1/IT Desktop Management 2 - Asset Console Planning and Configuration Guide.

2.1 Building a basic configuration system (relay system)

2.1.1 Overview of building a basic configuration system

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

1. Build the management server environment.
2. Install and set up the relay system program on the computers that will serve as relay systems.

This completes the process of building a basic configuration system.

Tip

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

Related Topics:

- [1.2 Creating a management server environment](#)
- [2.1.2 Installing a relay system](#)
- [2.1.5 Procedure for setting up a relay system](#)
- [2.1.6 Procedure for installing Remote Installation Manager only](#)

2.1.2 Installing a relay system

There are three 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.

Deploying the software to individual computers

You can deploy the relay system program to individual computers found by a discovery process. To deploy the relay system program individually, you need to create an agent configuration for the relay system. The administrator can then select a target computer in the user interface and deploy the agent configuration for the relay system to that computer individually. 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, or the method in which the program is individually deployed on target computers.

Tip

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

Related Topics:

- 2.1.3 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
- 2.1.4 Procedure for installing a relay system by deploying from the management server

2.1.3 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 note

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 note

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 note

On a computer running 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 note

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.

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\jplitdma`. 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\jplitdma\`.

Important note

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

Important note

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.

2.1.4 Procedure for installing a relay system by deploying from the management server

You can install relay systems by deploying the software to selected managed computers.

Tip

To install a relay system by deploying it from the management server, you first need to prepare the agent configuration for the relay system.

Tip

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

To install a relay system by deploying the software to individual computers:

1. In the Settings module, select **Agent** and then **Agent Deployment** to display the **Agent Deployment** view.
2. Select the computer on which you want to deploy the relay system.
3. Click the **Deploy Agent** button.
4. In the dialog box that appears, select the agent configuration you want to apply.
5. Click the **OK** button.

A relay systems is deployed to the computer you selected. To deploy the relay system on multiple computers, repeat the steps above for each computer. You can view the deployment status in the **Agent Deployment** view of the Settings module.

2.1.5 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 *Job Management Partner 1 Version 10 Job Management Partner 1/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.

2.1.6 Procedure for installing Remote Installation Manager only

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

Important note

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 note

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 note

On a computer running 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 note

Before installation, make sure that all Windows applications have been closed. If you perform installation without terminating Remote Installation Manager, restart the OS regardless of whether installation was successful. If the service does not start or Remote Installation 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.

To install Remote Installation 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 for Usage** dialog box, select **Accept the license agreement for usage**, 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 dialog box where you select a component to install, select **Remote Install Manager** as the component to be installed, specify the installation method, and then click the **Next** button.
If you are installing Remote Install Manager on its own, you do not need to install the Manager program. From the pull-down menu for Manager, select **This feature will not be available.**
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 Installation Manager is complete. Restart the computer if requested to do so.

If you only installed Remote Installation Manager, you can start using it immediately. To do so, start Remote Installation Manager, specify the host name or IP address of the management server and the database connection information, and log on.

2.2 Building offline management configuration systems

2.2.1 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 a minimal configuration system \(management servers and agents\)](#)

2.3 Building agentless configuration systems

2.3.1 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](#)

2.4 Building support service linkage configuration systems

2.4.1 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 *Job Management Partner 1 Version 10 Job Management Partner 1/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](#)

2.5 Building Active Directory linkage configuration systems

2.5.1 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](#)

2.6 Building MDM linkage configuration systems

2.6.1 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](#)

2.7 Building network monitoring configuration systems

2.7.1 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.

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.

Related Topics:

- [4.1.1 Specifying search conditions \(discovery from IP address\)](#)
- [4.6.1 Editing devices in the network control list](#)
- [2.7.2 Enabling the network monitor](#)
- [4.6.3 Adding network monitor settings](#)
- [4.6.4 Changing assignment of network monitor settings](#)


2.7.2 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 Device module.
2. In **Device Inventory** in the menu area, select the desired network segment from **Network List**.
3. In the information area, select a computer on which the agent has been installed.
4. In **Action**, select **Enable Network Access Control**.

The network monitor of the selected computer is enabled. The network of the selected network segment is monitored.

For computers for which the network monitor is enabled,  or

 is displayed as the management type. In addition,  is displayed for the group in the menu area.

Important note

Do not uninstall the network monitor agent from a computer for which the network monitor is enabled. Uninstalling the network monitor agent disables the network monitor for the network segment to which the computer belongs.

Important note

If the menu area displays the operation status of the network monitor as **Managing** or **Starting management**, the following restrictions apply:

- The group of the applicable network cannot be deleted.
- Computers for which the network monitor is enabled cannot be excluded or deleted.

Important note

When enabling the network monitor for a computer running Windows Server 2003, make sure that WinPcap is not installed. If WinPcap is installed, uninstall WinPcap before enabling the network monitor.

Important note

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

Tip

You can also enable the network monitor by selecting **Network Access Control** and then **Assign Network Access Control Settings** in the Settings module, and then using the **Assign Network Access Control Settings** view.

Tip

You can also enable the network monitor by using the provided media to install JP1/IT Desktop Management 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.

2.8 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 Control** to display the **Assign Network Monitor 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.

Related Topics:

- [1.1 Overview of building a minimal configuration system](#)

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_jpl_itdm_attr_ja.conf
```

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

```
JP1/IT Desktop Management 2-installation-folder\mgr\definition  
\hitachi_jpl_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 *Job Management Partner 1 Version 10 Job Management Partner 1 Version 10 Job Management Partner 1/Base User's Guide*. For details about the JP1/IM installation procedure and settings, see the *Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Configuration Guide*. For details about the location and format of the definition file for extended event attributes, see the manual *Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Important note

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 group resource 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 group resource 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 group resource 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](#)
- [2.10.2 Procedure for creating a group resource 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 group resource 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 group for the management server that is separate from any cluster groups that are already registered in Windows Server Failover Cluster.

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	IP address resource
	Network name resource
	Shared disk (physical disk) resource
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
	JP1_ITDM2_Service
	JP1_ITDM2_Agent Control

[#]: If the OS is Windows Server 2012 or Windows Server 2008, you must create resources from the CLI.

If the OS is Windows Server 2012, 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 ""
```

If the OS is Windows Server 2008, execute the following command from the command prompt as a user with administrator permissions:

```
cluster res "name-of-JP1_ITDM2_Web Server-service-resource" /priv StartupParameters=""
```

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 group resource is created.

For details about how to create a group resource, see the documentation for Windows Server Failover Cluster.

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
<ul style="list-style-type: none"> IP address resource Network name resource Shared disk (physical disk) resource 	Failover threshold	1 (recommended)
	Failover period (in seconds)	900 (recommended)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM2_DB Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_DB Service	Name	Specify a name.
	Resource type	Set a generic service.
	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.
	Dependency	Set the network name resource and the shared disk (physical disk) resource.
	Service name	Set HiRDBEmbeddedEdition_JE1.
	Registry copy	Not specified.
	Failover threshold	0 (fixed)
	Failover period (in seconds)	0 (fixed)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM2_DB Cluster Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_DB Cluster Service	Name	Specify a name.
	Resource type	Set a generic service.
	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.
	Dependency	Set a resource for JP1_ITDM2_DB Service.
	Service name	Set HiRDBClusterService_JE1.
	Registry copy	Not specified.
	Failover threshold	1 (recommended)
	Failover period (in seconds)	900 (recommended)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM2_Web Container settings

Resource name	Setting item	Setting value
JP1_ITDM2_Web Container	Name	Specify a name.
	Resource type	Set a generic service.
	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.

Resource name	Setting item	Setting value
JP1_ITDM2_Web Container	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Service name	Set JP1_DTNAVI_WEBCON.
	Registry copy	Not specified.
	Failover threshold	1 (recommended)
	Failover period (in seconds)	900 (recommended)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM2_Web Server settings

Resource name	Setting item	Setting value
JP1_ITDM2_Web Server	Name	Specify a name.
	Resource type	Set a generic service.
	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.
	Dependency	Set the network name resource.
	Service name	Set JP1_DTNAVI_WEBSVR.
	Registry copy	Not specified.
	Failover threshold	1 (recommended)
	Failover period (in seconds)	900 (recommended)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM2_Service settings

Resource name	Setting item	Setting value
JP1_ITDM2_Service	Name	Specify a name.
	Resource type	Set a generic service.
	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.
	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Service name	Set JP1_DTNAVI_MGRSRV.
	Registry copy	Not specified.
	Failover threshold	1 (recommended)
	Failover period (in seconds)	900 (recommended)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM2_Agent Control settings

Resource name	Setting item	Setting value
JP1_ITDM2_Agent Control	Name	Specify a name.
	Resource type	Set a generic service.
	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.
	Dependency	Set the JP1_ITDM2_DB Cluster Service resource.
	Service name	Set JP1_DTNAVI_AGCTRL.
	Registry copy	Not specified.
	Failover threshold	1 (recommended)
	Failover period (in seconds)	900 (recommended)
	Wait timeout (in seconds)	300 (recommended)

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.

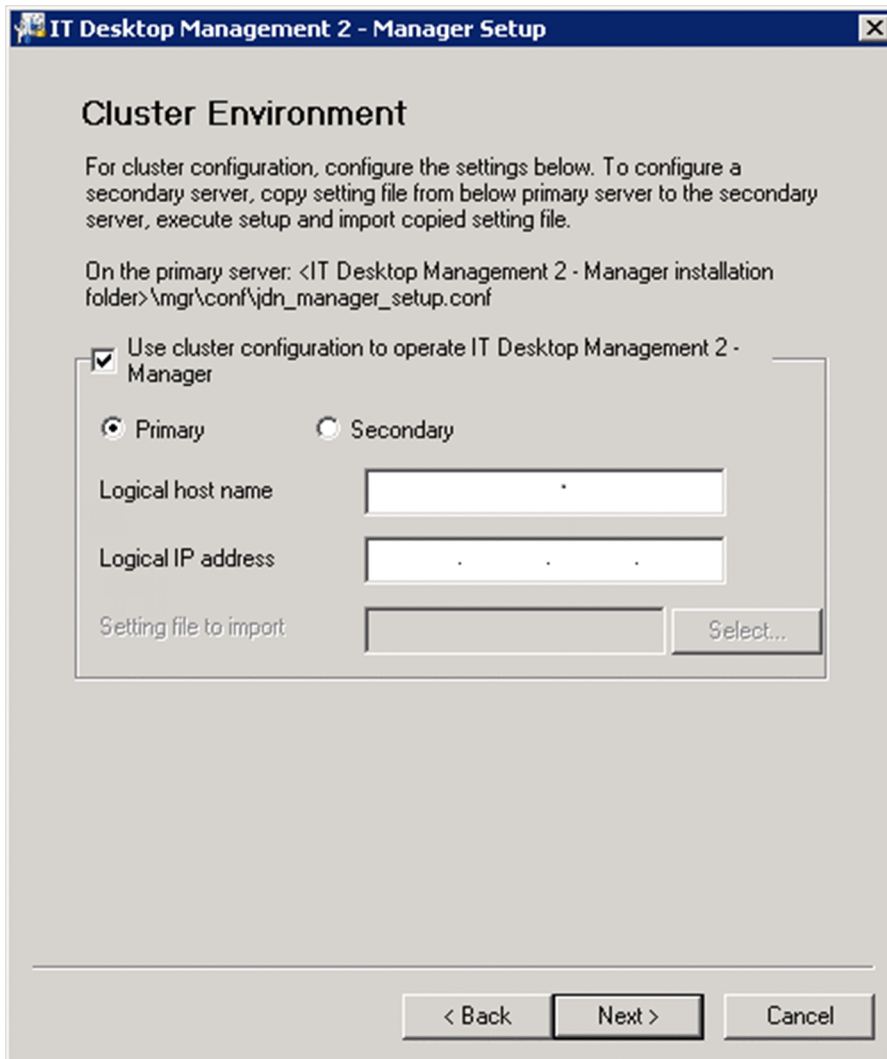
Important note

If the OS is 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**.

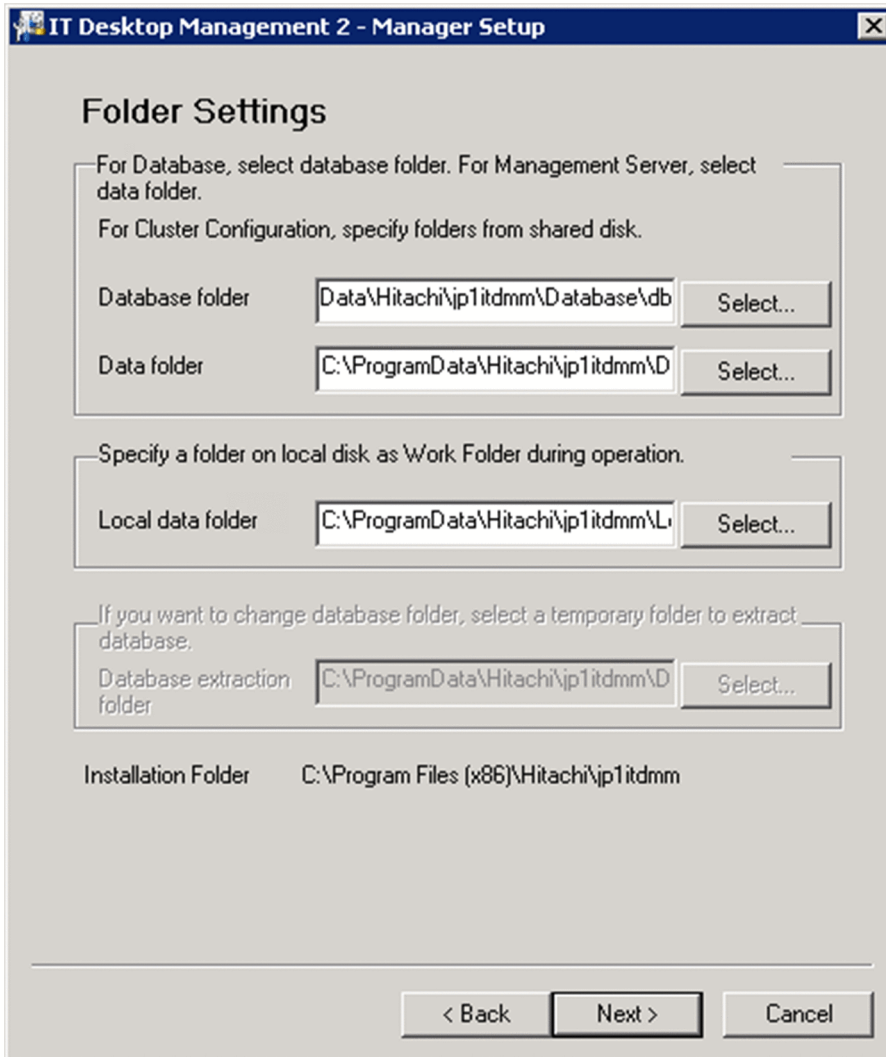
For this operation, you do not need to set **Setting file to import**.

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:

- [1.2.3 Procedure for setting up a management server](#)

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:

- [1.2.3 Procedure for setting up a management server](#)

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.

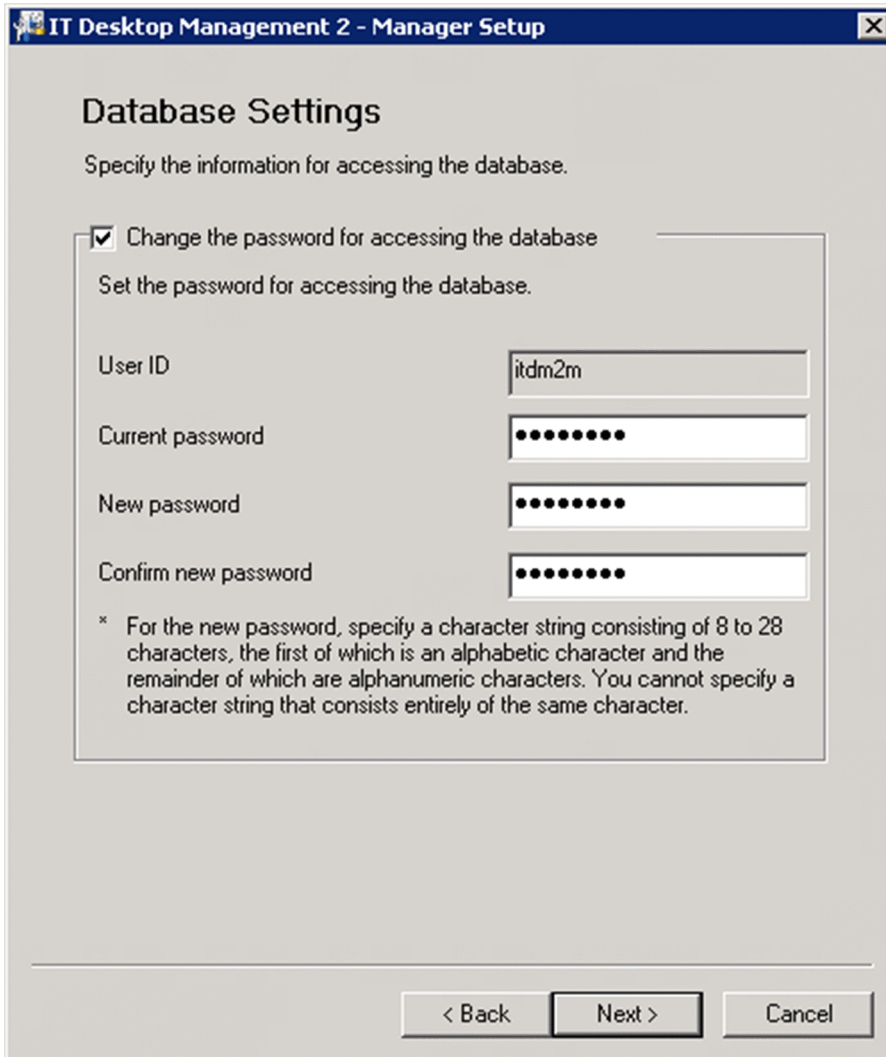
To set the password for accessing the database:

1. Stop the management server services.

From the Windows **Start** menu, select **Administrative Tools** and then **Services**. In the dialog box that appears, right-click the service name and click **Stop** to stop the service. You need to stop the following services:

- JP1_ITDM2_Agent Control
- JP1_ITDM2_Service
- JP1_ITDM2_Web Container
- JP1_ITDM2_Web Server

2. From the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management 2 - Manager**, **Tools**, and then **Setup**.
3. In the Setup view, 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, select the **Change the password for accessing the database** check box, enter the current and new passwords, and then click the **Next** button.



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

7. 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.

If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.

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

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

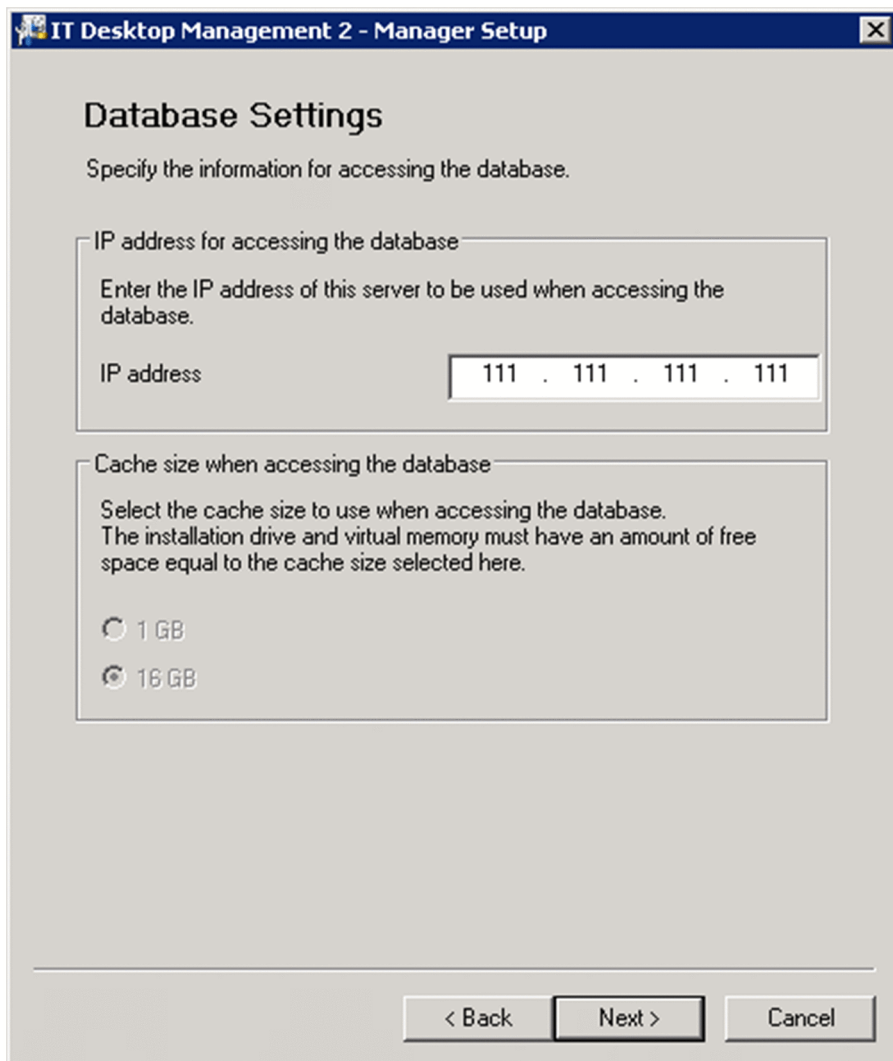
To change the database connection address:

1. Stop the management server services.

On the Windows **Start** menu, select **Administrative Tools** and then **Services**. In the dialog box that opens, right-click a service name, and then select **Stop** to stop the service. Stop the following services:

- JP1_ITDM2_Agent Control
- JP1_ITDM2_Service
- JP1_ITDM2_Web Container
- JP1_ITDM2_Web Server

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.
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.

If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.

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

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

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 note

On a computer running 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 in the database in the old folder is passed to the new folder.

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.

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 note

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.

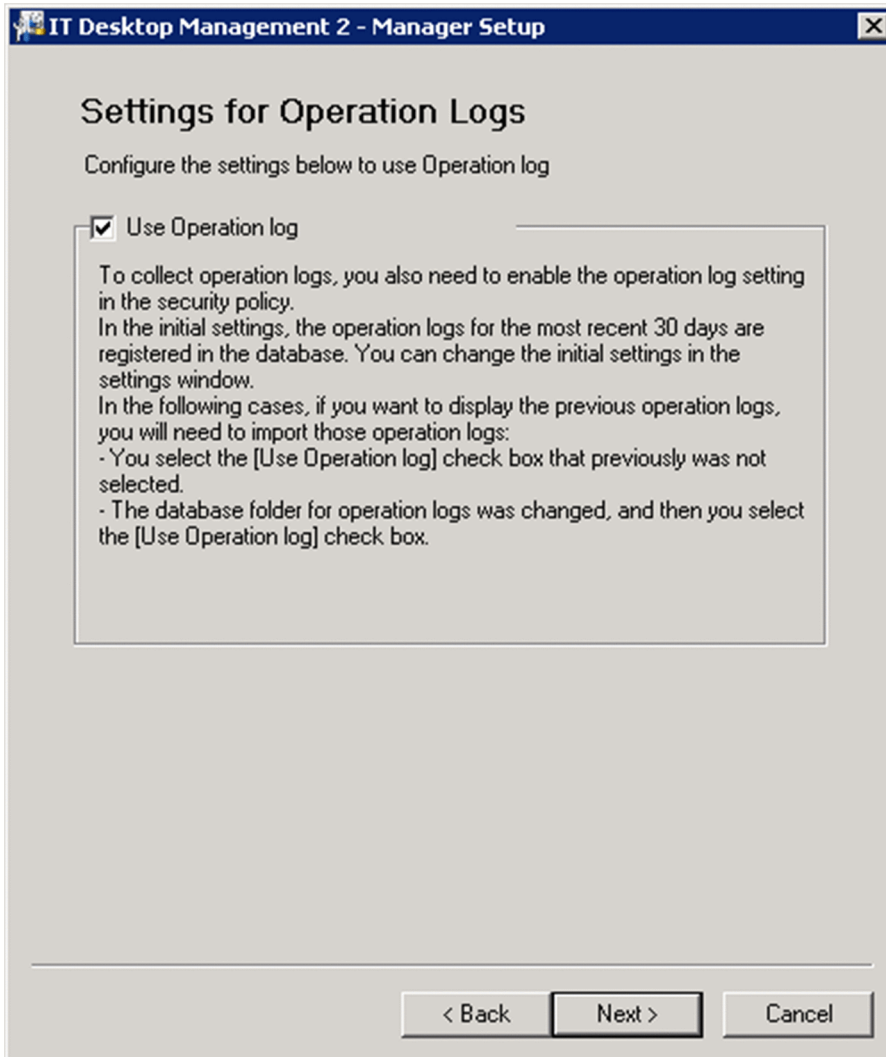
Important note

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

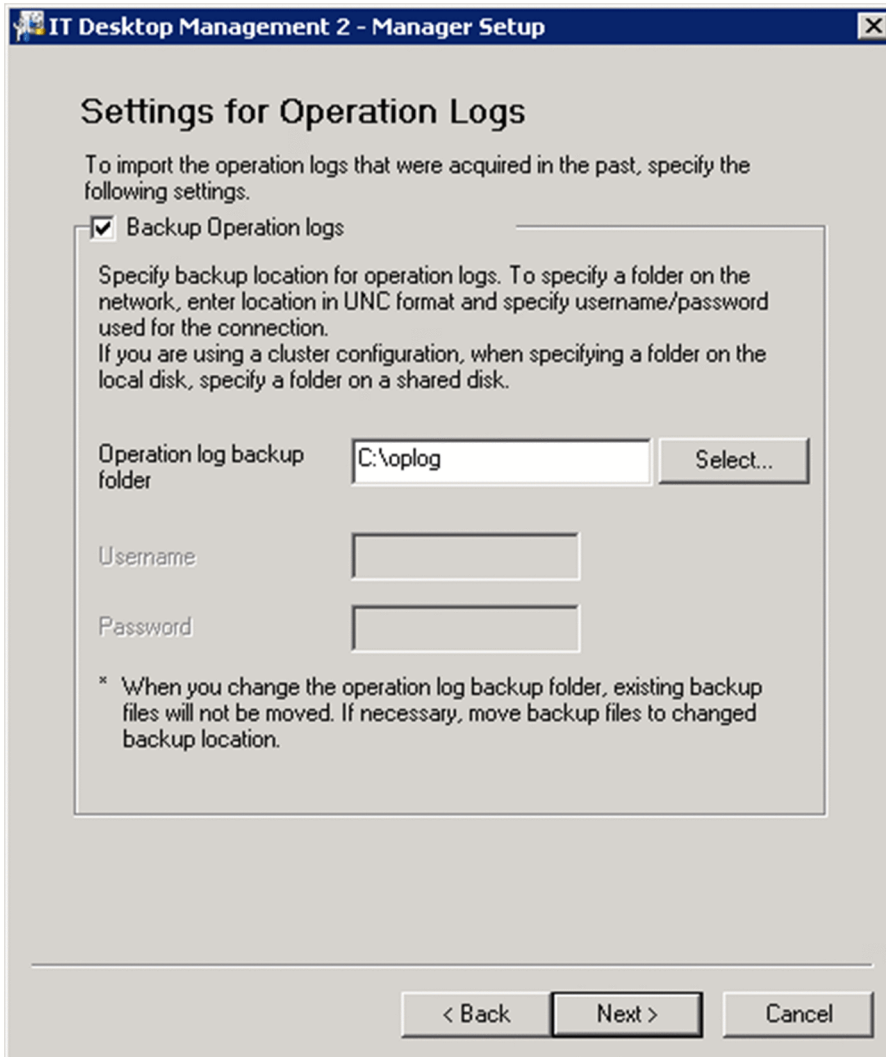
- Folders under *system-drive:\program files\WindowsApps*
- Folders in storage areas created by virtual provisioning

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 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**.

- **Operation log database**

Specify the folder in which you want to create the database for saving the operation logs. Specify the folder on a disk with free space greater than the capacity shown in **Required capacity**.

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.
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.
When a service needs to be stopped, a dialog box asking if it is OK to stop the service opens. Click the **OK** button to stop the service.
16. In the **Setup Complete** view, click the **OK** button.

Operation logs are now available.

Important note

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.

IT Desktop Management 2 - Manager Setup

Output Settings for Saving the Revision History

Specify these settings if you want to regularly output and save the revision history.

Regularly output and save the revision history

Specify the folder to which the revision history will be output. To specify a folder on the network, do so by using UNC syntax. In addition, specify the user name and password used to connect to the output folder. If you are using a cluster configuration, when specifying a folder on the local disk, specify a folder on a shared disk.

Output folder for the revision history:

Username:

Password:

< Back Next > Cancel

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

Important note

On a computer that runs 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.
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.
If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.
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 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 note

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.

IT Desktop Management 2 - Manager Setup

Port Number Settings

Specify the port numbers.

Management console connection port number	<input type="text" value="31080"/>
Port number for Agent connection	<input type="text" value="31000"/>
Agent startup port number	<input type="text" value="31001"/>
Port number used by the server	<input type="text" value="31002"/> . <input type="text" value="31012"/>
Remote Control port number	<input type="text" value="31016"/> . <input type="text" value="31020"/>

< Back Next > Cancel

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 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.

Remote Control port number

Enter the port number used by the remote control functionality.

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.

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.

If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.

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

The port number is changed.

3.6 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.

IT Desktop Management 2 - Manager Setup

Other Settings

Configure Other Settings

Currency Unit Setting
Set the currency unit to use for asset management.

Currency unit

Control network bandwidth from management server
Enter a value between 2 to 1024 (in MB/sec) for the maximum transmission speed of the management server.
The value entered here will be used as the maximum transmission speed when software is distributed by using ITDM-compatible distribution.

Maximum transmission speed MB/sec

< Back Next > Cancel

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.

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.

If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.

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

The currency unit is changed.

3.7 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 a network bandwidth:

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.

IT Desktop Management 2 - Manager Setup

Other Settings

Configure Other Settings

Currency Unit Setting
Set the currency unit to use for asset management.

Currency unit

Control network bandwidth from management server
Enter a value between 2 to 1024 (in MB/sec) for the maximum transmission speed of the management server.
The value entered here will be used as the maximum transmission speed when software is distributed by using ITDM-compatible distribution.

Maximum transmission speed MB/sec

< Back Next > Cancel

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.

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.

If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.

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

You can now control the network bandwidth.

3.8 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.

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.

IT Desktop Management 2 - Manager Setup

Other Settings

Configure Other Settings

Login information settings

To change the maximum values related to login information, specify the following settings:

Number of consecutive login failures before the account is locked (0: Do not lock the account) (0 to 10)

Number of days until the password expires (0: Does not expire) days (0 to 999)

Settings for asset management

Select this option if you want to install and use IT Desktop Management 2 - Asset Console. If you select this option, you will be able to perform operations on asset information from IT Desktop Management 2 - Asset Console only. This helps you maintain the consistency of asset information, because operations on asset information from the operation window are suppressed. Operations on USB devices are performed in the operation window.

Suppress operations on asset information from the operation window

< Back Next > Cancel

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.

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.

If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.

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

The changes to login restrictions take effect.

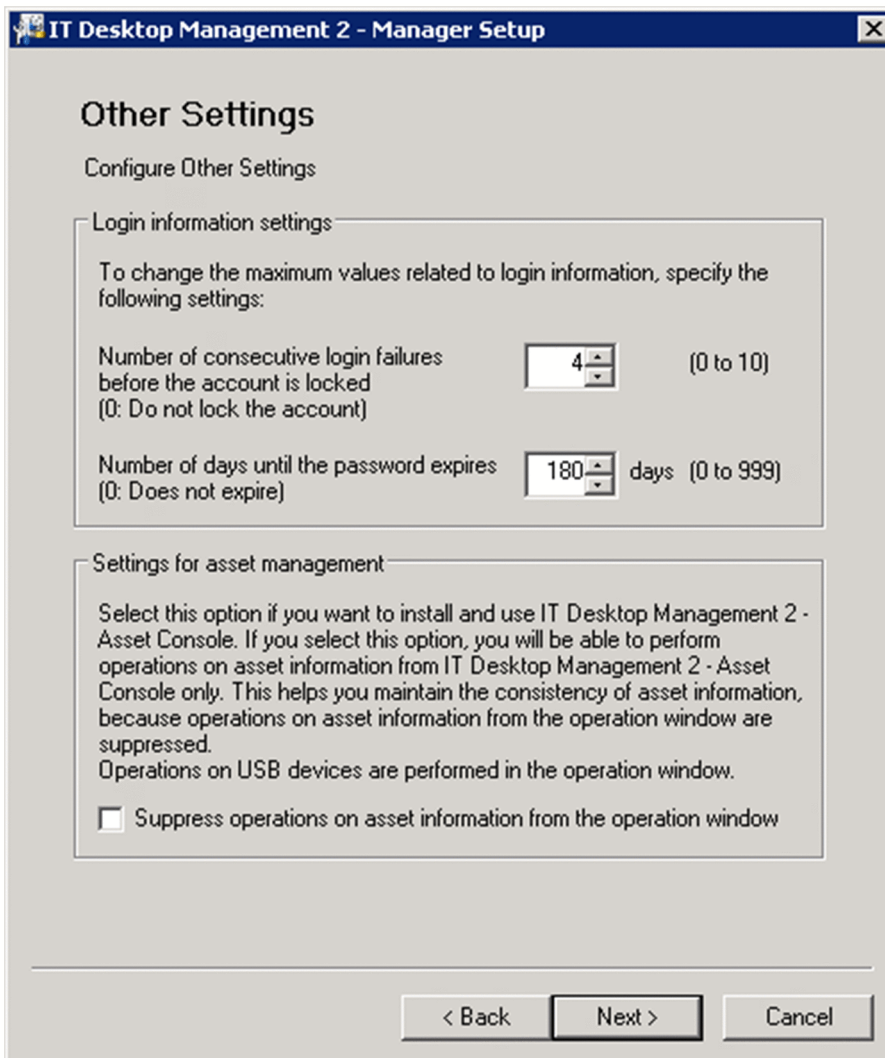
3.9 Procedure for suppressing asset information registration and modification

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.
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.
If a service needs to be stopped, a dialog box appears asking permission to do so. Click the **OK** button to stop the service.
9. In the **Setup Complete** view, click the **OK** button.

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

3.10 Procedure for upgrading a database

This is a management server setup item.

If you performed an overwrite installation of JP1/IT Desktop Management 2, and you need to upgrade a database, use setup.

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.
5. In the **Database Upgrade Settings** view, specify the upgrade settings, and then click the **Next** button.
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 [5.7 Updating components](#).

The database is upgraded.

3.11 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.
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 [5.7 Updating components](#).

The database is initialized.

Important note

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.

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 a discovery range.
The discovery range named Management Server Segment is set by default. The management server segment is a segment that contains a management server.
4. In **Credentials Used**, specify credentials.
Specify credentials if you want to perform a search by using credentials. After registering the credentials, in **Search Node Locations**, assign credentials to each discovery range.
5. Edit **Auto Discovery Schedule**.
Specify the schedule if you want to regularly perform searches according to the determined schedule.
6. Edit **Edit Discovery Option**.
Specify operations for cases in which a new device is discovered after the device search.
7. Edit **Notification of Discovery Completion**.
To send a notification email to administrators of JP1/IT Desktop Management 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 note

The device type of a computer with the following OSs: Windows Me, Windows 98, Windows 95, and Windows NT 4.0, might be classified as Unknown after discovery.

Important note

If multiple network cards are used for a single device, when a search is performed using ICMP, the device is discovered as multiple devices.

Tip

Specify a user ID to be used in authentication for Windows administrative shares in the following format if the ID is to be authenticated as a domain user: *User ID@FQDN (fully qualified domain name)*, or *domain name \user ID*. The fully qualified domain name is a format in which no host name or domain name are omitted. For example, specify an ID in the following format: `User001@PC001.hitachi.com`.

Tip

If Windows administrative share authentication is used, administrative share setting of a computer must be enabled in advance.

A search is performed by combining credentials for each discovery range. By default, all the specified credentials are used for discovery. If, however, SNMP community names differ among departments, or the Windows credentials differ among computers, you can perform a search by selecting the credentials necessary for each discovery range.

Note that the credentials used in discovery from IP addresses are also used when the agent is delivered. To deliver the agent after discovery, in the Settings module, select **Discovery** and then **Configurations**, and in the **IP Address Range** view, specify Windows administrative share credentials for the discovery range that includes the computer to which the agent is to be delivered.

4.1.3 Adding agent configurations

To set different monitoring intervals for each computer, you can add agent configurations.

To add agent configurations:

1. Display the Settings module.
2. In the menu area, select **Agent**, and then **Agent Configuration and Installation Set Creation**.
3. In the information area, click **Add Agent Configuration**.
4. In the displayed dialog box, type the agent configuration information, and then click **OK**.

The agent configuration is added and displayed in the list of agent configurations.

The added agent configuration can be applied to computers with the agent already installed by assigning the agent configuration in the **Assign Agent Configuration** view.

4.1.4 Procedure for adding relay system configurations

In environments in which Remote Installation 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 **Agent Configuration and Installation Set Creation**.
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 **Assign Agent Configuration** 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.

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
<code>State_AfterAgentUninstalling#</code>	Specifies whether the system interprets 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
<code>Report_Data_MakeTime</code>	When to compile data for reports	00:00 to 23:59	23:00
<code>Report_Digest_MakeTime</code>	When to create digest reports	00:00 to 23:59	06:00
<code>DB_MaintenanceTime</code>	When to perform database maintenance	00:00 to 23:59	05:00
<code>ChangeHistory_GetTime</code>	When to acquire revision history data	00:00 to 23:59	00:00
<code>OpLog_DB_DeleteTime</code>	When to maintain the database of automatically acquired operation log data	00:00 to 23:59	01:00

#:

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.

The following is an example of a configuration file setting:

```
#
# Configuration file
#
# Time for collecting revision history
ChangeHistory_GetTime=00:00
```

4.1.6 Procedure for changing agent monitoring items

You can use an inventory settings file (`jdnng_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:

- Using a text editor, create an inventory settings file (`jdnng_inventory.conf`) with the content shown in the table below, and place it in the `%ALLUSERSPROFILE%\HITACHI\jpltdma\conf` folder.

Section	Key name	Description	Setting values	Default setting
SystemInventory	<code>DHCPLeaseExpires</code>	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.	<ul style="list-style-type: none"> 0: Do not monitor 1: Monitor 	0
	<code>DHCPLeaseObtained</code>	You can specify whether to monitor for changes in the time of obtaining the DHCP lease.	<ul style="list-style-type: none"> 0: Do not monitor 	0

Section	Key name	Description	Setting values	Default setting
SystemInventory	DHCPLeaseObtained	If this section or key is omitted or the specified value is invalid, the system operates as if 0 were specified.	<ul style="list-style-type: none"> 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.

4.2 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.

4.3 Settings for building a support service linkage configuration system

4.3.1 Setting information for connecting to the support service

To judge whether the Windows security update is up to date, you must regularly download the latest updated program information from the support service site. To do this, you must set information for connecting to the support service site.

Connecting to the support service site allows the information about updated programs to be automatically updated..

By obtaining the latest information from the support service site, you can use the security policy to judge whether the latest updated program is applied to the managed computers.

Important note

To connect to the support service site, you must have a contract for the support service.

To set information for connecting to the support service:

1. Display the Settings module.
2. In the menu area, select **General** and then **Product Update**.
3. In the information area, specify information about the support service to be connected.
For details about the information of the support service to be connected, check the Release Notes. Click the **Test** button to check if a connection to the specified support service site can be established.
In **Edit Import Schedule**, you can specify the schedule to obtain the latest information about updated programs from the support service site.
In addition, in **Specify users to receive Product Update notification e-mails**, you can specify recipients of a notification mail that informs users that the update program list on the Security module has been updated.
4. Click the **Apply** button.

The latest support information is downloaded from the support service site according to the schedule specified in **Edit Import Schedule**. In addition, when the update programs list is updated after downloading, a notification mail is sent to the specified addresses.

Tip

If a management server cannot connect to the external network, use computers that can connect to the external network to download the support information from the support service site. You can register the downloaded support information on the management server by using the `updatesupportinfo` command.

Tip

When the security policy is updated after the information is obtained from the support service site, the security status of a device is judged.

Related Topics:

- [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 **Asset Management** and then **Asset Field Definitions**.
3. Create an item for obtaining the information from the Active Directory, or edit an existing item.
To create a new item, click the **Add Fields** button. To edit an existing item, select the item and then click the **Edit** button.
4. In the displayed dialog box, specify **Data Source** for **Active Directory**.
5. Specify the Active Directory management item from which information is obtained.

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

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.
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 note

The search cannot be performed if the Active Directory domain to be connected to is not specified. In the **Active Directory** view, specify a domain for Active Directory.

Settings for the search conditions are completed.

If you want to immediately start searching with the specified search conditions, click the **Start Discovery** button. If you do not perform an immediate search, the search is performed according to the **Auto Discovery Schedule**.

To check the search execution status and results, in the Settings module, select **Last Discovery Log**, and then the **Active Directory** view.

Related Topics:

- [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 Device module.

Tip

When the network monitor function is installed on a device, the device network connection is controlled at the time it is detected, based on the settings for the network monitor and the network control list. When a device is set as a management target, its network connection is automatically allowed.

Important note

One license is assigned to a device when it is set as a management target. If the number of licenses is insufficient, the devices without a license cannot be set as management targets. If this is the case, you need to purchase additional licenses.

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 note

Only a single MDM linkage setting can be specified for each MDM server. If more than one setting is specified for a single MDM server, JP1/IT Desktop Management 2 might fail to control smart devices.

To set information for linking with an MDM system:

1. Obtain a server certificate for an MDM product.
 1. In the Web browser, access the portal of MDM products.
 2. Export the server certificate to a file.For Internet Explorer:
 - (i) Right click on the window, and select **Properties, Certificates, Details**, and then **Copy to File**.
 - (ii) Use the certificate export wizard to export the certificate in the DER encoded binary X.509 format.For Firefox:
 - (i) Right click on the window, and select **View Page Info, Security, View Certificate, Details**, and then **Export**.
 - (ii) In the dialog box for saving certificates, save the certificate in the X.509 Certificate (DER) format.
2. Copy the server certificate obtained in step 1 to a management server.
3. Import the server certificate to the management server.

Execute the following command in the command prompt of the management server:

```
JP1/IT Desktop Management 2 - Manager installation folder\mgr\uCPSB\jdk\jre\bin\keytool.exe -import -keystore JP1/IT Desktop Management 2 - Manager installation folder\mgr\uCPSB\jdk\jre\lib\security\cacerts -file \server certificate path\ -alias \server certificate alias\#
```

#: The string *server certificate path* indicates the path of the server certificate copied in step 2. The string *server certificate alias* indicates another name of the server certificate to be imported. You can specify any name for the alias.

When the command is executed, you are asked to type a password to import the server certificate. Type the password. The default password is change it.
4. Display the Settings module of JP1/IT Desktop Management 2.
5. In the menu area, select **General** and then **MDM Linkage Settings**.
6. In the information area, click the **Add** button in the **MDM Linkage Settings**.
7. In the displayed dialog box, specify information about the MDM system to be connected to.
8. Click the **Test** button to check if a connection to the specified MDM system can be established.
9. Edit **Collection Schedule**.

Specify the schedule if you want to regularly update the smart device information according to a determined schedule.

10. Click **OK**.

11. In the information area, click the **Edit** button in **Edit Discovery Option**.

12. In the displayed dialog box, specify whether the discovered smart device is to be automatically managed.

The smart device information is obtained from the MDM system according to the schedule specified in **MDM Linkage Settings**.

To link with MobileIron, you must assign API permission in MobileIron to the user ID specified in **MDM Linkage Settings**.

Tip

Discovered smart devices are to be managed according to the settings specified in **Edit Discovery Option**. If the discovered devices are not specified as a device to be automatically managed, to manage the smart devices, you must specify the smart devices as management target in the **Discovered Nodes** view of the Settings module.

Tip

After importing the server certificate that you obtained from the MDM system to the management server, if you change the server certificate, you need to obtain the changed server certificate, and then re-import it to the management server.

Related Topics:

- [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, click the **Edit** button for the device that you want to edit.
4. In the displayed dialog box, edit the necessary information, and then click **OK**.

The network control settings of the selected device are updated.

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**.

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.

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
<code>NetworkControl_Default</code>	Specifies how the network connections of detected devices added to the network control list will be controlled.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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
```

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.

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 2.4 gigabytes of free space on the hard disk drive.

Important note

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 note

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 note

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 note

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 for Usage** dialog box, check the displayed information, select **Accept the license agreement for usage**, and then click the **Next** button.

5. 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.

6. 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 [5.7 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.

Related Topics:

- [1.2.3 Procedure for setting up a management server](#)

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 note

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 note

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 note

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.

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 note

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 note

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 note

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.
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 note

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 note

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.

5.5 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 Installation 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 note

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 note

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 note

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.

Important note

You cannot upgrade to JP1/IT Desktop Management 2 from JP1/IT Desktop Management operating in a multi-server configuration system.

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 *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Overview and System Design Guide*.

Related Topics:

- [5.6 Procedure for upgrading JP1/IT Desktop Management 2 - Manager](#)
- [5.7 Updating components](#)

5.6 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 note

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 note

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. If you do not have the old version of the program, contact the support service.

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 *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Overview and System Design Guide*.

5.7 Updating components

Components include agents and network access control agents. You can upgrade these programs as follows:

Important note

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 note

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 [5.5 Overview of upgrading the entire JP1/IT Desktop Management 2 system](#).

Tip

If the same version of a package is already registered, overwrite registration is not performed.

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 [5.5 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 note

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

Related Topics:

- [5.8 Procedure for registering components](#)

5.8 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.

5.9 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 group resource on the primary server](#). The IP address resource, network name resource, and shared disk (physical 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 group resource 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 group resource 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](#)

5.10 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.

Important note

If you have set a security policy that applies to prohibited operations, we recommend that you re-enter the security policy settings in the **Suppression of Device Usage** area of the **Prohibited operations** view after performing an overwrite installation from JP1/IT Desktop Management to JP1/IT Desktop Management 2. For details about how to set a policy for prohibited operations, see the description of suppressing device usage in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 Administration Guide*.

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						
		Manager	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

JP1/NETM		JP1/IT Desktop Management 2						
		Manager	Agent	Relay system	Controller	Remote control agent	Network monitor	Asset Console
JP1/NM	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 [5.5 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 note

- 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.

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

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 Installation 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 how to uninstall Asset Console, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management 2 - Asset Console Planning and Configuration Guide*.

Tip

The remote control agent is uninstalled automatically when the agent is uninstalled.

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 note

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 note

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 Installation Manager

If you want to reinstall Remote Installation Manager on the administrator's computer, or to change the computer on which Remote Installation Manager is installed, you first need to uninstall Remote Installation Manager.

Important note

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 note

Before uninstallation, make sure that all Windows applications have been closed.

To uninstall Remote Installation 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 Installation 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 note

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 note

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 note

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 note

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 note

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 note

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 Device module.
2. In **Device Inventory** in the menu area, select the desired network segment group from **Network List**.
3. In the information area, select a computer for which the network monitor is enabled.

The management type of the computer for which the network monitor is enabled is displayed as   or    .

4. In **Action**, select **Disable Network Access Control**.

The network monitor for the selected computer is disabled, and the network is no longer monitored.

Tip

Disabling the network monitor uninstalls the network monitor agent from the computer.

If the network monitor is disabled, the management type changes back to  or  .

The network monitor cannot be disabled if the operation status of the network monitor displayed in the menu area is **Stopped management**.

Important note

If the operation status of a computer on which the network monitor agent is installed is **Stopped management** or **Failed to stop management**, the computer cannot be excluded.

Important note

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

Tip

You can also disable the network monitor by selecting **Network Access Control** and then **Assign Network Access Control Settings** in the Settings module, and then using the **Assign Network Access Control Settings** view.

Tip

If a computer for which the network monitor is disabled belongs to multiple network segments, the network monitor is disabled on all of the network segments.

Tip

If a computer has the network monitor agent installed and cannot connect to the management server, you can disable the network monitor by selecting and deleting **JP1/IT Desktop Management 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:

- [2.7.2 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 group resource on the primary server](#). The IP address resource, the network name resource, and the shared disk (physical disk) resource remain online.
2. On the primary server, uninstall JP1/IT Desktop Management 2 - Manager.
3. Move the owner of the group resource 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](#)

7

Migrating environments

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

7.1 Procedure for 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.

Important note

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 note

You cannot upgrade JP1/IT Desktop Management 2 - Manager while replacing a management server. Accordingly, install the upgrade before or after replacement.

Important note

On a computer running 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

The procedure here describes how to replace a management server. You replace the server by installing JP1/IT Desktop Management 2 - Manager on the new computer and then migrating data from the old computer.

To replace a management server:

1. Stop the JP1/IT Desktop Management 2 services.

After backing up the database, stop the services so that new operation log data reported from the agent will not be saved.

From the Windows **Start** menu, select **Administrative Tools** and then **Services**. In the dialog box that opens, right-click a service name, and then select **Stop** to stop the service. Stop the following services:

- JP1_ITDM2_Agent Control
- JP1_ITDM2_Service
- JP1_ITDM2_Web Container

2. Back up the database.

On the old computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management 2 - Manager, Tools**, and then **Database Manager**. Start Database Manager for JP1/IT Desktop Management 2 - Manager, and back up the database. Leave at least 20 gigabytes of free space on the drive containing the backup folder.

3. Save the backup of the operation log data.

If you have configured the system to retain operation log data, back up the backup data stored in **Operation log backup folder** specified during setup.

To find out whether the system is configured to retain operation log data, from the **Start** menu, select **All Programs, JP1_IT Desktop Management 2 - Manager, Tools**, and then **Setup** to start JP1/IT Desktop

Management 2 - Manager setup. In the **Settings for Operation Logs** view, check whether **Store the operation logs** is selected. This function is enabled if the check box is selected.

4. Store the backup of the operation log data on the new computer.

If you saved a backup of the operation log data in step 3, before installation, save it in the folder you plan to specify as the operations log backup folder on the new computer. Do not store any data other than the operation log data you backed up in this folder.

5. Disconnect the old computer from the network.

6. On the new computer, install JP1/IT Desktop Management 2 - Manager.

7. Perform setup for JP1/IT Desktop Management 2 - Manager.

On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management 2 - Manager, Tools**, and then **Setup** to start setup for JP1/IT Desktop Management 2 - Manager, and then perform setup.

If you have enabled the storage of operation log data, in the **Automatic Backup Settings for Operation Logs** view, specify the folder in which you stored the backup data in step 4.

8. Restore the database you backed up in step 2.

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

9. Register the license.

In the Login window of JP1/IT Desktop Management 2 - Manager that you installed on the new computer, click the **License** button. In the dialog box that opens, click the **Register License** button to register the license.

10. Change the connection destination of the agent.

Log in to JP1/IT Desktop Management 2 - Manager that you installed on the new computer. In agent setup, select **Basic Settings** and then **Management Server** to set the IP address or the host name of the new computer.

Note that this procedure is required only when the IP address or host name of the management server is not the same before and after replacement.

11. Make sure that the system operates correctly.

In the JP1/IT Desktop Management 2 - Manager that you installed on the new computer, confirm that the agent is connected to the management server. To do so, in the **Device List** of the Device module, make sure that the value in the **Last Alive Confirmation Date/Time** column has been updated.

The **Last Alive Confirmation Date/Time** column is hidden by default. To show it, right-click any of the columns displayed in the **Device List** view, select **Select Columns**, and then select **Last Alive Confirmation Date/Time** in the dialog box that appears. If **Last Alive Confirmation Date/Time** has not been updated, from the Windows **Start** menu of the user's computer, select **All Programs, JP1_IT Desktop Management 2 - Agent, Administrator Tool**, and then **Setup**. Next, start setup for the agent, and make sure that the management server on the new computer is set as the connection destination.

12. On the old computer, uninstall JP1/IT Desktop Management 2 - Manager.

Replacement of the management server is complete.

Tip

If necessary, delete the backup data on the new computer after replacement.

Tip

You can check whether the agent is connected to the management server after replacement in the **Device List** view of the Device module. If **Last Alive Confirmation Date/Time** has been updated, the agent is connected. If the agent is not connected, make sure that the connection destination was set correctly during agent setup on the user's computer.

Cautions applying to the replacement procedure

Important note

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 note

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 note

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 note

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. In this case, 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 note

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.

Related Topics:

- [1.2.2 Procedure for installing JP1/IT Desktop Management 2 - Manager](#)
- [1.2.3 Procedure for setting up a management server](#)
- [2.10.1 Overview of building a cluster system](#)

7.2 Replacing a computer with only Remote Installation Manager installed

To replace a computer with Remote Installation Manager installed:

1. If needed, uninstall Remote Installation Manager from the computer being replaced.
2. Replace the computer.
3. On the new computer, install Remote Installation 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 Installation Manager installed.

Related Topics:

- [2.1.6 Procedure for installing Remote Installation Manager only](#)

7.3 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.

7.4 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.
2. Open the command prompt, and execute the following command:
`relay-system-installation-folder\bin\dmpstop.exe`
3. Using Task Manager or a similar tool, make sure that the processes below have stopped. If any of these processes are still running, wait for them to stop.
 - `jdngdmpsetup.exe`
 - `jdngwinst.exe`
 - `jdngsite.exe`
 - `jdngschserv.exe`
 - `jdngsrvmain.exe`
4. On the relay system being replaced, back up the following 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`
5. Back up the following files:
 - 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`
6. Start the relay system service on the relay system being replaced.
7. Log off from the relay system computer, and then log in again.

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.
4. Open the command prompt, and execute the following command:
`relay-system-installation-folder\bin\dmpstop.exe`
5. Using Task Manager or a similar tool, make sure that the processes below have stopped. If any of these processes are still running, wait for them to stop.
 - `jdngdmpsetup.exe`
 - `jdngwinst.exe`
 - `jdngsite.exe`
 - `jdngschserv.exe`
 - `jdngsrvmain.exe`
6. Restore the backup information to the new computer.
7. Using a text editor, create an inventory settings file (`jdng_inventory.conf`) with the following content, and place it in the `%ALLUSERSPROFILE%\HITACHI\jpltdma\conf` folder.
`[NodeID]`
`ReproductionLimit=0`
8. Set up the relay system on the new computer.
9. Start the relay system service on the new computer.
10. Log off from the relay system computer, and then log in again.

This completes the process of replacing the relay system.

Important note

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:

- [2.1.2 Installing a relay system](#)
- [2.1.3 Procedure for installing a relay system from supplied media](#)
- [2.1.4 Procedure for installing a relay system by deploying from the management server](#)
- [2.1.5 Procedure for setting up a relay system](#)
- [6.5 Procedure for uninstalling a relay system](#)

7.5 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 [2.7.2 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.

7.6 Changing host names and IP addresses in the system configuration

7.6.1 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:

- Agent connection destinations (when specified by host name)
- Connection destination in the login window of Remote Installation Manager (when specified by host name)
- The Asset Console data source

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 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.

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 Installation Manager (when specified by host name)

If a host name is specified in the **Management server** field of the login window of Remote Installation 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.

7.6.2 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:

- Agent connection destinations (when specified by IP address)
- Exception connection for devices denied network access
- Connection destination in the login window of Remote Installation Manager (when specified by IP address)
- The Asset Console data source

To change the IP address of the management server:

1. Stop any processing in progress in the Asset Console and Remote Installation Manager.
2. On the management server, execute the `stopservice` command to stop services.
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:

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 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.
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 Installation Manager (when specified by IP address)

If an IP address is specified in the **Management server** field of the login window of Remote Installation 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.

7.6.3 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 Installation 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 Installation 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 **Agent Configuration and Installation Set Creation**, 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 that uses Remote Installation Manager for distribution** 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.

7.6.4 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 Installation 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 Installation Manager.
2. Take the resources listed in [2.10.2 Procedure for creating a group resource 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:
JPI/IT-Desktop-Management-2-Manager-installation-folder\mgr\conf\jdn_manager_setup.conf
5. Transfer the ownership of the cluster 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 cluster group back to the primary server.
8. Place the resources listed in [2.10.2 Procedure for creating a group resource 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 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.
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 Installation Manager (when specified by host name)

If a host name is specified in the **Management server** field of the login window of Remote Installation 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.

7.6.5 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 Installation 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 Installation Manager.
2. Take the resources listed in [2.10.2 Procedure for creating a group resource 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:
JPI/IT-Desktop-Management-2-Manager-installation-folder\mgr\conf\jdn_manager_setup.conf
5. Transfer the ownership of the cluster 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 cluster group back to the primary server.
8. Place the resources listed in [2.10.2 Procedure for creating a group resource 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 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.
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 Installation Manager (when specified by IP address)

If an IP address is specified in the **Management server** field of the login window of Remote Installation 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.

7.7 Procedure for switching the management server to which an agent connects

To switch the management server to which an agent connects:

1. Display the Settings module.
2. In the menu area, select **Agent** and then **Agent Configuration and Installation Set Creation**.
3. In the information area, click the **Edit** button for the agent configuration whose management server 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.

Important note

Immediately after you switch the management server, the status of agent configuration assignment will be indeterminate. After registering the device information for agents whose management server was switched, you must assign the agent configurations again.

7.8 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 **Agent Configuration and Installation Set Creation**.
3. In the information area, click the **Edit** button for the agent configuration whose relay system you want to switch.
4. Under **Higher system that uses Remote Installation Manager for distribution** 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.

To change the connection destination relay system for a specific agent:

1. Display the Settings module.
2. In the menu area, select **Agent** and then **Assign Agent Configuration**.
3. Select a device, and then click the **Cancel** button.
The agent configuration is unassigned from the device, and the default agent configuration assigned in its place.
4. Click the **Assign** button, and in the **Assign Agent Configuration** window, assign the agent configuration that connects the agent to the new relay system.

The connection destination is changed for the specific agent that connects to the relay system.

Important note

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.

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 as a user who has administrator permissions. In Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, if User Account Control (UAC) is enabled, right click to open **JP1ITDM2 Utility Console** or the Windows command prompt. Then, select **Run as administrator**. Execute the `getinv.vbs` command as a user who has full control permissions over the folder in which the `getinv.vbs` command is stored.

To execute commands on 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

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, 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

```
updatesupportinfo -i support-information-file-name
```

Argument

`-i support-information-file-name`

Select the absolute path to the file to be registered to the management server (a support information file). To specify a path containing a space, enclose the strings with double quotation marks ("").

Storage location

`JP1/IT Desktop Management 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 exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils exporttoplog`
 - `ioutils exportpolicy`
 - `ioutils exporttemplate`
 - `ioutils exportupdategroup`

- `ioutils importasset`
 - `ioutils importfield`
 - `ioutils importfilter`
 - `ioutils importpolicy`
 - `ioutils importtemplate`
 - `ioutils importupdategroup`
 - `reorgdb`
 - `startservice`
 - `stopservice`
- This command cannot be executed 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 exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils exporttoplog`
 - `ioutils exportpolicy`
 - `ioutils exporttemplate`
 - `ioutils exportupdategroup`
 - `ioutils importasset`
 - `ioutils importfield`
 - `ioutils importfilter`
 - `ioutils importpolicy`
 - `ioutils importtemplate`
 - `ioutils importupdategroup`
 - `reorgdb`
 - `startservice`
 - `stopservice`
 - `updatesupportinfo`
- The argument `-s` cannot be specified in a cluster environment. 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.

Return value	Description
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 <code>-s</code> 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 exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils exporttoplog`
 - `ioutils exportpolicy`
 - `ioutils exporttemplate`
 - `ioutils exportupdategroup`
 - `ioutils importasset`
 - `ioutils importfield`
 - `ioutils importfilter`
 - `ioutils importpolicy`
 - `ioutils importtemplate`
 - `ioutils importupdategroup`
 - `reorgdb`
 - `startservice`
 - `stopservice`
 - `updatesupportinfo`
- The argument `-s` cannot be specified in a cluster environment. 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 <code>-s</code> 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 services associated with the management server 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 exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils exporttoplog`
 - `ioutils exportpolicy`
 - `ioutils exporttemplate`
 - `ioutils exportupdategroup`
 - `ioutils importasset`
 - `ioutils importfield`
 - `ioutils importfilter`
 - `ioutils importpolicy`
 - `ioutils importtemplate`

- `ioutils importupdategroup`
- `reorgdb`
- `startservice`
- `updatesupportinfo`

Return values

The following table shows the return values of the `stopservice` command.

Return value	Description
0	The command finished normally.
1	The management server 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 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.

Execute this command on the management server or a computer on which Remote Installation Manager is installed.

Format

```
getlogs[ -f troubleshooting-information-storage-folder]
```

Argument

-f troubleshooting-information-storage-folder

Specify the absolute path to the storage folder for troubleshooting information. Only a folder in a local drive can be specified.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. All characters that Windows systems allow for folder names are acceptable.

If this argument is not specified, the troubleshooting information is stored into the following folder:

JP1/IT Desktop Management 2-installation-folder\mgr\troubleshoot

A temporary folder `tsinf` is created under the troubleshooting information folder when collecting information. It is deleted when the command is completed.

Storage location

JP1/IT Desktop Management 2-installation-folder\mgr\bin

You can execute this command without specifying a storage location for the executable file, by using the command prompt provided by JP1/IT Desktop Management 2.

Notes

- If the storage folder for the troubleshooting information already contains one or more of the following folders or files, the command cannot be not executed until the folder or the file is deleted:
 - `tsinf` folder
 - `tsinf_1st.dat`
 - `tsinf_2nd.dat`
- The `getlogs` command uses a temporary folder which is set in the user environment variables `TEMP`. If a message (KDEX4041-E) is returned on `getlogs` command execution, check if there is enough space in this folder.

Return value

The following table shows the return values of the `getlogs` command.

Return value	Description
0	The command finished normally.

Return value	Description
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](#)

8.8 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 Installation 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\PCC26427AAL\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.
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](#)

8.9 resetnid.vbs (resetting the host ID)

This section describes the `resetnid.vbs` command, which resets the unique ID (host ID) which is generated by the agent in order to distinguish devices from each other.

Functionality

A host ID is automatically created when an agent is installed.

If you install an agent by using the disk copy functionality, the host ID must be reset on the copy-source computer prior to the copy so that a new host ID will be created on the copy-destination computer. The host ID for the agent can be reset by executing the `resetnid.vbs` command on the copy-source computer. As the old ID is reset, a new host ID is created when the agent is installed, and the computer will be able to be identified with a unique ID.

Tip

If you install an agent via a disk copy without executing the `resetnid.vbs` command, the copy-destination computer is defined as an identical device to the copy-source computer. In such cases, because two or more computers are identical, execute the `resetnid.vbs` command on those computers and go to the Settings module, **Discovery**, and then **Managed Nodes** to delete the device information for the computers.

When the `resetnid.vbs` command is executed on a computer that was once identified by JP1/IT Desktop Management 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 note

Do not execute the `resetnid.vbs` command on a device on which the network monitor is installed.

If you execute the `resetnid.vbs` on the device on which the network monitor is installed, 2 instances of the device information appear per computer. To resolve this problem, you need to perform the following: Temporarily disable the network monitor. After that, in the Settings module, select **Discovery** and then **Managed Nodes**, and then temporarily delete both device information stances.

Execute this command on a computer on which the agent is already installed.

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]
```

Argument

`/nodeid`

Always specify this argument. If this argument is omitted, the command cannot be executed.

/i

Displays, on the user's computer, the dialog box for selecting whether to execute the command and the dialog box for displaying execution results.

Storage location

agent-installation-folder\bin\

Notes

When the `resetnid.vbs` command is executed, the time required 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\jplitdma`:

```
cd "C:\Program Files\Hitachi\jplitdma\bin"
```

```
start /wait Cscript.exe resetnid.vbs /nodeid
```

```
echo %errorlevel%
```

Related Topics:

- [8.1 Executing commands](#)

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:

- *KDEXnnnn-Zmessage-text*
- *KFPHnnnnn-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](#)

- 9.5 Troubleshooting during building of a support service linkage configuration system
- 9.6 Troubleshooting during building of an Active Directory linkage configuration system
- 9.7 Troubleshooting during building of an MDM linkage configuration system
- 9.8 Troubleshooting during building of a network monitoring configuration system
- 9.9 Troubleshooting during building of a cluster 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 [8.8 getinstlogs \(collecting troubleshooting information about installation\)](#).

Log type you can obtain

Log type	Output destination	File name	Description
Installer trace log file	<ul style="list-style-type: none">• When JP1/IT Desktop Management 2 - Manager is installed correctly: <i>JP1/IT Desktop Management 2 - Manager\installation-folder\log</i>• When JP1/IT Desktop Management 2 - Manager is not installed correctly: <i>%WINDIR%\Temp\JDNINST</i>	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:

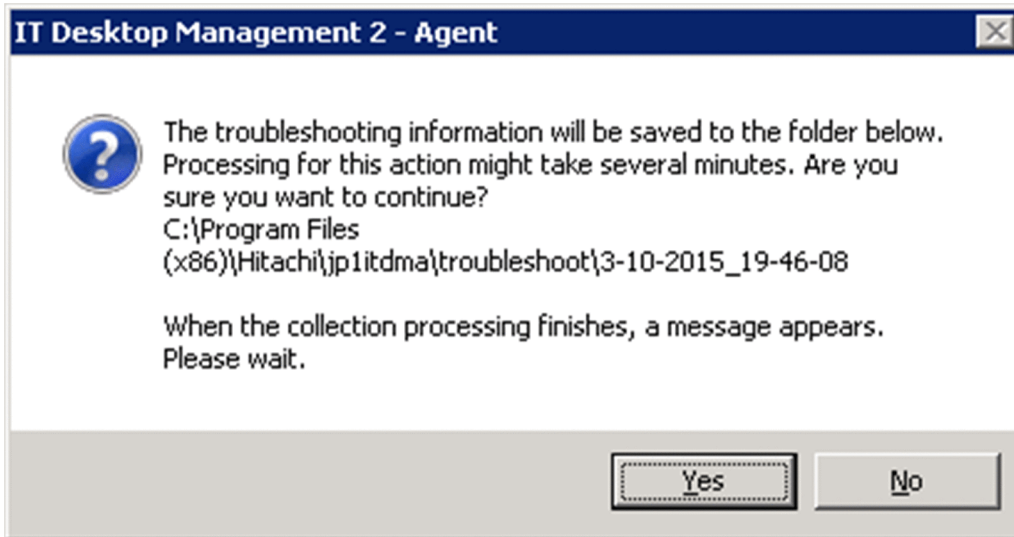
Collect troubleshooting information on the computer on which the problem occurred. Perform this operation as a user with administrator permissions.

1. Double-click `getlogs.vbs`.

The location of `getlogs.vbs` is as follows:

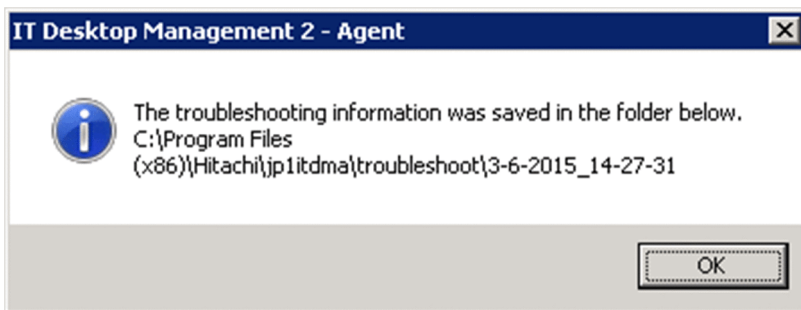
JPI/IT-Desktop-Management-2-Agent-installation-folder\bin

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:

JPI/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	<i>JPI/IT Desktop Management 2 - Agent-installation-folder\log</i>
System information	<ul style="list-style-type: none">• System informationResult of <code>msinfo32/nfo</code> execution

Troubleshooting information	Information collected
System information	<ul style="list-style-type: none"> • Environment variable Result of SET command execution • Registry information <ul style="list-style-type: none"> • 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 <i>JP1/IT Desktop Management 2 - Agent-installation-folder</i> • Event log Application, system, and security information

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):

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

The configuration is complete, and the user computer is now switched to online management.

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 note

When switching to offline management, you need to consider the operations for switching back to online management again. When switching a computer that is disconnected from the network from offline management to online management, you also need to change the agent configuration in the **Setup** dialog box on all computers that are switched.

To switch to offline management (changing the agent configuration):

Important note

If the security policy assigned to the target computer has operation log acquisition enabled, change the security policy to disable the operation log acquisition first, and then switch to online management. If you leave the security policy with operation log acquisition enabled, the user computer will keep acquiring operation log files.

1. In the **Basic settings** view for the agent configuration, clear the **Communicate with the higher system** check box, and then click **OK**.
2. In the displayed dialog box, click **OK**.

The configuration is complete, and the user computer is now switched to offline management.

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, make sure that the URL, ID, and password used for download that are set in the **Product Update** view are correct. You can open this view by selecting **General** in the Settings module. 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.

JP1/IT Desktop Management 2 - Manager port number list

Management server

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
31080	←	Administrator's computer [ephemeral]	TCP	Used for communication from an administrator's computer to a management server when the operation window is referenced or used. This port number is also used for communication from Remote Installation Manager or Packager installed on the administrator's computer to a management server.
31000	←	Agent or relay system [ephemeral]	TCP	Used for communication from an agent or relay system to a management server
Ephemeral	→	agent or relay system [31001]	TCP	Used for communication from a management server to an agent or relay system during distribution using Remote Installation Manager
31006 to 31009, 31011, 31012	None	None	TCP	Used for JP1/IT Desktop Management 2 internal processing
31010	←	<ul style="list-style-type: none"> Remote Installation Manager [ephemeral] Asset Console (jamTakeITDM2 Info.exe) [ephemeral] 	TCP	Used for communication from Remote Installation Manager or Asset Console to a management server, or internal processing
Ephemeral	→	Agent or relay system [31014]	TCP	Used for communication from a management server to an agent or relay system to distribute jobs by multicasting
31015	←	Agent or relay system [ephemeral]	TCP	Used for communication from an agent or relay system to a management server for requesting retransmission during multicast distribution
31021	←	<ul style="list-style-type: none"> Remote Installation Manager [ephemeral] Agent [ephemeral] Relay system [ephemeral] Packager [ephemeral] 	TCP	Used for communication from Remote Installation Manager, agent, relay system, and Packager to a management server during distribution using Remote Installation Manager

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
Ephemeral	➔	Agent [16992]	TCP	Used for controlling the power source of a computer that uses AMT

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, in the setup, change them to port numbers that are not used.

If a management server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if you install JP1/IT Desktop Management 2 - Manager in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Administrator's computer (Remote Installation Manager)

Port number for administrator's computer	Connection direction	Connected to [port number]	Protocol	Use
Ephemeral	➔	Management server [31010 and 31021]	TCP	Used for communication from Remote Installation Manager to a management server during distribution using Remote Installation Manager
Ephemeral#	↔	Management server [ephemeral#]	TCP	Used for Remote Installation Manager internal processing

#: The following describes how to fix the port numbers used for connecting the database to the agent.

To fix the port number of the management server (connection destination):

1. Execute the `stop-service` 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 `start-service` command to restart the services on the management server.

To fix the port numbers of Remote Installation Manager (connection destination):

For receiving ports, the OS automatically assigns port numbers by default. Ten or more receiving ports are used.

1. Stop Remote Installation Manager and other applications for JP1/IT Desktop Management 2.
2. Use a text editor to open the `HirDB.ini` file stored in `Remote-Install-Manager-installation-folder\mgr\db\emb`.
If Remote Install Manager and the management server are installed in the same computer, `HirDB.ini` is stored in `JP1/IT Desktop Management 2-Manager-installation-folder\mgr\db\CONF\emb`.
3. For `PDCLTRCVPORT=`, specify the range of port numbers you want to use in the `port-number-port-number` format. Note that the range of port numbers is not set if you do not specify anything or specify 0 after `PDCLTRCVPORT=`. By default, the range of port numbers is not set.

Example: To specify 10000-10500 as the range of port numbers, enter as follows:

```
PDCLTRCVPORT=10000-10500
```

4. Start Remote Installation Manager and other applications for JP1/IT Desktop Management 2.

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, in the setup, change them to unused port numbers.

If the administrator's server controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if you install Remote Install Manager in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Port number list for a relay system

Port number for relay system	Connection direction	Connected to [port number]	Protocol	Use
31001	←	Management server [ephemeral]	TCP	Used for communication from a management server to a relay system during distribution using Remote Installation Manager
31002	←	Agent [ephemeral]	TCP	Used for communication from an agent to a relay system during distribution using Remote Installation Manager
31014	←	Management server [ephemeral]	TCP	Used for communication from a management server to a relay system to distribute jobs by multicasting
31015	←	Agent [ephemeral]	TCP	Used for communication from an agent to a relay system for requesting retransmission during multicast distribution
Ephemeral	→	Management server [31021]	TCP	Used for communication from a relay system to a management server during distribution using Remote Installation Manager
Ephemeral	→	Agent [16992]	TCP	Used for controlling the power source of a computer that uses AMT

Port number list for a controller and remote control agent

Controller or remote control agent [port number]	Connection direction	Connected server [port number]	Protocol	Use
Remote control agent [31016]	←	Controller [ephemeral]	TCP	Used for window operation from a controller to a remote control agent
Remote control agent [31017]	←	Controller [ephemeral]	TCP	Used for transferring files from a controller to a remote control agent
Remote control agent or controller [31018] (when used as a chat server)	← →	Remote control agent or controller [ephemeral]	TCP	Used for chat
Remote control agent [ephemeral]	→	Controller [31019]	TCP	Used for requesting a remote connection from a remote control agent to a controller
Remote control agent [ephemeral]	→	Controller [31020]	TCP	Used for callback file transfer from a remote control agent to a controller

If a computer with a controller installed or a computer that is remotely controlled controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if a controller and remote control agent are installed in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, follow the steps below to change them to port numbers that are not used.

- Port number for a controller
Specify port numbers in the **Options** dialog box of the controller.
- Port number for a remote controller agent
Specify port numbers in the **Remote control settings** view used for agent configuration.
- Port number for the chat functionality
In the **Chat** window, select **Options**, and in the displayed dialog box, in the **Connect** tab, specify the port numbers.

JP1/IT Desktop Management 2 - Agent port number list

Agent port number	Connection direction	Connected server [port number]	Protocol	Use
31001	←	Management server [ephemeral]	TCP	Used for communication from a management server to the agent
16992	←	Management server [ephemeral]	TCP	Used for controlling the power source of a computer that uses AMT
Ephemeral	→	Relay system [31002]	TCP	Used for communication from an agent to a relay system during distribution using Remote Installation Manager
31014	←	Management server or relay system [ephemeral]	TCP	Used for communication from a management server or relay system to an agent to distribute jobs by multicasting
Ephemeral	→	Management server or relay system [31015]	TCP	Used for communication from an agent to a management server or relay system for requesting retransmission during multicast distribution
Ephemeral	→	Management server [31021]	TCP	Used for communication from an agent to a management server system during distribution using Remote Installation Manager

Each port number is set as a default when the product is provided. If the port numbers shown in the table are already used in the system environment you are using, when setting up a management server, change them to port numbers that are not used.

If a computer with an agent installed controls port numbers by using Windows Firewall, specify firewall settings to enable the above ports. Note that if an agent is installed in an environment in which Windows Firewall is enabled, the ports are automatically set to pass through Windows Firewall (they are registered in the exception settings).

If networks between JP1/IT Desktop Management 2 - Manager and JP1/IT Desktop Management 2 - Agent control ports by using Windows Firewall, specify firewall settings to enable the ports in the above table.

Port numbers for agentless devices

For agentless devices, the port numbers for Windows administrative shares or SNMP are used depending on the authentication status of the devices.

A.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.[#]

[#]: 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 Summary of amendments

Changes in 10-50

- 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.

Changes in 10-10

- 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.

Changes in 10-01

- The following information items are now collectively described in the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management Overview and System Design Guide*:
 - Abbreviated Microsoft product names
 - Conventions: Fonts and symbols
 - About help
 - Related manuals
 - Related documentation
 - Abbreviated product names (other than Microsoft product names)
 - Acronyms
 - Conversions: KB, MB, GB, and TB
 - Glossary
- A default file name (`ITDMAgt.exe`) for the installation set has been added.
- Information about automatic startup of agent installation has been added. When a CD-R is used as the agent installation media, agent installation can be started automatically by using `Autorun.inf`.
- The offline management functionality can now be used to manage computers that are not connected to the management server via a network.
- Information about JP1/IT Desktop Management can now be updated by acquiring support service information, including anti-virus product information.
- Notes on JP1/IM linkage systems when JP1/IM and JP1/Base are not connected have been improved.
- The procedure for setting information used to link with an MDM system has been corrected.
- An overview of upgrading the entire JP1/IT Desktop Management system has been added.
- The procedure for upgrading JP1/IT Desktop Management - Manager has been corrected.
- The explanation about how to update components has been corrected.
- An overview of the overwrite installation of JP1/IT Desktop Management - Manager in a multi-server configuration system has been added.
- An overview of upgrading JP1/IT Desktop Management - Manager in a multi-server configuration system has been added.
- A procedure for replacing site servers and notes on the `recreatelogdb` command used to replace site servers have been corrected.
- The procedure for replacing computers with network access control enabled has been added.
- Notes on executing the `recreatelogdb` command with an argument other than `-node` specified have been corrected.
- A description of the `stopservice` command that stops services has been added. This command can be used for building-related operations.
- For the `getlogs` command, information about using the folder set for the TEMP user environment variable as a general folder has been added.

- The description related to reference information when an agent is installed from a disk copy without executing the `resethid.vbs` command has been improved.
- The port numbers used by JP1/IT Desktop Management - Manager have been described separately for a single-server configuration and for a multi-server configuration.
- A maximum of 50,000 devices can now be managed by using a multi-server configuration system.
- JP1 events can now be reported by linkage with JP1/IM.
- The URL of the Login window for JP1/IT Desktop Management was included.
- Information about settings for **Set the account to install Agent** in the **Create Agent Installer** dialog box that apply only when an agent is installed on a computer whose OS is Windows 2000, Windows XP, or Windows Server 2003, was added.
- Information about setting a schedule for obtaining the latest update program information from the support service site by selecting **General**, **Customer Support configuration**, and **Edit Import Schedule** of the Settings module was added.
- Corrective action for multiple devices treated as a single device when the agent is installed from a disk copy were added.
- The time it takes after execution of the `resethid.vbs` command for a new host name to be generated was added.
- The Controller and Remote Control Agent port numbers were been corrected.
- The timing for regeneration of a host identifier was added.
- A description of when users are prompted to change their passwords at login was added. Also, a description stating that any login password must be changed every 180 or fewer days was added.
- The procedure for unlocking a user account was added.
- Smart devices can now be managed by linkage with the MDM products.
- A description stating the following was added: If a domain user is authenticated by a Windows administrative share, the user ID must be in *user-ID@FQDN* (FQDN: fully qualified domain name) or in *domain-name\user-ID* format.
- Detailed procedures for replacing management servers were added.
- Corrective action for executing the `deletelog` command that deletes site server operation log data, when the file for recording the execution status (`deletelog_lasttime.txt`) is in the work folder was added.
- Port number 31000 was added to the list of port numbers for site servers.

Index

A

- acquiring backup, exportdb command 166
- Active Directory
 - searching for devices registered in 106
- Active Directory linkage configuration system
 - building 56
 - overview of building 56
- adding
 - relay system configuration 99
- adding, agent configurations 99
- adding agent configurations 99
- adding network monitor settings 111
- adding product license 20
- agent
 - automatically installing 39
 - changing monitored items 100
 - checking installation status 39
 - deploying during search (network search) 40
 - deploying to computer on which agent has not yet been installed 43
 - deploying to selected group of computers 43
 - installing on computer 29
 - manually installing 27
 - planning installation 25
 - procedure for setting up 37
- agent installation
 - disk copy 35
 - distributing agent by email 33
 - distributing media 32
 - logon script 33
 - uploading to file server 31
 - uploading to Web server 30
- agentless configuration system
 - building 54
 - overview of building 54
- asset information
 - suppressing registration and modification 92
- automatically deploying agent (network search) 40

B

- basic configuration system
 - overview of building 46
- basic configuration system (relay system)
 - building 46

- building
 - basic configuration system 46
 - basic configuration system (relay system) 46
 - cluster system 64
 - minimal configuration system 13
 - minimal configuration system (management servers and agents) 12
- building JP1/Network Monitor - Manager linkage configuration systems 61

C

- changing
 - logical host name in cluster system 154
 - logical IP address in cluster system 155
 - setting 72
- changing assignment of network monitor settings 112
- changing default password 22
- checking
 - agent installation status 39
 - discovered device 41
 - excluded device 43
 - latest discovery status 41
 - managed device 42
- cluster system
 - building 64
 - changing logical host names 154
 - changing logical IP addresses 155
 - overview of building 64
 - overwrite installation 129
- collecting troubleshooting information, getlogs command 175
- collecting troubleshooting information about installation, getinstlogs command 177
- command
 - used for building-related operation 160
- command description format 163
- components
 - updating 116
- configuration files
 - using to configure processing 99
- controller, uninstalling 140
- creating
 - installation set 27
- credentials, discovery from IP address 97
- credentials, SNMP 98

- credentials, Windows administrative share [98](#)
- credentials for Windows administrative share [98](#)
- credentials used in discovery from IP address [97](#)
- customizing setting
 - specified when building system [96](#)

D

- deploying agent
 - computer on which agent has not yet been installed [43](#)
- deploying agent during search (network search) [40](#)
- device
 - checking discovery status [40](#)
 - identifying in organization [24](#)
- device information
 - troubleshooting when computer has two sets [186](#)
- disabling the network monitor [138](#)
- discovered device
 - checking [41](#)
- discovery status
 - checking latest status [41](#)

E

- editing
 - network control settings file [113](#)
- editing, automatic update settings for network control list [111](#)
- editing devices in the network control list [111](#)
- enabling
 - JP1/NETM/NM - Manager linkage settings [112](#)
- enabling the network monitor [58](#)
- excluded device
 - checking [43](#)
- executing commands [161](#)
- exportdb command [166](#)

G

- getinstlogs command [177](#)
- getlogs command [175](#)
- group resource
 - procedure for creating on primary server [64](#)

H

- host name
 - changing for management server [152](#)
 - changing in system configuration [152](#)

- host name or IP address
 - changing for relay system [154](#)

I

- identifying
 - all devices used in organization [24](#)
- importdb command [169](#)
- installation set
 - creating [27](#)
- installation types
 - JP1/IT Desktop Management 2 - Manager [14](#)
- installing
 - agent automatically [39](#)
 - agent manually [27](#)
 - agent on computer [29](#)
 - JP1/IT Desktop Management 2 - Manager [14](#)
 - relay system [46](#)
 - relay system (deploying from management server) [49](#)
 - relay system (from supplied media) [47](#)
 - Remote Installation Manager [50](#)
- installing agent
 - disk copy [35](#)
 - distributing agent by email [33](#)
 - distributing media [32](#)
 - from supplied media [36](#)
 - logon script [33](#)
 - uploading to file server [31](#)
 - uploading to Web server [30](#)
- installing product (overwrite installation) [116](#)
- IP address
 - changing for management server [152](#)
 - changing in system configuration [152](#)

J

- JP1/IM linkage configuration system
 - overview of building [62](#)
- JP1/IT Desktop Management
 - overwrite installation to JP1/IT Desktop Management 2 [130](#)
- JP1/IT Desktop Management 2
 - setting up on primary server [68](#)
 - setting up on standby server [71](#)
- JP1/IT Desktop Management 2 - Manager
 - installation types [14](#)
 - overwrite installation [117](#)
 - procedure for installing [14](#)

- uninstalling 134
- uninstalling in cluster system 141
- JP1/NETM/NM - Manager
 - troubleshooting during linkage with 195
- JP1/NETM/NM - Manager linkage configuration system
 - overview of building 61
- JP1/NETM/NM - Manager linkage settings
 - enabling 112
- JP1/Network Monitor - Manager linkage configuration systems, building 61

L

- license
 - registering 20
- logging in 21
- logging in to operation window 21

M

- mail notification, discovery from IP address 97
- mail notification, searching Active Directory 106
- managed device
 - checking 42
- management server
 - changing host name 152
 - changing IP address 152
 - replacing 143
 - setting up 16
 - switching connection-target for agents 158
- management server environment
 - creating 14
- MDM linkage configuration system
 - building 57
 - overview of building 57
- message
 - output format 182
- migrating
 - environment 142
- minimal configuration system
 - building 12
 - overview of building 13
 - setting for building 97
 - troubleshooting 184
- miscellaneous information 197
- monitoring
 - procedure for changing agent monitoring items 100

N

- network
 - searching for devices connected to 24
- network control appliance
 - replacing computer by network control appliance (when network monitor is enabled) 114
- network control list
 - editing automatic update settings 111
- network control list, editing devices in 111
- network control settings file
 - editing 113
- network monitoring configuration system
 - building 58
 - overview of building 58
- network monitor settings, adding 111

O

- offline management configuration system
 - building 53
 - overview of building 53
- operation log
 - procedure for acquiring 78
- operation window, logging in 21
- overview of building
 - JP1/NETM/NM - Manager linkage configuration system 61
- overview of troubleshooting
 - during building of environment 182
- overview of uninstalling
 - entire system 133
- overview of upgrading
 - entire JP1/IT Desktop Management 2 system 122
- overwrite installation
 - from JP1/IT Desktop Management 130
 - in cluster system 129
 - relay system from supplied media 120
- overwrite-installing product 116

P

- planning installation
 - agent 25
- port number list 197
- procedure for changing
 - currency unit 86
 - folders used 77
 - login restrictions 90

- port number 84
- setting for connection to database 73
- procedure for controlling
 - network bandwidth used for distribution 88
- procedure for initializing
 - database 95
- procedure for performing overwrite installation
 - agent from supplied media 119
 - JP1/IT Desktop Management 2 - Manager 117
 - network access control agent from supplied media 121
- procedure for registering
 - component 128
- procedure for replacing
 - computer for which network access control enabled 151
 - computer on which agent installed 148
- procedure for uninstalling
 - agent 136
 - JP1/IT Desktop Management 2 - Manager 134
 - relay system 137
 - Remote Installation Manager 135
- procedure for upgrading
 - database 94
 - JP1/IT Desktop Management 2 - Manager 124
- product license
 - adding 20
 - registering 20

R

- recognition procedure
 - when agent environment is changed 201
- registering
 - product license 20
- relay system
 - adding configurations 99
 - changing host name 154
 - changing IP address 154
 - installing 46
 - installing by deploying from management server 49
 - installing from supplied media 47, 120
 - replacing 149
 - setting up 49
 - switching connection-target for agents 159
 - uninstalling 137
- Remote Installation Manager
 - installing 50

- uninstalling 135
- replacing
 - management server 143
 - relay system 149
- resetnid.vbs command 179
- resetting host ID, resrtnid.vbs command 179
- restoring data using a backup, importdb command 169

S

- searching
 - devices connected to network 24
 - devices registered in Active Directory 106
- Setting additional management item, information acquired from Active Directory 105
- setting for building
 - Active Directory linkage configuration system 105
 - agentless configuration system 102
 - MDM linkage configuration system 109
 - minimal configuration system 97
 - network monitoring configuration system 111
 - support service linkage configuration system 103
- setting management target 107
- setting up
 - management server 16
 - relay system 49
- setting user account information 22
- SNMP credentials 98
- specifying an update interval, agentless 102
- specifying search conditions, discovery from IP address 97
- specifying search conditions, searching Active Directory 106
- specifying search conditions for Active Directory 106
- specifying search conditions for IP address range 97
- specifying settings for connecting to Active Directory 105
- specifying settings for connecting to the support service 103
- specifying settings to link with an MDM system 109
- stopping services, stopservice command 173
- stopservice command 173
- support service linkage configuration system
 - building 55
 - overview of building 55
- suppressing
 - asset information registration and modification 92
- switching from offline management to online management 187

switching from online management to offline management 188

system configuration

- building 45
- changing host names and IP addresses 152

T

troubleshooting 181

- during agent installation 184
- during building of Active Directory linkage configuration system 191
- during building of agentless configuration system 189
- during building of cluster system 194
- during building of management server 184
- during building of MDM linkage configuration system 192
- during building of minimal configuration system 184
- during building of network monitoring configuration system 193
- during building of offline management configuration system 187
- during building of support service linkage configuration system 190
- during linkage with JP1/NETM/NM - Manager 195
- when two sets of device information appear for one computer 186

troubleshooting information

- agent 185

U

uninstalling

- JP1/IT Desktop Management 2 - Manager in cluster system 141
- product 132

uninstalling controllers 140

unlocking user account 23

updatesupportinfo command 164

updating

- component 126
- components 116

uploading support service information 164

user account, unlocking 23