

Job Management Partner 1 Version 10

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

3021-3-338-10(E)

Notices

■ Relevant program products

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

The above product includes the following:

- P-2642-74AL Job Management Partner 1/IT Desktop Management - Manager (for Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003)
- P-2642-75AL Job Management Partner 1/IT Desktop Management - Remote Site Server (for Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003)
- P-2642-76AL Job Management Partner 1/IT Desktop Management - Network Monitor (for Windows 8 Enterprise, Windows 8 Pro, Windows Server 2012, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Ultimate, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003 (x86))
- P-2642-77AL Job Management Partner 1/IT Desktop Management - Agent (for Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 Datacenter, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Vista, Windows Server 2003, Windows XP, Windows 2000)

■ Trademarks

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

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

Firefox is a registered trademark of the Mozilla Foundation.

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

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

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

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

Microsoft and 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 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 is a registered trademark or a trademark 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 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

Feb. 2014: 3021-3-338-10(E)

■ Copyright

All Rights Reserved. Copyright (C) 2013, 2014, Hitachi, Ltd.

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

Summary of amendments

The following table lists changes in this manual (3021-3-338-10(E)) and product changes related to this manual.

Changes	Location
Windows 8 and Windows Server 2012 were added as applicable OSs for the following programs: <ul style="list-style-type: none"> • Job Management Partner 1/IT Desktop Management - Manager • Job Management Partner 1/IT Desktop Management - Remote Site Server • Job Management Partner 1/IT Desktop Management - Network Monitor 	1.2.2, 1.6.9, 2.3.3, 2.4.1, 2.4.3, 2.11.4, 3.2, 3.3, 3.4, 3.5, 7.1, 7.6, 8.1
Notes on installation, overwrite installation, and uninstallation were added.	1.2.2, 5.1, 6.2
It is now possible to acquire the revision history for device information.	1.2.3, 2.4.2, 2.11.4, 3.5
A description of the following restriction was added: To narrow the search range by specifying a period when searching for network devices, the number of IP addresses subject to search must not exceed 50,000.	1.5.1
By linking with Job Management Partner 1/NETM/Network Monitor - Manager, you can now, from Job Management Partner 1/IT Desktop Management, control network connections that are monitored by the appliance products on which Job Management Partner 1/NETM/Network Monitor is installed.	2.9, 4.7.5, 4.7.6, 4.7.7, 9.12
A description was added about how to change 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.	4.6.1
For the Network Filter List, you can now specify whether to enable automatic updates for all items or only for additional items.	4.7.2
The description of overwrite-installing the product and updating the components was corrected.	5.
A description was added to the procedure for upgrading the entire Job Management Partner 1/IT Desktop Management system and to the procedure for updating Job Management Partner 1/IT Desktop Management - Manager.	5.5, 5.6, 5.10
A 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.	7.1
All descriptions related to command execution permissions were gathered in 8.1. A description of executing commands (other than <code>getinv.vbs</code>) when User Account Control (UAC) of the OS is enabled was added.	8.
A procedure for executing commands on a computer on which an agent program is installed was added. Notes that apply when commands are being executed were added.	8.1
Definitions of shared management items and added management items can now be exported and imported in CSV format.	8.3, 8.4, 8.5, 8.7
A description of the characters that can be used in the names of folders used by the following commands was added: <ul style="list-style-type: none"> • <code>exportdb</code> command • <code>getlogs</code> command • <code>getinstlogs</code> command • <code>importdb</code> command 	8.4, 8.5, 8.8, 8.9

Changes	Location
<p>The <code>/i</code> option was added to the <code>resetnid.vbs</code> command, and dialog boxes allowing the user to select whether to execute the command and displaying the execution result are now set to appear on the user's computer.</p> <p>In addition, the following items were added:</p> <ul style="list-style-type: none"> • A procedure for resetting the host ID on a computer on which the site server program is installed • A note on executing the <code>resetnid.vbs</code> command on devices on which a network monitor is installed 	<p>8.10</p>
<p>The description about port settings was modified. In addition, a description about the network between Job Management Partner 1/IT Desktop Management - Remote Site Server and agentless computers was added.</p>	<p>A.1</p>

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

Preface

This manual describes how to build Job Management Partner 1/IT Desktop Management - Manager (hereafter, called JP1/IT Desktop Management).

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

■ Organization of this manual

This manual is organized as follows:

1. Building a basic configuration system (management servers and agents)
This chapter describes how to build a basic configuration system (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 during management server, database server, or site server setup.
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 - Manager and updating of the components (agent, site server program, and network monitor agent).
6. Uninstalling products
This chapter describes how to uninstall JP1/IT Desktop Management programs.
7. Migrating environments
This chapter describes how to migrate an environment in JP1/IT Desktop Management.
8. Commands used for building-related operations
This chapter describes the JP1/IT Desktop Management 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.

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

Contents

Notices 2

Summary of amendments 5

Preface 7

1 Building a basic configuration system (management servers and agents) 15

- 1.1 Overview of building a basic configuration system 16
- 1.2 Creating a management server environment 17
 - 1.2.1 Types of JP1/IT Desktop Management - Manager installation 17
 - 1.2.2 Procedure for installing JP1/IT Desktop Management - Manager 17
 - 1.2.3 Procedure for setting up a management server in a single-server configuration 19
- 1.3 Registering a Product License 21
 - 1.3.1 Registering a product license 21
 - 1.3.2 Adding a product license 21
- 1.4 Logging in to the Operation Window 22
 - 1.4.1 Logging in 22
 - 1.4.2 Changing the default password 23
 - 1.4.3 Setting user account information 23
 - 1.4.4 Unlocking a user account 24
- 1.5 Identifying all devices used in your organization 25
 - 1.5.1 Searching for devices connected to the network 25
 - 1.5.2 Planning the installation of agents 27
- 1.6 Manually installing agents on computers 28
 - 1.6.1 Creating an installation set 28
 - 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 34
 - 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 42
- 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 offline management configuration systems 46
 - 2.1.1 Overview of building an offline management configuration system 46
- 2.2 Building agentless configuration systems 47
 - 2.2.1 Overview of building an agentless configuration system 47
- 2.3 Building site server configuration systems 48
 - 2.3.1 Overview of building a site server configuration system 48
 - 2.3.2 Procedure for installing the site server program 48
 - 2.3.3 Procedure for installing the site server program from the supplied media 49
 - 2.3.4 Procedure for installing the site server program in the operation window 50
 - 2.3.5 Procedure for setting up a site server 51
- 2.4 Building multi-server configuration systems 52
 - 2.4.1 Overview of building a multi-server configuration system 52
 - 2.4.2 Procedure for setting up a database server 53
 - 2.4.3 Procedure for setting up a management server for a multi-server configuration system 54
- 2.5 Building support service linkage configuration systems 56
 - 2.5.1 Overview of building a support service linkage configuration system 56
- 2.6 Building Active Directory linkage configuration systems 57
 - 2.6.1 Overview of building an Active Directory linkage configuration system 57
- 2.7 Building MDM linkage configuration systems 58
 - 2.7.1 Overview of building a MDM linkage configuration system 58
- 2.8 Building network monitoring configuration systems 59
 - 2.8.1 Overview of building a network monitoring configuration system 59
 - 2.8.2 Enabling the network monitor 59
- 2.9 Building JP1/NETM/NM - Manager linkage configuration systems 62
 - 2.9.1 Overview of building a JP1/NETM/NM - Manager linkage configuration system 62
- 2.10 Building JP1/IM linkage configuration systems 63
 - 2.10.1 Overview of building a JP1/IM linkage configuration system 63
- 2.11 Building a cluster system 65
 - 2.11.1 Overview of building a cluster system in a single-server configuration system 65
 - 2.11.2 Overview of building a cluster system in a multi-server configuration system 66
 - 2.11.3 Procedure for creating a group resource on the primary server 67
 - 2.11.4 Setting up JP1/IT Desktop Management on the primary server 71
 - 2.11.5 Setting up JP1/IT Desktop Management on the standby server 74

- 3 Changing settings 75**
 - 3.1 Procedure for changing the setting for connection to the database 76
 - 3.2 Procedure for changing the folders that are used 78
 - 3.3 Procedure for changing a data folder shared by servers 79
 - 3.4 Procedure for specifying the settings used for recording an operation log on a management server in a single-server configuration system 81
 - 3.5 Procedure for setting up the output folder for the revision history 85
 - 3.6 Procedure for changing a port number 87
 - 3.7 Procedure for controlling the network bandwidth used for distribution 90
 - 3.8 Procedure for changing the currency unit 92
 - 3.9 Procedure for upgrading a database 94
 - 3.10 Procedure for initializing a database 95

- 4 Customizing the settings specified when building a system 96**
 - 4.1 Settings for building a basic 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
 - 4.2 Settings for building agentless configuration systems 100
 - 4.2.1 Regularly updating agentless device information 100
 - 4.3 Settings for building site server configuration systems 101
 - 4.3.1 Managing server configurations 101
 - 4.3.2 Specifying server configurations 101
 - 4.3.3 Adding site server groups 101
 - 4.3.4 Editing site server group information 102
 - 4.3.5 Removing site server groups 102
 - 4.4 Settings for building a support service linkage configuration system 104
 - 4.4.1 Setting information for connecting to the support service 104
 - 4.5 Settings for building Active Directory linkage configuration systems 106
 - 4.5.1 Setting information for connecting to Active Directory 106
 - 4.5.2 Setting the information acquired from Active Directory as an additional management item 106
 - 4.5.3 Searching for devices registered in Active Directory 107
 - 4.5.4 Specifying search conditions (searching Active Directory) 108
 - 4.5.5 Setting a device as a management target 108
 - 4.6 Settings for building MDM linkage configuration systems 110
 - 4.6.1 Specifying settings to link with an MDM system 110
 - 4.7 Settings for building network monitoring configuration systems 112
 - 4.7.1 Editing devices in the network control list 112
 - 4.7.2 Editing the automatic update of the network filter list 112
 - 4.7.3 Adding network monitor settings 112
 - 4.7.4 Changing assignment of network monitor settings 113
 - 4.7.5 Enabling the JP1/NETM/NM - Manager linkage settings 113

4.7.6	Procedure for editing the network control settings file	114
4.7.7	Procedure for replacing a computer by a network control appliance when the network monitor on the computer is enabled	115
4.8	Settings for building JP1/IM linkage configuration systems	116
4.8.1	Procedure for setting the configuration file used for linkage with JP1/IM	116
5	Overwrite-installing the product and updating the components	117
5.1	Procedure for performing an overwrite installation of JP1/IT Desktop Management - Manager	118
5.2	Procedure for performing an overwrite installation of an agent from the supplied media	120
5.3	Procedure for performing an overwrite installation of a site server program from the supplied media	121
5.4	Procedure for performing an overwrite installation of a network access control agent from the supplied media	122
5.5	Overview of upgrading the entire JP1/IT Desktop Management system	123
5.6	Procedure for upgrading JP1/IT Desktop Management - Manager	125
5.7	Updating components	127
5.8	Procedure for registering components	129
5.9	Overview of performing an overwrite installation of JP1/IT Desktop Management - Manager in a multi-server configuration system	130
5.10	Overview of upgrading JP1/IT Desktop Management - Manager in a multi-server configuration system	131
5.11	Overview of performing an overwrite installation in a cluster system in a single-server configuration system	133
5.12	Overview of performing an overwrite installation in a cluster system in a multi-server configuration system	134
6	Uninstalling products	135
6.1	Overview of uninstalling the entire system	136
6.2	Procedure for uninstalling JP1/IT Desktop Management - Manager	137
6.3	Procedure for uninstalling the agent	138
6.4	Procedure for uninstalling the site server program	139
6.5	Disabling the network monitor	140
6.6	Uninstalling a controller	142
6.7	Procedure for uninstalling JP1/IT Desktop Management - Manager in a cluster system in a single-server configuration system	143
6.8	Procedure for uninstalling JP1/IT Desktop Management - Manager in a cluster system in a multi-server configuration system	144
7	Migrating environments	145
7.1	Procedure for replacing a management server in a single-server configuration system	146
7.2	Procedure for replacing a management server in a multi-server configuration system	150
7.3	Procedure for replacing computers on which an agent is installed	153
7.4	Procedure for replacing site servers	154
7.5	Procedure for connecting a site server to another management server	156
7.6	Procedure for migrating from a single-server configuration system to a multi-server configuration system	158

- 7.7 Procedure for migrating JP1/IT Desktop Management 09-51 or earlier in a single-server configuration system to a multi-server configuration system 162
- 7.8 Procedure for replacing database servers 163
- 7.9 Procedure for replacing a management server and a database server in a multi-server configuration system at one time 166
- 7.10 Procedure for replacing computers for which network access control is enabled 170

8 Commands used for building-related operations 171

- 8.1 Executing commands 172
- 8.2 Command description format 174
- 8.3 updatesupportinfo (uploading support service information) 175
- 8.4 exportdb (acquiring backup data) 177
- 8.5 importdb (restoring backup data) 181
- 8.6 recreatelogdb (recreating an operation log index on the site server) 185
- 8.7 stopservice (stopping services) 188
- 8.8 getlogs (collecting troubleshooting information) 190
- 8.9 getinstlogs (collecting troubleshooting information about installation) 192
- 8.10 resetnid.vbs (resetting the host ID) 194

9 Troubleshooting 196

- 9.1 Overview of troubleshooting during building of an environment 197
- 9.2 Troubleshooting during building of a basic configuration system 199
 - 9.2.1 Troubleshooting during building of a management server 199
 - 9.2.2 Troubleshooting during agent installation 199
- 9.3 Troubleshooting during building of an offline management configuration system 202
 - 9.3.1 Switching from offline management to online management 202
 - 9.3.2 Switching from online management to offline management 203
- 9.4 Troubleshooting during building of an agentless configuration system 204
- 9.5 Troubleshooting during building of a site server 205
- 9.6 Troubleshooting during building of a multi-server configuration system 206
- 9.7 Troubleshooting during building of a support service linkage configuration system 207
- 9.8 Troubleshooting during building of an Active Directory linkage configuration system 208
- 9.9 Troubleshooting during building of an MDM linkage configuration system 209
- 9.10 Troubleshooting during building of a network monitoring configuration system 210
- 9.11 Troubleshooting during building of a cluster system 211
- 9.12 Troubleshooting during linkage with JP1/NETM/NM - Manager 212

Appendix 213

- A Miscellaneous Information 214
 - A.1 Port number list 214
 - A.2 Recognition procedure when an agent environment is changed 217
 - A.3 Summary of amendments 218

1

Building a basic configuration system (management servers and agents)

After building a basic configuration system, you can change the settings or install other configuration components to tailor your system configuration to your management needs. To build a system other than a basic configuration system, see [2. Building system configurations](#) first.

1.1 Overview of building a basic configuration system

To build a basic configuration system, build a management server, and then install an agent on the computers that will be managed.

1. Build the management server.
2. Register the JP1/IT Desktop Management 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.

Building of a basic configuration system is complete.

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 - Manager.

1.2.1 Types of JP1/IT Desktop Management - Manager installation

The following are the JP1/IT Desktop Management - 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 - Manager

To install JP1/IT Desktop Management - 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 that runs Windows 8, 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 - Manager, restart the OS regardless of whether installation was successful. If the service JP1_ITDM_Service does not start or JP1/IT Desktop Management - 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_ITDM_Service).
3. Perform overwrite installation again. (The service you stopped will start.)

To install JP1/IT Desktop Management - 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 - 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 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.
9. When the installation finishes, click the **Completed** button.

Installation of JP1/IT Desktop Management - 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 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 in a single-server configuration

When you perform a custom installation of JP1/IT Desktop Management - 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 - Manager, Tools**, and then **Setup**.
2. In the **Setup** view, click the **Next** button.
3. In the **Server Configuration Settings** view, select **Single-server configuration**, set **Cache size when accessing the database**, and then click the **Next** button.
This view appears only when the OS of the computer on which JP1/IT Desktop Management - Manager is installed is a 64-bit version.
4. In the **Server Configuration Settings** view, select a setup type, and then click the **Next** button.
This view does not appear for the initial setup after installation.
5. In the **Cluster Environment** view, specify the settings for using a cluster system, and then click the **Next** button.
6. In the **Folder Settings** view, specify the folders that will be used by JP1/IT Desktop Management - 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.
7. In the **Operation Log Settings** view, specify whether to record an operation log, and then click the **Next** button.
8. In the **Automatic Backup Setting for Operation Logs** view, specify whether to back up the operation log automatically, and then click the **Next** button.
9. 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.
10. In the **Port Number Settings** view, specify the port number to be used by JP1/IT Desktop Management - Manager, and then click the **Next** button.
11. In the **Other Settings** view, specify whether to use flow control when using the currency marks displayed in the operation window and the distribution functionality, and then click the **Next** button.
12. 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.
13. 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, site server programs, and network monitor agents. Registering these programs on the management server allows you to distribute an agent and install a site server program or to install a network monitor agent from the operation window.
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, 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 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](#)

1.4 Logging in to the Operation Window

This section describes how to log in to the Operation window of JP1/IT Desktop Management.

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.

You need to register a license for JP1/IT Desktop Management when logging in for the first time. To register the license, click the **License** button.

To log in:

1. Enter the following URL into the address bar of your Web browser:

`http://management-server-IP-address-or-host-name:port-number-for-connection-from-administrator-computer#/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

The password is valid for 180 days from the setup date. Beginning seven days prior to expiration, you will be prompted to change the password when logging in. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Important note

If login fails three times consecutively, the user account is locked. You must unlock the user account before you can use it to log in.

Related Topics:

- [1.4.4 Unlocking a user account](#)

1.4.2 Changing the default password

When you log in to JP1/IT Desktop Management for the first time by using the built-in account or a newly created account, you are required to change the password. If an administrator who has user account management permissions has changed the user account password, you are required to change the password the next time you log in. Make sure to change the default password to enhance security. After the password is changed, you must use the new password from the next login.

Tip

The password is valid for 180 days from the setup date. Beginning seven days prior to expiration, you will be prompted to change the password when logging in. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Tip

If the password you specified is easy to guess, your user account might be used illegally. We recommend that you specify a strong password by following the password policies described below:

- Use a combination of uppercase letters, lowercase letters, numbers, and symbols.
- Do not use an obvious sequence of characters, such as 12345.
- Do not use your name or birthday, the name or birthday of a friend or relative, or a word taken from a dictionary.

To change the password for the user account that is currently logged in, click the link of the user ID to the left of the **Log Out** button, and then change the password in the displayed dialog box.

An administrator who has user account management permissions can change the password for each user account in the **Account Management** view by selecting **User Management** in the Settings module and then **Account Management**.

1.4.3 Setting user account information

After logging in to JP1/IT Desktop Management, set user account information.

Click the link of the user ID to the left of the **Log Out** button, and then edit the user account information in the displayed dialog box.

Specify the following information for the user account:

- Name of the account user
- Email address of the account user

After you specify an email address for a user account, digest reports and notifications of search completion or event occurrences can be sent to that email address. We recommend that you specify an email address, so that the user can be made aware of the operating status without having to frequently check the operation window. Note that to receive such notifications, you also need to specify the recipients of digest reports, the search conditions, and the event notification settings, in addition to the email address.

Tip

You can also set user account information in the **Account Management** view by selecting **User Management** in the Settings module and then **Account Management**. In addition, you can also add a new user account in the **Account Management** view.

1.4.4 Unlocking a user account

A user account is locked if the user fails to log in three consecutive times. You must unlock the account before it can be used.

To unlock a user account:

1. Log in as a user who has user account management authority.
2. In the Settings module, select **User Management**, and then **Account Management** to display the **Account Management** view.
3. Click the **Edit** button of the locked user account.
4. In the dialog box that appears, select **Enabled** from **Status**.

The user account is unlocked.

Tip

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

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 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. Using the **Getting Started** wizard, you can search for devices connected to the network.

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

To search for devices connected to the network:

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

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

Important note

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

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

Important note

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

Important note

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

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

Important note

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

9. Set whether to automatically include the discovered devices as management targets and whether to automatically deploy agents to them, and then click the **Next** button.

10. If you want to inform yourself (administrator) of completion of the search by email, specify the notification destination and the mail server information, and then click the **Next** button.

11. In the **Confirm Content and Finish Settings** view, check the settings, and then click the **Complete** button.

12. In the displayed **Discovery Settings Configured** view, click the **Close** button.

The search is performed according to the set search schedule.

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

Tip

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

Related Topics:

- [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, and then install agents on them.

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

Tip

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

How to install agents

You can install agents on computers either manually or automatically.

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

Manually installing agents on computers

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

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

Automatically installing agents on computers

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

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

Related Topics:

- [1.6 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.

3. Select **Create Agent Installer**, and then click the **Next** button.

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

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

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

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

Change Installation Folder

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

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

Set the account to install Agent.

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

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

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

Downloading of the installation set begins.



Tip

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

Related Topics:

- [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.

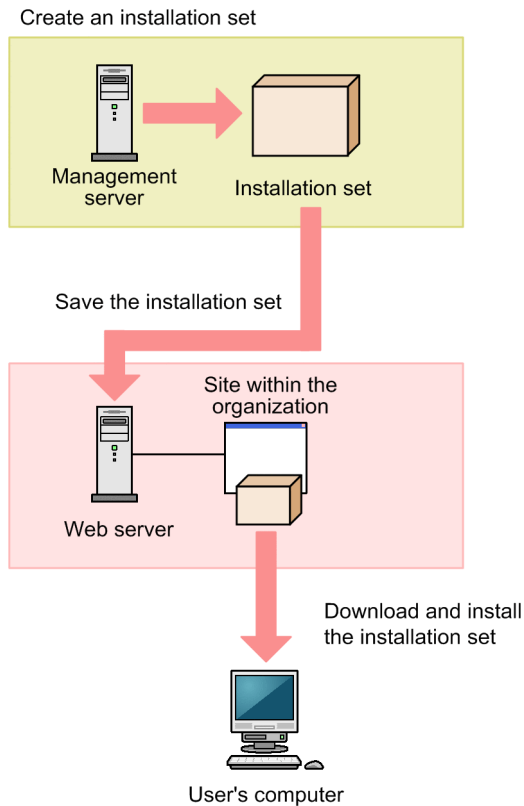
Advantage:

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.

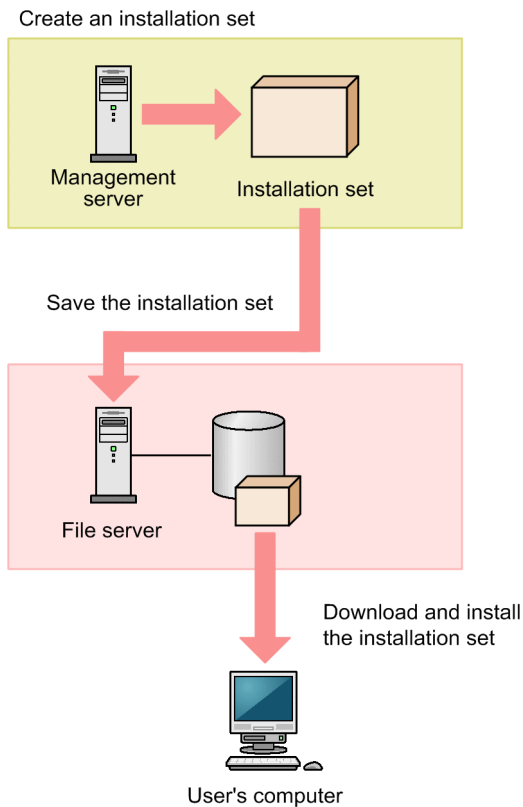
Advantage:

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:

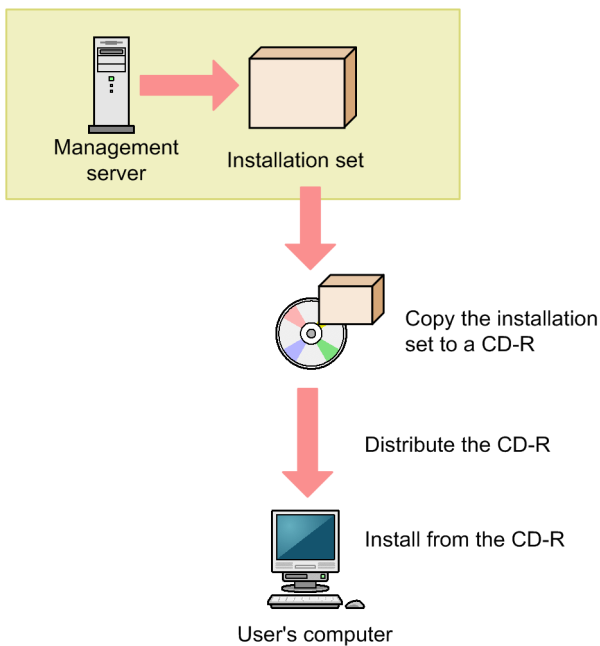
This approach does not require you to create a security control page on a Web site, or to create an environment that allows for shared folder. This approach is useful when there are relatively small number of computers on which to install agents. In addition, even when the network speed is slow, users 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:

Create an installation set



Tip

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

```
[Autorun]
```

```
open=ITDMAgt.exe
```

Related Topics:

- [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:

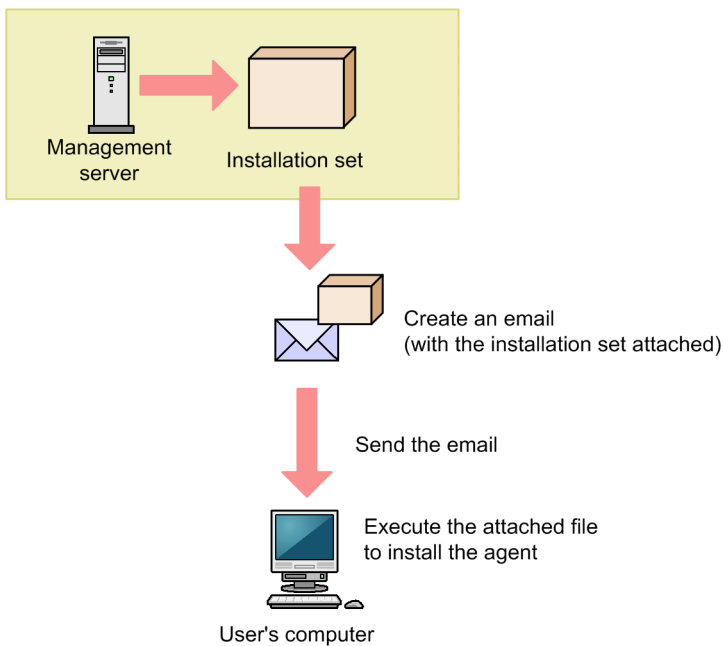
Sending emails to all applicable users is a quick way of having agents installed on a large number of computers.

Disadvantage:

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

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

Create an installation set



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

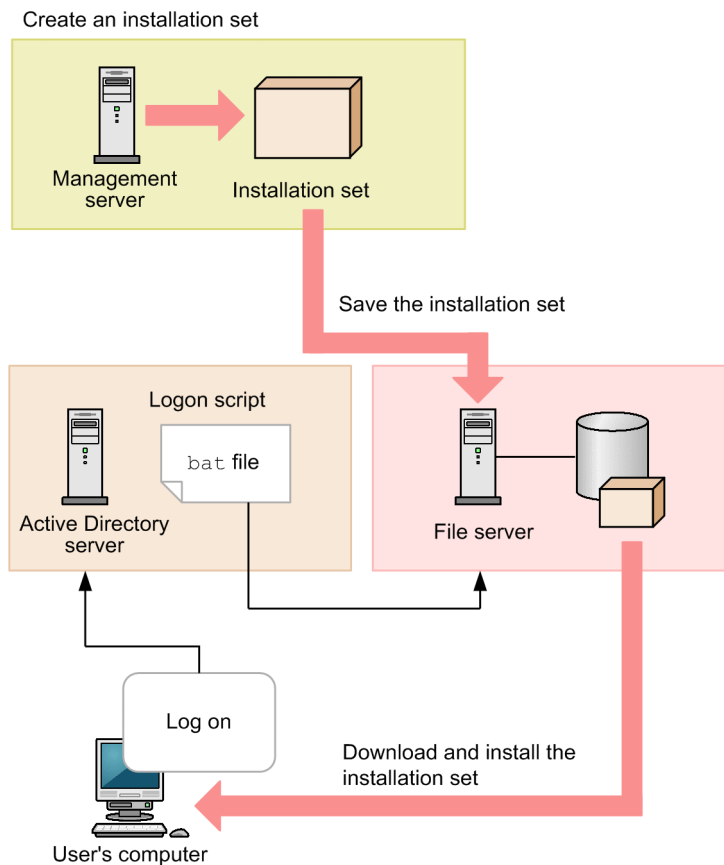
Advantage:

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

Disadvantage:

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

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



Related Topics:

- [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.

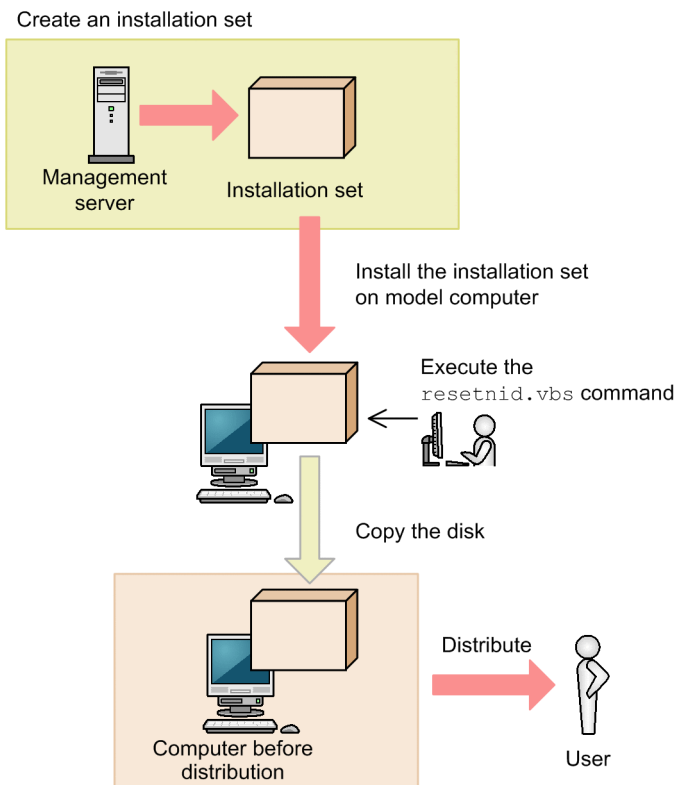
Advantage:

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](#)
- [8.10 resetnid.vbs \(resetting the host ID\)](#)

1.6.9 Procedure for installing the agent from supplied media

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

Important 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, do not specify the following folders during installation:

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

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 **JPI/IT Desktop Management - 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 select quick installation, go to step 7.

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

5. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.
6. In the dialog box indicating the preparations for starting installation are complete, click the **Install** button.
Installation starts.
7. 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 JPI/IT Desktop Management - 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.

To set up the agent:

1. From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - 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. In the **Setup** dialog box, specify the IP address or the host name of the destination management server and the port number, and then click the **OK** button.
3. 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 30 MB of data is transmitted to each computer.

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

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

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

Tip

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

1.7.3 Checking the device discovery status

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

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

- Active Directory discovery history

- IP discovery history

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

Discovered

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

Managed

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

Ignored

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

Related Topics:

- [1.7.4 Checking the latest discovery status](#)
- [1.7.5 Checking the discovered devices](#)
- [1.7.6 Checking the managed devices](#)
- [1.7.7 Checking the excluded devices](#)

1.7.4 Checking the latest discovery status

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

To check the latest discovery status:

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

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

Tip

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

1.7.5 Checking the discovered devices

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

To check the discovered devices:

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

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

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

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

Related Topics:

- [1.7.6 Checking the managed devices](#)
- [1.7.7 Checking the excluded devices](#)

1.7.6 Checking the managed devices

You can check the devices managed by JP1/IT Desktop Management 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 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 30 MB of data is transmitted to each computer.

To deploy agents to selected groups of computers:

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

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

Tip

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

2

Building system configurations

This chapter describes how to build each system configuration.

2.1 Building offline management configuration systems

2.1.1 Overview of building an offline management configuration system

To build an offline management configuration system, first build a basic configuration system, and then install the offline management agent on a computer.

1. Build the basic 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 basic configuration system \(management servers and agents\)](#)

2.2 Building agentless configuration systems

2.2.1 Overview of building an agentless configuration system

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

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

Building of the agentless configuration system is complete.

Tip

If you want to build a system that includes both computers with the agent installed and computers without an agent installed, build a basic configuration system first, and then go to step 2.

Related Topics:

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

2.3 Building site server configuration systems

2.3.1 Overview of building a site server configuration system

To build a site server configuration system, first build a basic configuration system first, and then specify the site server configuration settings and server configuration settings.

1. Build the basic configuration system.
2. Install the site server program on a computer on which an agent is installed, and then perform setup.
3. In the operation window, configure the server.

Building of the site server configuration system is complete.

Related Topics:

- [1. Building a basic configuration system \(management servers and agents\)](#)
- [2.3.2 Procedure for installing the site server program](#)
- [2.3.5 Procedure for setting up a site server](#)
- [4.3.1 Managing server configurations](#)

2.3.2 Procedure for installing the site server program

You can use either of the following methods to install the site server program. Select the appropriate method for your needs.

Installing the program from supplied media

On the applicable computer, proceed with the installation by specifying the necessary settings. When installation is complete, you must perform setup. If you want to specify special values during installation and setup, we recommend this method.

Installing the program in the operation window

In the operation window that opens on the administrator's computer, select the computer on which you want to install the program. The default values are used during installation and setup. We recommend this method if you do not need to specify special settings.

Tip

When the site server program is installed, a message appears at the top of the Home module and in the **Topic** panel.

2.3.3 Procedure for installing the site server program from the supplied media

When you install the site server program, you must log on to a computer with an installed agent as a user with administrator permissions.

Important note

If you install the program on a Windows computer that supports User Account Control (UAC), a dialog box that asks for elevating permissions might appear. If this dialog box opens, elevate permissions.

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 that runs Windows 8, do not specify the following folders during installation:

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

Tip

You cannot install the site server program on a management server.

To install the site server program from supplied media:

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 - Remote Site Server**, and then click the **Install** button.
3. In the dialog box indicating the start of installation, click the **Next** button.
4. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.
5. In the **Installation folder** dialog box, select the installation folder, and then click the **Next** button.
6. In the confirmation dialog box used for the installation, make sure the installation is correct, and then click the **Install** button.
Installation starts. If you notice a problem, click the **Back** button to correct the applicable setting.
7. When installation finishes, click the **Completed** button.

Installation of the site server program is complete. If a message asking you to restart the computer appears, restart it.

After installation, setup must be performed to create a database. If you selected **Setup**, setup starts automatically when installation finishes.

2.3.4 Procedure for installing the site server program in the operation window

In the Device module of the operation window, you can select a computer on which an agent is installed to install the site server program.

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.

Tip

To install the site server program from the Device module, you must have registered the component (site server program) beforehand on the management server.



Tip

You cannot install the site server program on a management server.

To install the site server program in the operation window:

1. Open the Device module.
2. In the menu area, select the list of devices in **Device Inventory** to display in the information area the computer on which you want to install the site server program.
3. In the information area, select a computer on which an agent is installed.
4. From **Actions**, select **Install Site Server Program**.
5. In the **Install Site Server Program** dialog box, click the **OK** button.

The site server program is installed on the computer you selected. If you want to install the site server program on multiple computers, repeat this procedure for each computer.

An icon (  ) indicating the management type is displayed on a computer on which the site server program is installed.

Tip

Disconnection by network access control is suppressed for computers on which the site server program is installed. In addition, the site server program is automatically registered as an exclusive communication destination. However, if you install the site server program on a computer that has already been disconnected, connection to the network will not be permitted.

2.3.5 Procedure for setting up a site server

When you install the site server program from the supplied media, you must perform setup as soon as installation is complete to create a database and specify the environment settings.

To set up a site server:

1. From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Remote Site Server**, 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 **Folder Settings** view, specify the folders used by the site server program, and then click the **Next** button.
5. In the **Port Number Settings** view, set the port number to be used by the site server program, and then click the **Next** button.
6. In the **Other Settings** view, specify whether to use flow control when using the distribution functionality, and then click the **Next** button.
7. In the **Confirm Setup Settings** view, make sure the setup information 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.
8. When setup finishes, click the **OK** button.

Setup is complete, and the site server starts operation with the specified settings.

Tip

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

2.4 Building multi-server configuration systems

2.4.1 Overview of building a multi-server configuration system

To build a multi-server configuration system, first build a management server and a database server, and then install an agent on the computers that will be managed.

Important note

Before building a system, specify the following settings in **Date & Time** in **Control Panel** in Windows:

- On the **Date & Time** page, synchronize the date and time of the management server and the date and time of the database server.
- On the **Time Zone** page, set the same time zone for the management server and the database server.

During operation, we recommend that you select the **Automatically synchronize with an Internet time server** on the **Internet Time** page.

Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

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

1. Build a database server.

Perform a custom installation of JP1/IT Desktop Management - Manager on the computer that will be used as the database server. After installation, start setup, and then in the **Server Configuration Settings** view, select **Multi-server configuration**, and then **Database server**.

Also, in the **Folder Settings** view, specify a folder that can be accessed from a management server by setting sharing in **Data folder**.

2. Set the folder specified in **Data folder** during database setup as the shared folder that can be accessed from the management server.

3. Build a management server.

Perform a custom installation of JP1/IT Desktop Management - Manager on the computer that will be used as the management server. After installation, start setup, and then in the **Server Configuration Settings** view, select **Multi-server configuration**, and then **Management Server**.

Also, in the **Settings for the Data Folder Shared Between** view, specify the folder set as the shared folder in step 2 in **Data folder shared between servers**.

4. Register the JP1/IT Desktop Management product license.

5. Log in to the operation window and set user account information.

6. Have a good understanding of the devices in the organization, and prepare a plan that covers the computers on which an agent is to be installed and the installation method.

7. Install an agent on the computers that will be managed by JP1/IT Desktop Management.

Building of the multi-server configuration system is complete.

Related Topics:

- [1.2.2 Procedure for installing JP1/IT Desktop Management - Manager](#)
- [2.4.2 Procedure for setting up a database server](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)

2.4.2 Procedure for setting up a database server

To build a database server for a multi-server configuration system, setup the database server by specifying the necessary settings as soon as the custom installation of JP1/IT Desktop Management - Manager finishes.

To change the database server settings in a multi-server configuration system, use the following procedure to set up the database server. Next, select **Settings Modification** on the management server to perform setup. It is not necessary to change the settings in the management server setup.

To set up a database server:

1. From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**.
2. In the **Setup** view, click the **Next** button.
3. In the **Select a Setup** view, select the setup type, and then click the **Next** button.
This view dose not appear in the initial setup after installation.
4. In the **Server Configuration Settings** view, select **Multi-server configuration, Database server** and then **16GB**, and then, click the **Next** button.
5. In the **Cluster Environment** view, specify whether to use a cluster environment, and then click the **Next** button.
If you are using a cluster environment and select **Primary**, you can skip step 6, and go to step 7.
If you are using a cluster environment and select **Secondary**, steps 6 to 10 will be skipped.
6. In the **Database Connection Settings** view, specify the IP address of the database server, and then click the **Next** button.
7. In the **Folder Settings** view, specify the folders used by JP1/IT Desktop Management - Manager, and then click the **Next** button.

Important note

For the **data folder**, specify a folder that can be accessed from the management server by setting sharing.

8. 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.
9. In the **Port Number Settings** view, specify the port number to be used by JP1/IT Desktop Management - Manager, and then click the **Next** button.

10. In the **Other Settings** view, specify whether to use the currency marks displayed in the operation window, and whether to use flow control when using the distribution functionality, and then click the **Next** button.
11. 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.
12. In the view that indicates that setup is complete, click the **OK** button.
If **Register components** appears, specify whether to register the components after setup, and then click the **OK** button.
Components include agents, site server programs, and network monitor agents. Registering these programs on a database server allows you to distribute an agent, or install a site server program or network monitor agent from the operation window.
When you register a component, specify the registration and update settings related to the component in the displayed **Component Registration** dialog box.

Tip

If you start setup after installation, you can set update related settings for components in the view that indicates that setup is complete.

When setup finishes, the database server starts operation with the specified settings.

If you want to continue by building a management server, set the folder you specified as the **data folder** as a shared folder that can be accessed from the management server.

Tip

In the initial setup after a custom installation, a new database will be created as part of the setup process.

Related Topics:

- [5.7 Updating components](#)

2.4.3 Procedure for setting up a management server for a multi-server configuration system

To build a management server for a multi-server configuration system, setup the management server as soon as the custom installation of JP1/IT Desktop Management - Manager finishes.

Before you can build a management server, a database server must have been built. Also, during database server setup, set the folder specified in **Data folder** as a shared folder that can be accessed from the management server.

Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

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

To set up a management server:

1. From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**.
2. In the **Setup** view, click the **Next** button.
3. In the **Select a Setup** view, select the setup type, and then click the **Next** button.
This view dose not appear in the initial setup after installation.
4. In the **Server Configuration Settings** view, select **Multi-server configuration** and **Single-server configuration**, and then click the **Next** button.
5. In the **Cluster Environment** view, specify whether to use a cluster environment, and then click the **Next** button.
If you are using a cluster environment and select **Secondary**, skip steps 6 and 7, and go to step 8.
6. In the **Folder Settings** view, specify the data folder that will be used by JP1/IT Desktop Management, and then click the **Next** button.
7. In the **Settings for the Data Folder Shared Between Servers** view, specify the database server and the shared folder, and then click the **Next** button.
8. In the **Confirm Setup Settings** view, make sure the setup information 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.
9. In the view indicating that setup is complete, click the **OK** button.

Setup is complete, and the management server starts operation with the specified settings.

Related Topics:

- [2.4.1 Overview of building a multi-server configuration system](#)
- [2.4.2 Procedure for setting up a database server](#)

2.5 Building support service linkage configuration systems

2.5.1 Overview of building a support service linkage configuration system

To build a support service linkage configuration system, first build a basic configuration system, and then set the information needed to access the support service site.

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

Tip

To determine the status of update programs on a managed computer, or to have action taken based on a judgment, you must set a security policy. For details about how to use the security policy to manage update programs, see the *Job Management Partner 1 Version 10 Job Management Partner 1/IT Desktop Management Administration Guide*.

Building of the support service linkage configuration system is complete.

Related Topics:

- [4.4.1 Setting information for connecting to the support service](#)

2.6 Building Active Directory linkage configuration systems

2.6.1 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 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](#)
- [4.5.1 Setting information for connecting to Active Directory](#)
- [4.5.2 Setting the information acquired from Active Directory as an additional management item](#)
- [4.5.3 Searching for devices registered in Active Directory](#)

2.7 Building MDM linkage configuration systems

2.7.1 Overview of building a MDM linkage configuration system

To build a MDM linkage configuration system, first build a basic system, and then obtain information about smart devices from the MDM system.

1. Build the basic configuration system.
2. Set the information for linking JP1/IT Desktop Management 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:

- [4.6.1 Specifying settings to link with an MDM system](#)

2.8 Building network monitoring configuration systems

2.8.1 Overview of building a network monitoring configuration system

To build a network monitoring configuration system, first build a basic configuration system, and then enable network access control for each network segment.

1. Build the basic 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 \(discovery from IP address\)](#)
- [4.7.1 Editing devices in the network control list](#)
- [2.8.2 Enabling the network monitor](#)
- [4.7.3 Adding network monitor settings](#)
- [4.7.4 Changing assignment of network monitor settings](#)




2.8.2 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 in the group in the menu area.

Important note

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

Important note

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

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

Important note

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

Important note

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

Tip

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

Tip

You can also enable the network monitor by using the provided media to install JP1/IT Desktop Management - Network Monitor on the computer on which the agent is installed.

Tip

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

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

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

To build a JP1/NETM/NM - Manager linkage system, first build a basic configuration system, and then deploy network control appliances. Next, install JP1/NETM/NM - Manager, and enable linkage with JP1/NETM/NM - Manager.

For details about how to install and set up JP1/NETM/NM - Manager, see the relevant descriptions in the *Job Management Partner 1 Version 9 Job Management Partner 1/Network Monitor - Manager Description, User's Guide and Operator's Guide* or the *Job Management Partner 1 Version 10 Job Management Partner 1/NETM/Network Monitor - Manager*. For details about how to specify JP1/NETM/NM - Manager settings, see the descriptions of operations in the *Job Management Partner 1 Version 9 Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide* or the *Job Management Partner 1 Version 10 Job Management Partner 1/NETM/Network Monitor*.

1. Build a basic 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 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, 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 [4.7.6 Procedure for editing the network control settings file](#).
10. In JP1/IT Desktop Management, enable linkage with JP1/NETM/NM - Manager.
For details about this procedure, see [4.7.5 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 basic configuration system](#)

2.10 Building JP1/IM linkage configuration systems

2.10.1 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. For a single-server configuration, install JP1/Base on the management server. For a multi-server configuration system, install JP1/Base on the database 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-installation-folder\mgr\definition  
\hitachi_jp1_itdm_attr_ja.conf
```

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

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

Destination folder of the definition file for extended event attributes

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

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

```
system-drive:\Program Files\HITACHI\JP1Cons
```

6. Restart JP1/IM - Manager.

The settings for the definition file for extended event attributes take effect when JP1/IM - Manager is restarted.

7. Specify connection settings for JP1/Base and JP1/IM.

8. Restart JP1/IT Desktop Management and P1/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:

- [4.8.1 Procedure for setting the configuration file used for linkage with JP1/IM](#)

2.11 Building a cluster system

2.11.1 Overview of building a cluster system in a single-server configuration system

When building a cluster system in a single-server configuration system, build a management server first.

To build a cluster system:

1. Install JP1/IT Desktop Management - 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 online.
Bring the service resources (generic services) other than JP1_ITDM_Service and JP1_ITDM_Agent Control that are registered in a management server group online by using Microsoft Cluster Service or Windows Server Failover Cluster.
9. In the operation window, register the license.
10. Bring the JP1/IT Desktop Management services online.
Bring JP1_ITDM_Service and JP1_ITDM_Agent Control online.

Building of the cluster system is complete.

Related Topics:

- [1.2.2 Procedure for installing JP1/IT Desktop Management - Manager](#)
- [2.11.3 Procedure for creating a group resource on the primary server](#)
- [2.11.4 Setting up JP1/IT Desktop Management on the primary server](#)
- [2.11.5 Setting up JP1/IT Desktop Management on the standby server](#)
- [1.3.1 Registering a product license](#)

2.11.2 Overview of building a cluster system in a multi-server configuration system

To build a cluster system in a multi-server configuration system, first build a database server and then build a management server.

To build a cluster system in a multi-server configuration system:

1. Install JPI/IT Desktop Management - Manager on the primary and standby servers of the management server and the database server.
Select custom installation as the installation type. After installation, do not continue by performing setup.
2. Create a group resource on the primary server of the database server.
3. Set up the primary server of the database server.
4. Copy the file that is output when setup of the primary server for the database server finishes, to the standby server of the database 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 of the database server.
6. Set up the standby server of the database server.
7. Move the owner of the group resource you created in step 2 to the primary server of the database server.
8. Bring all service resources on the database server online.
9. Create a group resource on the primary server of the management server.
10. Set up the primary server of the management server.
11. Copy the file that is output when setup of the primary server for the management server finishes, to the standby server for the management server.
12. To perform setup on the standby server, move the owner of the group resource you created in step 9 to the standby server of the management server.
13. Set up the standby server of the management server.
14. To start cluster system operation, move the owner of the group resource you created in step 9 to the primary server of the management server.
15. Bring the service resources that are a part of JPI/IT Desktop Management online.
Bring the service resources (generic services) other than *JPI_ITDM_Service* and *JPI_ITDM_Agent Control* that are registered in a group on the management server online by using Microsoft Cluster Service or Windows Server Failover Cluster online.
16. In the operation window, register the license.
17. Bring the JPI/IT Desktop Management service resources online.
Bring *JPI_ITDM_Service* and *JPI_ITDM_Agent Control* online.

Building of the cluster system in the multi-server configuration system is complete.

Related Topics:

- 1.2.2 Procedure for installing JP1/IT Desktop Management - Manager
- 2.11.3 Procedure for creating a group resource on the primary server
- 2.11.4 Setting up JP1/IT Desktop Management on the primary server
- 2.11.5 Setting up JP1/IT Desktop Management on the standby server
- 1.3.1 Registering a product license

2.11.3 Procedure for creating a group resource on the primary server

After JP1/IT Desktop Management has been installed, use Microsoft Cluster Service or Windows Server Failover Cluster to create a JP1/IT Desktop Management 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 Microsoft Cluster Service or Windows Server Failover Cluster.

2. Register the resources that are necessary for the group you created.

The table below lists the resources that must be registered in the group. Note that the resources that must be registered differ depending on the server configuration.

For single-server configuration systems:

Resource type	Resource name
Resources other than JP1/IT Desktop Management service resources	IP address resource
	Network name resource
	Shared disk (physical disk) resource
JP1/IT Desktop Management service resources (generic services)	JP1_ITDM_DB Service
	JP1_ITDM_DB Cluster Service
	JP1_ITDM_Web Container [#]
	JP1_ITDM_Web Server
	JP1_ITDM_Service
	JP1_ITDM_Agent Control

[#]: If the OS is Windows Server 2012 or Windows Server 2008, you must create resources from the CLI. Before you can create resources, make sure that you log on as a member of the Administrators group. To create a resource, execute the following command from the command prompt:

```
cluster res "name-of-a-JP1_ITDM_Web-Server-service-resource" /priv
StartupParameters=""
```

For multi-server configuration systems:

Resource type	Resource name	Registration required	
		Management server	Database server
Resources other than JP1/IT Desktop Management service resources	IP address resource	Y	Y
	Network name resource	Y	Y

Resource type	Resource name	Registration required	
		Management server	Database server
Resources other than JP1/IT Desktop Management service resources	Shared disk (physical disk) resource	--	Y
JP1/IT Desktop Management service resources (generic services)	JP1_ITDM_DB Service	--	Y
	JP1_ITDM_DB Cluster Service	--	Y
	JP1_ITDM_Web Container	Y	--
	JP1_ITDM_Web Server	Y	--
	JP1_ITDM_Service	Y	Y
	JP1_ITDM_Agent Control	Y	--

Legend: Y: Resource that must be registered, --: Resource that does not need to be registered

3. Set the primary server as the priority server.

4. Bring the resources other than JP1/IT Desktop Management service resources online.

The JP1/IT Desktop Management service resources (generic services) remain offline.

The group resource is created.

For details about how to create a group resource, see the documentation for Microsoft Cluster Service or 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 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_ITDM_DB Service settings

Resource name	Setting item	Setting value
JP1_ITDM_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.

Resource name	Setting item	Setting value
JP1_ITDM_DB Service	Failover threshold	0 (fixed)
	Failover period (in seconds)	0 (fixed)
	Wait timeout (in seconds)	300 (recommended)

JP1_ITDM_DB Cluster Service settings

Resource name	Setting item	Setting value
JP1_ITDM_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_ITDM_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_ITDM_Web Container settings

Resource name	Setting item	Setting value
JP1_ITDM_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.
	Dependency	For a single-server configuration system, set the JP1_ITDM_DB Cluster Service resource. For a multi-server configuration system, set the network name and physical disk resources.
	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_ITDM_Web Server settings

Resource name	Setting item	Setting value
JP1_ITDM_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_ITDM_Service settings

Resource name	Setting item	Setting value
JP1_ITDM_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	For a single-server configuration system, or a database server in a multi-server configuration system, set the JP1_ITDM_DB Cluster Service resource. For a management server in a multi-server configuration system, set the network name and physical disk resources.
	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_ITDM_Agent Control settings

Resource name	Setting item	Setting value
JP1_ITDM_Agent Control	Name	Specify a name.
	Resource type	Set a generic service.

Resource name	Setting item	Setting value
JP1_ITDM_Agent Control	Group	Set the group name of a management server.
	Possible owner	Set both the primary and standby servers.
	Dependency	For a single-server configuration system, set the JP1_ITDM_DB Cluster Service resource. For a multi-server configuration system, set the network name and physical disk resources.
	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)

2.11.4 Setting up JP1/IT Desktop Management on the primary server

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

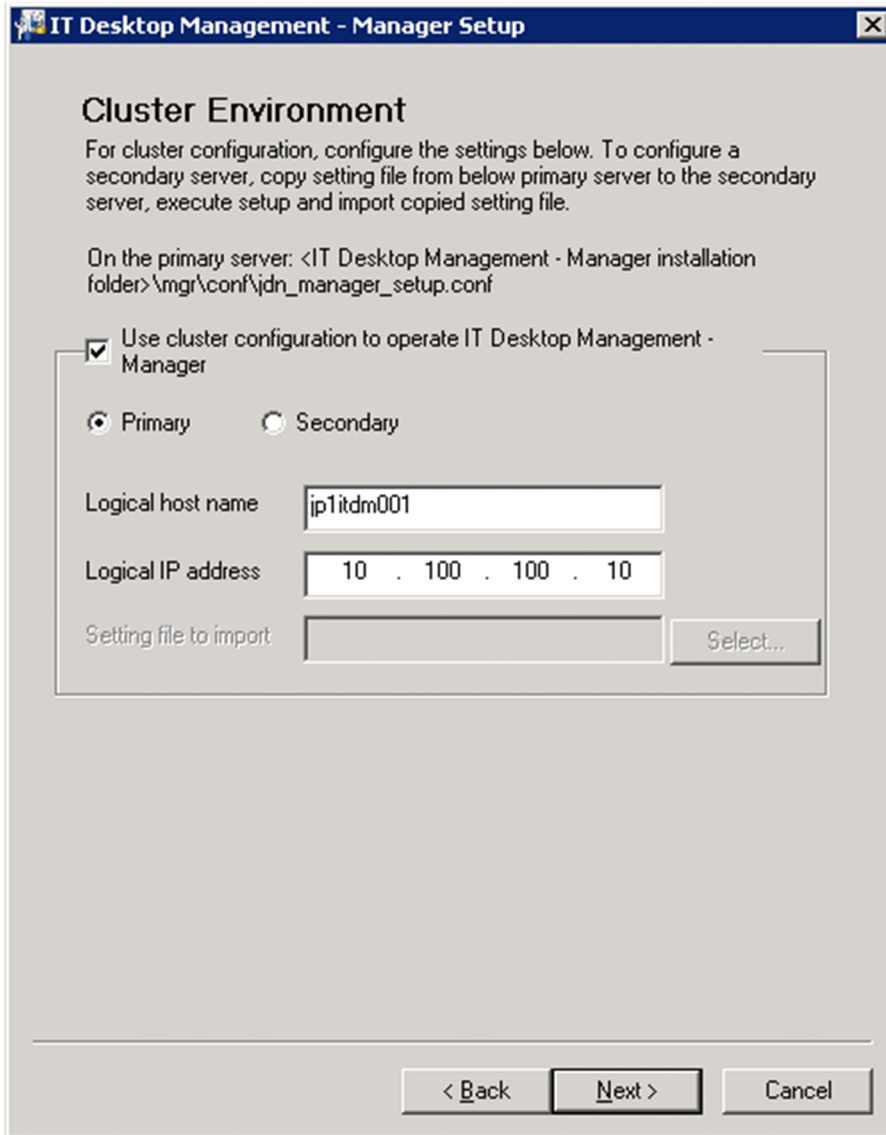
Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

- 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 - Manager**.
- Select **Primary**.
- Set **Logical host name** and **Logical IP address**.

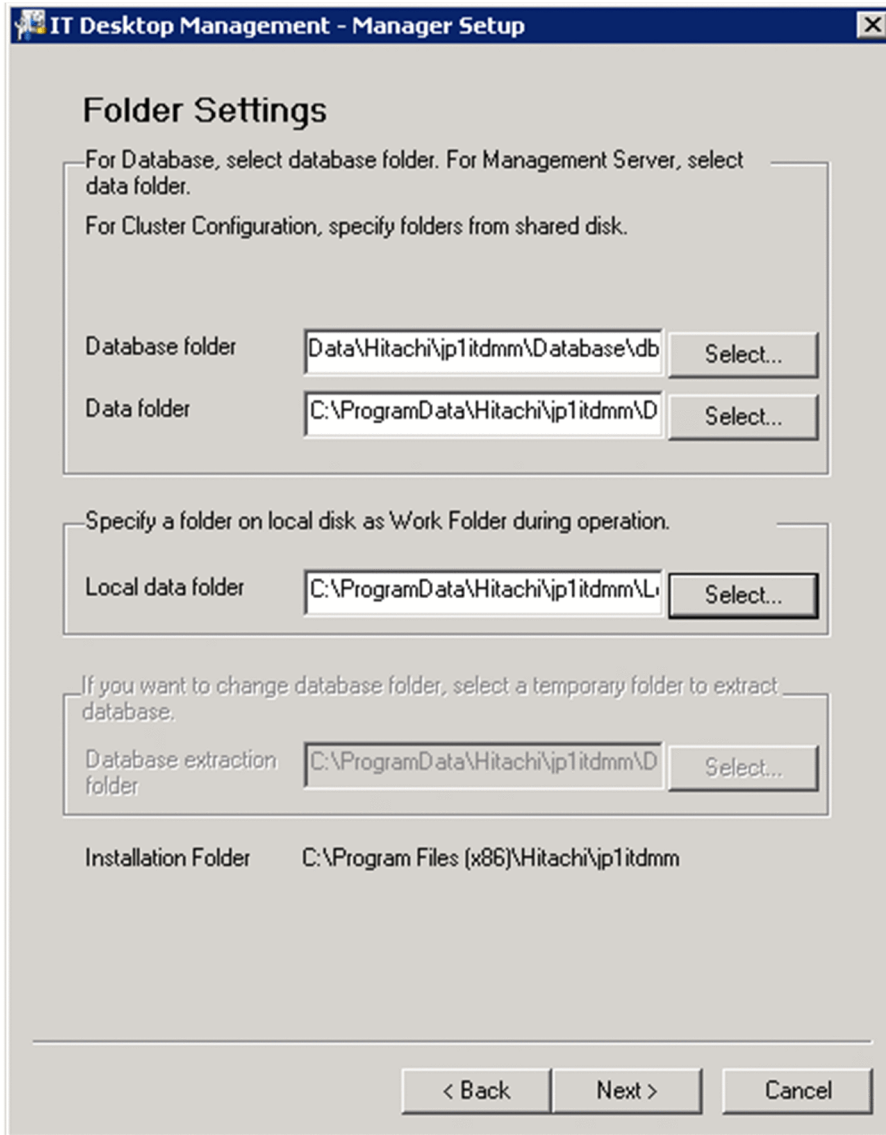
For this operation, you do not need to set **Setting file to import**.

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

JP1/IT Desktop Management-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** in the **Operation Log Settings** view (when recording an operation log)
- **Operation log backup folder** in the **Automatic Backup Setting for Operation Logs** view (when specifying a folder on the local disk as the folder for storing the operations log)
- **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 in a single-server configuration](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)

- [2.4.2 Procedure for setting up a database server](#)

2.11.5 Setting up JP1/IT Desktop Management 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 - 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 in a single-server configuration](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)
- [2.4.2 Procedure for setting up a database server](#)

3

Changing settings

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

3.1 Procedure for changing the setting for connection to the database

Set the IP address of a database server that is connected to JP1/IT Desktop Management.

To set the IP address of the database server in a multi-server configuration system, use the following procedure on the database server. Next, select **Settings Modification** on the management server to perform setup again. It is not necessary to change the management server setup settings.

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_ITDM_Agent Control
- JP1_ITDM_Service
- JP1_ITDM_Web Container
- JP1_ITDM_Web Server

2. Log on to the OS as a user with administrator permissions.

3. On the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**.

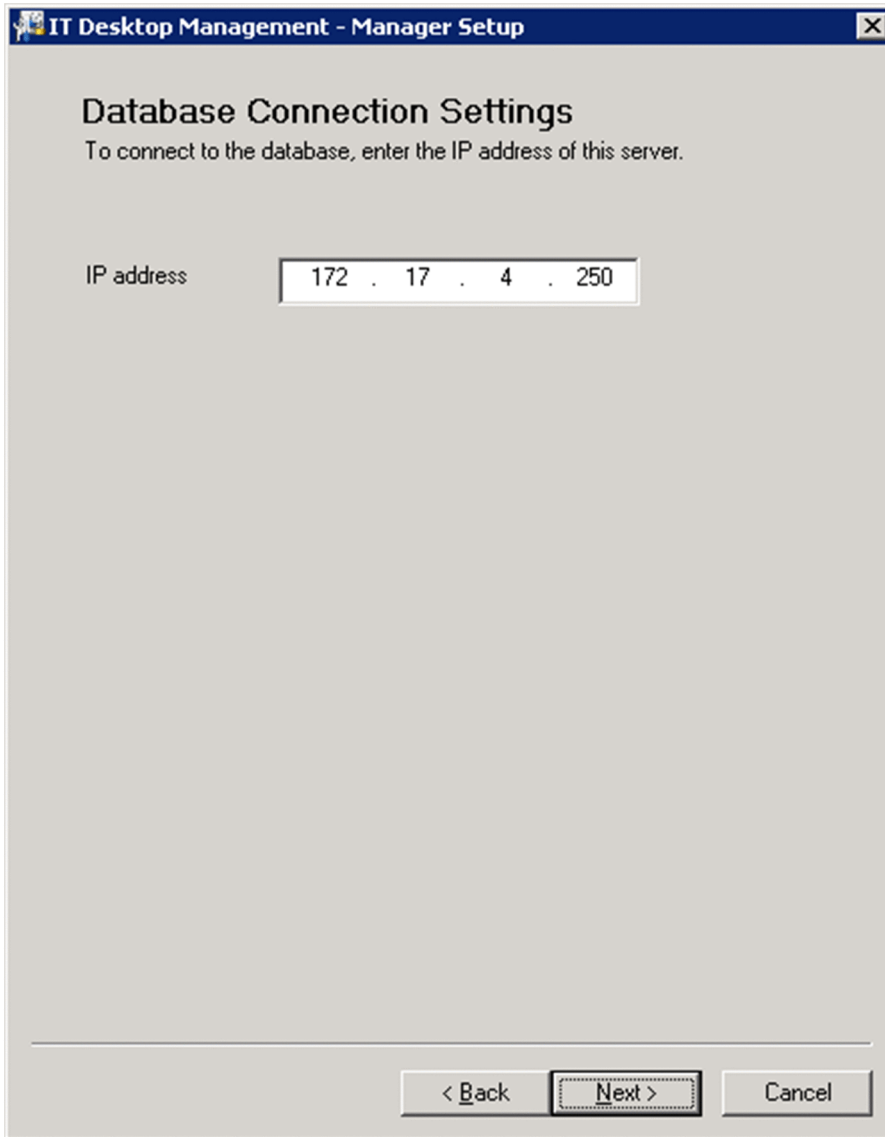
4. In the Setup window, click the **Next** button.

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

6. In the **Server Configuration Settings** view, click the **Next** button.

7. In the **Cluster Environment** view, select the setting indicating that a cluster configuration is not being used, and then click the **Next** button.

8. In the **Database connection Settings** view, enter the IP address of the database server, and then click the **Next** button.



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

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

Setup starts, and a dialog box indicating the progress appears. When 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.

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

The IP address of the database server that is connected to JP1/IT Desktop Management is changed.

3.2 Procedure for changing the folders that are used

You can change the folders you use on a management server, a database server, or a site 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.

To change a folder used in a multi-server configuration system, use the following procedure on the database server. Then select **Settings Modification** on a management server to perform setup. It is not necessary to change the management server setup settings.

Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

- 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. On the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools, and Setup**, or **All Programs, JP1_IT Desktop Management - Remote Site Server, 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 **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.

Although the data in data folders is moved to the new folder, the data folder for the operation logs in the old folder and any data stored in the folder remain in the old folder. In the new folder, operations data logged after the change of folders is saved.

3.3 Procedure for changing a data folder shared by servers

This is a management server setup item.

You can set a data folder that will be shared by JP1/IT Desktop Management and database servers.

Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

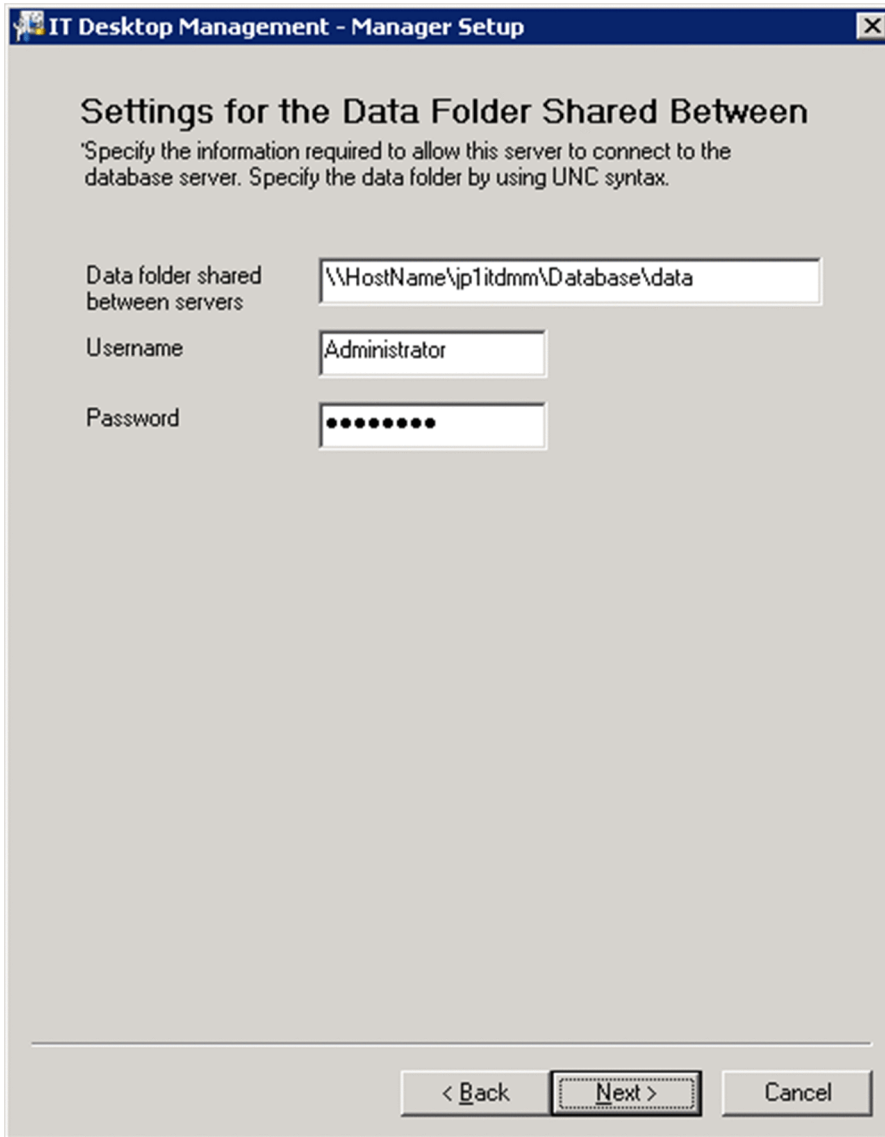
- Folders under *system-drive*:\program files\WindowsApps
- Folders in storage areas created by virtual provisioning

To set a data folder for sharing:

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 - 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 **Server Configuration Settings** view, click the **Next** button.
6. Continue to click the **Next** button until the **Settings for the Data Folder Shared Between** view opens.
7. In the **Settings for the Data Folder Shared Between** view, set the path to the data folder that will be shared by the servers, the user name, and the password, and then click the **Next** button.

Specify the path in UNC format.

The following is a screenshot of a management server.



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.

Setup starts, and a dialog box indicating the progress appears. When 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.

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

You can access data folders shared among servers.

3.4 Procedure for specifying the settings used for recording an operation log on a management server in a single-server configuration system

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.

Tip

Because operation logs cannot be obtained from a management server in a multi-server configuration system, you cannot use the settings described here. If you want to obtain operation logs in a multi-server configuration system, use a site server to obtain distributed operation logs.

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.

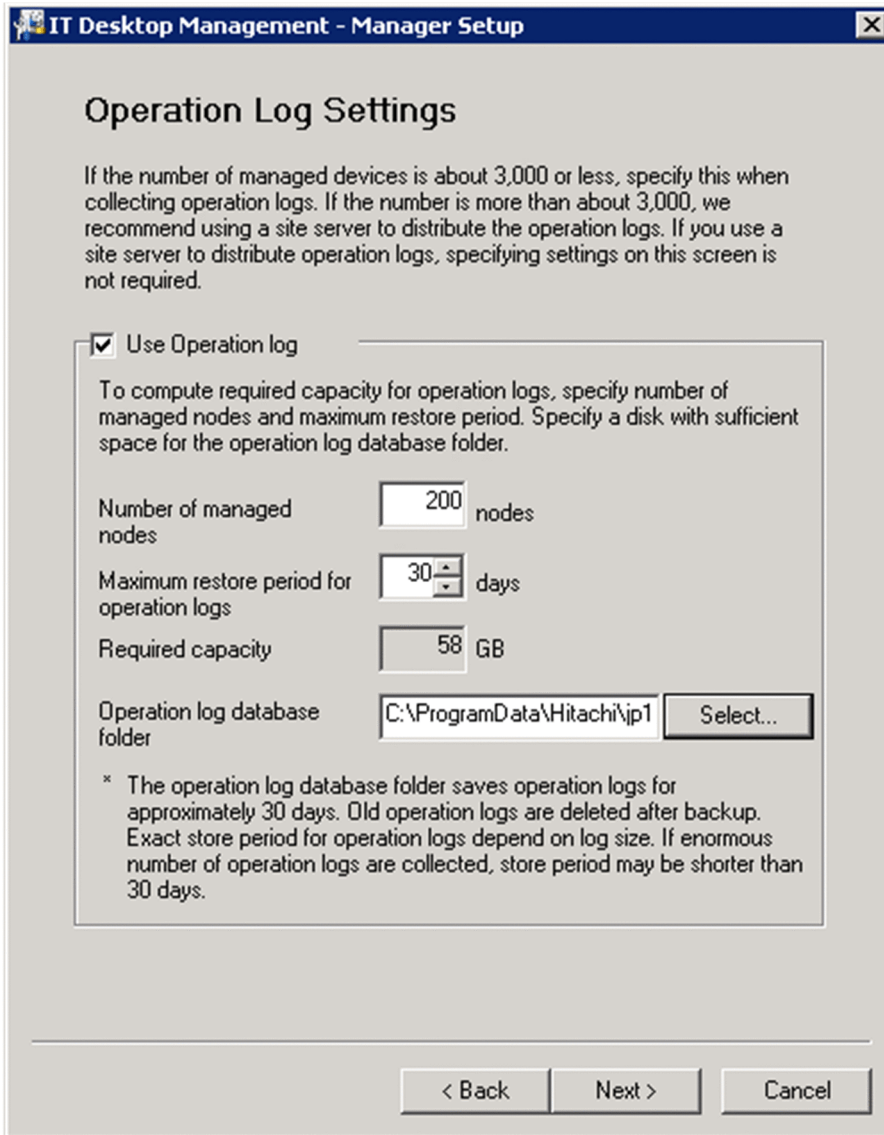
Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

- 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 - 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 **Use Operation log**, and then set the following items:

- **Total Managed Nodes**

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

- **Maximum restore period for operation logs**

User operation logs are saved for one month in the folder specified in **Operation log database**. Operation logs older than one month are automatically saved in a separate folder that can be imported when you want to see those logs.

Specify the number of days that you want operation logs to be saved automatically in the separate folder.

If you want to specify this value, use the **Automatic Backup Setting for Operation Logs** view that opens next.

- **Required capacity**

This value is calculated automatically based on the values specified in **Total Managed Nodes** and **Maximum restore period for operation logs**.

- **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 restore period for operation logs** 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.

- Click the **Next** button.
- If you specify **Maximum restore period for operation logs** in the **Operation Log Settings** view, select **Backup Operation logs automatically** in the **Automatic Backup Setting for Operation Logs** view to specify **Operation log backup folder**.

IT Desktop Management - Manager Setup

Automatic Backup Settings for Operation Logs

Configure the settings below for Operation log automatic backup.

Backup Operation logs automatically

Specify backup location for operation logs. To specify a folder on the network, enter location in UNC format and specify user name/password used for the connection.

Operation log backup folder

Username

Password

* When you change the operation log backup folder, existing backup files will not be moved. If necessary, move backup files to changed backup location.

< Back Next > Cancel

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

11. 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 restore period for operation logs**.

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

In a single-server configuration, perform the procedure described below on the management server. In a multi-server configuration, perform the procedure on the database 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 - Manager, Tools, and then Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Modify settings**, 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 - 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.

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 8, do not specify the following folders during installation:

- 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. Setup starts and a dialog box that notifies you that processing is in progress appears. When setup terminates, the **Setup Complete** view appears.

If it is necessary to stop services, a dialog box asking you whether to stop services appears. If this dialog box appears, click the **OK** button to stop services.

9. 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.

3.6 Procedure for changing a port number

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

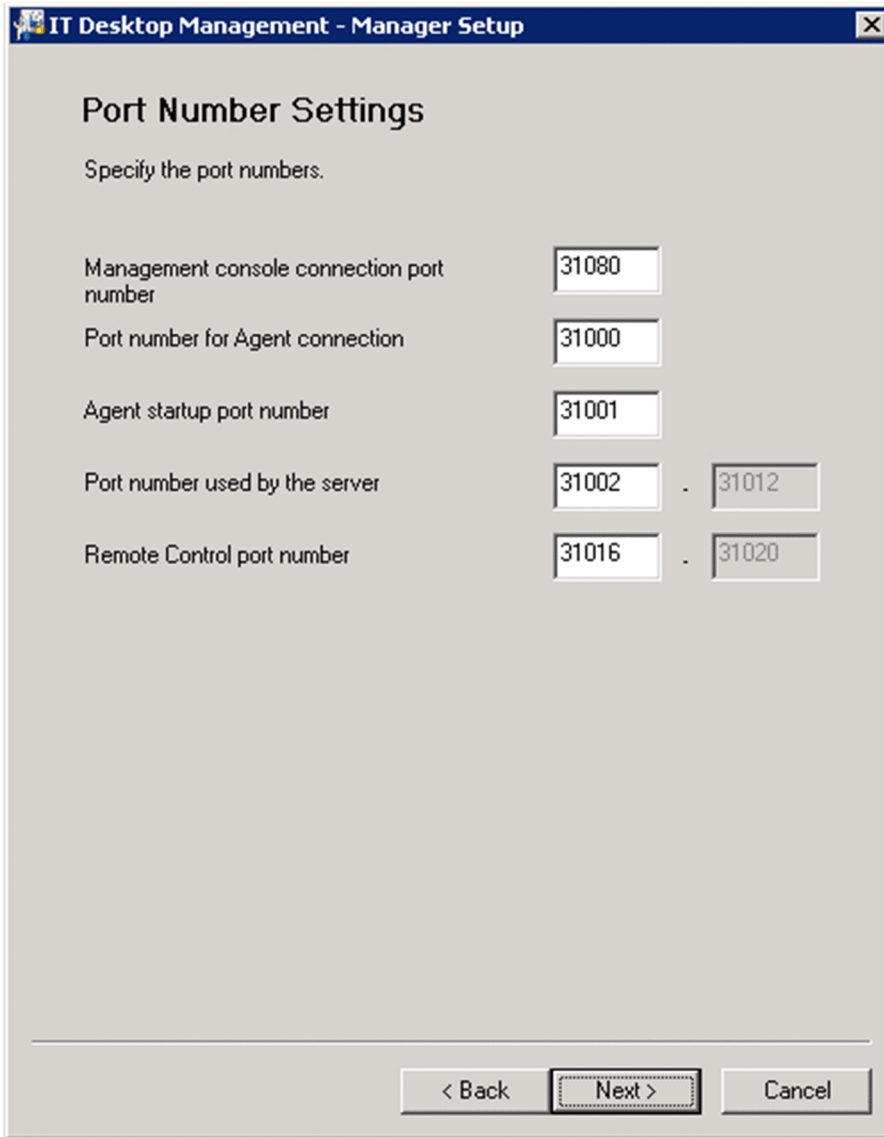
To change a port number in a multi-server configuration system, use the following procedure on the database server. Then select **Settings Modification** on a management server to perform setup. It is not necessary to change the management server setup settings.

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. On the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**, or **All Programs, JP1_IT Desktop Management - Remote Site Server**, and then **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Port Number Settings** view opens.



6. Change a port number as needed.

The following port numbers on management servers can be changed:

Management console connection port number

On the computer on which JP1/IT Desktop Management 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.

Remote Control port number

Enter the port number used by the remote control functionality.

You can change the following port number for site servers:

Port number used for the site server

Enter the port number used on the site server.

For details about port numbers, see [A.1 Port number list](#).

7. Continue to click the **Next** button until the **Confirm Setup Settings** view opens.
8. In the **Confirm Setup Settings** view, check the settings, and then click the **Next** button.
Setup starts, and a dialog box indicating the progress appears. When setup finishes, the **Setup Complete** view appears.
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.
9. In the **Setup Complete** view, click the **OK** button.

The port number is changed.

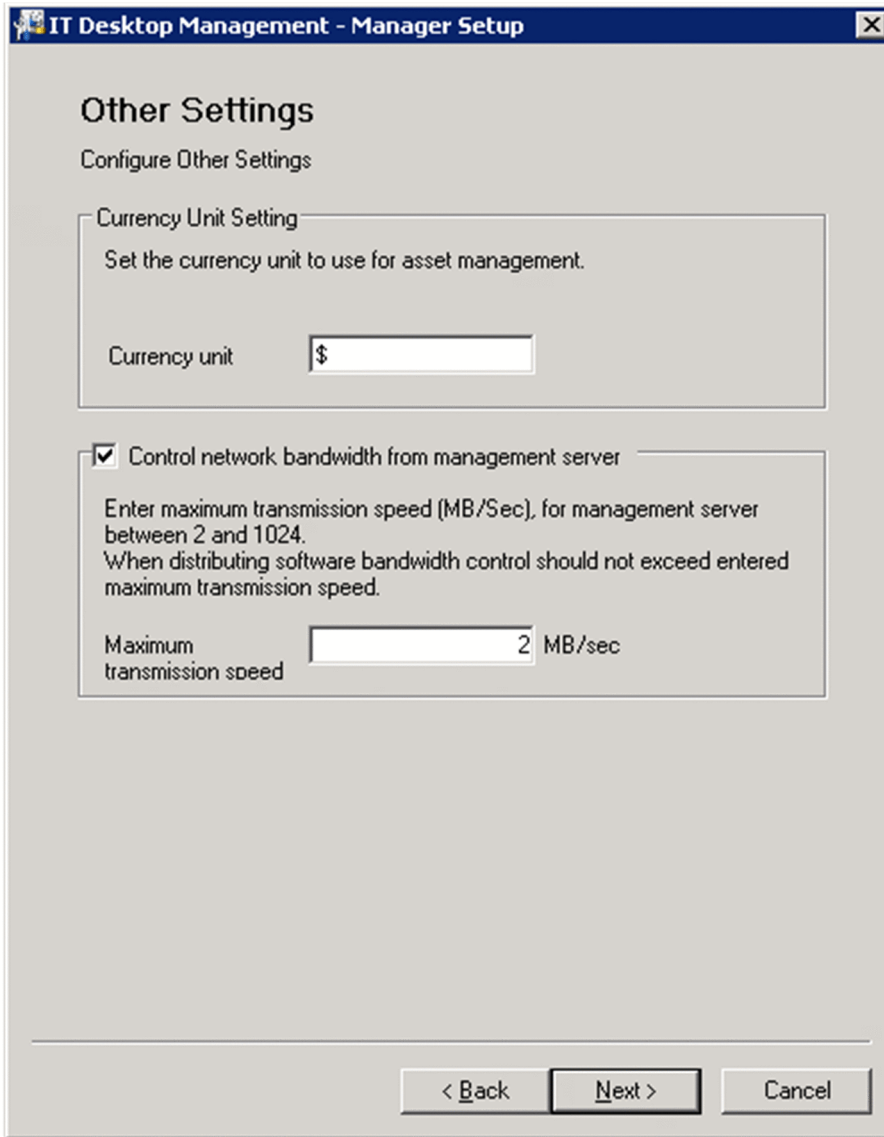
3.7 Procedure for controlling the network bandwidth used for distribution

You can control the network bandwidth from a management server or a site server by setting the maximum transfer speed so that the entire network bandwidth is not used when software or files are distributed to managed computers.

To control the network in a multi-server configuration system, use the procedure on the database server. Then select **Settings Modification** on a management server to perform setup. It is not necessary to change the management server setup settings.

To control a network bandwidth:

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 - Manager, Tools**, and then **Setup**, or **All Programs, JP1_IT Desktop Management - Remote Site Server**, 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.
The follow shows a screenshot of a management server.



6. Select **Control network bandwidth from management server** or **Control network bandwidth from the site 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.
Setup starts, and a dialog box indicating the progress opens. When setup finishes, the **Setup Complete** view appears. 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.
8. In the **Setup Complete** view, click the **OK** button.

You can now control the network bandwidth.

3.8 Procedure for changing the currency unit

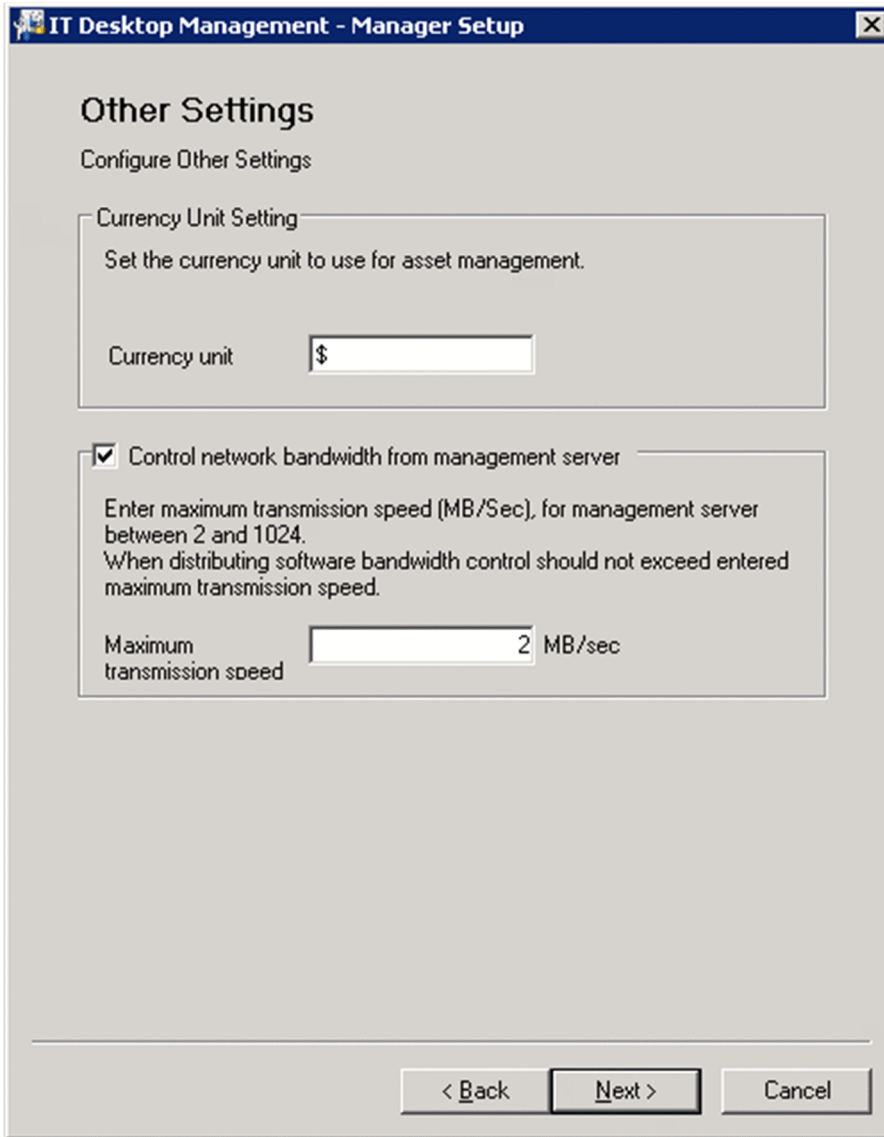
This is a management server setup item.

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

To change the currency unit in a multi-server configuration system, use the following procedure on the database server. Then select **Settings Modification** on the management server and perform setup. It is not necessary to change the management server setup settings.

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 - Manager, Tools**, and then **Setup**.
3. In the Setup window, click the **Next** button.
4. In the **Select a Setup** view, select **Settings Modification**, and then click the **Next** button.
5. Continue to click the **Next** button until the **Other Settings** view opens.



6. In the **Currency Unit Setting** section, enter a value in **Currency Unit**, and then click the **Next** button.

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

Setup starts, and a dialog box indicating the progress opens. When 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.

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

The currency unit is changed.

3.9 Procedure for upgrading a database

This is a management server setup item.

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

In a multi-server configuration system, start setup on the database server.

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 - 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** 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, site server programs, and network access control agents. Registering these programs on the management server allows you to distribute an agent and install a site server program, or to install a network access control agent from the operation window.

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.

3.10 Procedure for initializing a database

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

In a multi-server configuration system, start setup on the database server.

To initialize 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 - Manager, Tools**, and then **Setup**, or **All Programs, JP1_IT Desktop Management - Remote Site Server**, 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.

For a site server, settings related to component registration are not displayed.

Components include agents, site server programs, and network access control agents. Registering these programs on the management server allows you to distribute an agent and install a site server program, or to install a network access control agent from the operation window.

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.

If you want to initialize a database from the management server in a site-server configuration system, first initialize the database, and then perform the following operation on the site server:

Reporting the index information for operation logs

On each site server in a system, execute the `recreatelogdb` command with the `-node` argument specified.

Related Topics:

- [8.6 recreatelogdb \(recreating an operation log index on the site server\)](#)

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 basic 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 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 computers, or use flow control on only selected computers, add agent configurations.

To add agent configurations:

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

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

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

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 recommends that you install the agent on managed computers for better security management.

4.3 Settings for building site server configuration systems

4.3.1 Managing server configurations

There are two types of servers for JP1/IT Desktop Management server: a management server and a site server. A site server is used for relaying package distribution and storing operation logs to balance the load on management servers and the network. To use a site server, define a site server group in the **Server Configuration Settings** view in the Settings module, and specify the group as a relay point for package distribution in each network segment or as an operation log backup location.

The following sections describe how to specify server configurations and how to manage site server groups.

4.3.2 Specifying server configurations

Specify a package distribution relay point and operation log backup location for each network segment. Management servers are specified for all network segments by default.

Tip

A package distribution relay point and operation log backup location are specified for each site server group. Therefore, adding the necessary site server groups before specifying server configurations makes operation easy.

To specify settings for server configurations:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.
3. In the information area, select **Server Configuration Settings**, and then click the **Edit** button of the network segment for which you want to specify server configurations.
4. In the displayed dialog box, select the corresponding site server group (or management server) for each item, and then click **OK**.

Package distribution relay points and operation log backup locations for the selected network segments are specified and displayed in the list.

4.3.3 Adding site server groups

Select multiple site servers in the system, and define them as a group.

Specify a package distribution relay point or operation log backup location for each site server group. You can either define a single site server as a group or group multiple site servers into one group. You can set connection priorities for each site server in a group.

Tip

If you use a site server as an operation log backup location, we recommend that you specify a single site server for the site server group specified for each network segment. This makes it easy to manage operation logs because the operation logs of a single computer are collected in a single site server.

To add site server groups:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.
3. In the information area, select **Site Server Group Settings**, and then click the **Add** button.
4. In the displayed dialog box, type information about site server groups, and then click **OK**.

Site server groups are added and displayed in the list.

4.3.4 Editing site server group information

You can edit the registered site server group information.

To edit the site server group information:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.
3. In the information area, select **Site Server Group Settings**, and then click the **Edit** button of the site server group you want to edit.
4. In the displayed dialog box, edit the site server group information, and then click **OK**.

The site server group information is updated.

4.3.5 Removing site server groups

You can remove the unnecessary site server groups.

Tip

You cannot remove a site server group specified as a package distribution relay point or operation log backup location for each network segment.

To remove site server groups:

1. Display the Settings module.
2. In the menu area, select **Server Configuration** and then **Server Configuration Settings**.

3. In the information area, select **Site Server Group Settings**, and then click the **Remove** button of the site server groups you want to remove.

The site server groups are removed.

4.4 Settings for building a support service linkage configuration system

4.4.1 Setting information for connecting to the support service

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

Connecting to the support service site automatically updates the information about update programs to the latest.

Obtaining the latest information from the support service site allows the security policy to judge whether the latest update program is applied to the managed computers.

Important note

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

To set information for connecting to the support service:

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

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

Tip

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

Tip

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

Related Topics:

- [8.3 updatesupportinfo](#) (uploading support service information)

4.5 Settings for building Active Directory linkage configuration systems

4.5.1 Setting information for connecting to Active Directory

To specify devices registered on Active Directory as a management target of JP1/IT Desktop Management or import department hierarchy information, you must set the domain information of Active Directory to be searched.

To set information for connecting to Active directory:

1. Display the Settings module.
2. In the menu area, select **General** and then **Active Directory**.
3. To obtain group hierarchy information from Active Directory, in the information area, select **Get Department Hierarchy Information**.
4. Specify the information about Active Directory to be connected
To set multiple Active Directory information items, click the **Add** button, and then add information.
5. Click the **Test** button to check if a connection to Active Directory can be established.
6. If no problems have been found in the connection, click the **Apply** button.

When the search for Active Directory is started, the Active Directory information specified here is collected.

If the agent is simultaneously delivered while Active Directory is being searched, the credentials specified in this view are used.

Related Topics:

- [4.5.4 Specifying search conditions \(searching Active Directory\)](#)

4.5.2 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.

4.5.3 Searching for devices registered in Active Directory

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

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

To search for devices registered in Active Directory:

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

The search is performed according to the set search schedule.

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

Tip

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

Related Topics:

- [4.5.4 Specifying search conditions \(searching Active Directory\)](#)
- [1.7.3 Checking the device discovery status](#)

4.5.4 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 after the completion of device discovery, specify the recipients.
If you have not set the mail server (SMTP server) information to be used by JP1/IT Desktop Management, click the **SMTP Server** link and set the mail server information in the window that appears.

Important note

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

Settings for the search conditions are completed.

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

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

Related Topics:

- [1.7.3 Checking the device discovery status](#)

4.5.5 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.

4.6 Settings for building MDM linkage configuration systems

4.6.1 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, you must specify information for connecting to the MDM system and the schedule for obtaining the smart device information.

Important note

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

To set information for linking with an MDM system:

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

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

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

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

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

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

10. Click **OK**.

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

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

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

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

Tip

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

Tip

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

Related Topics:

- [1.7.5 Checking the discovered devices](#)
- [1.7.6 Checking the managed devices](#)

4.7 Settings for building network monitoring configuration systems

4.7.1 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.

4.7.2 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.

4.7.3 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.

4.7.4 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.

4.7.5 Enabling the JP1/NETM/NM - Manager linkage settings

If JP1/NETM/NM - Manager linkage is enabled, you can use JP1/IT Desktop Management to control network connections to the network segments that are managed by JP1/NETM/NM - Manager.

To enable the JP1/NETM/NM - Manager linkage settings:

1. Display the Settings module.
2. In the menu area, select **Network Access Control** and then **Network Access Control Settings**.
3. In the information area, in **JP1/NETM/NM - Manager Link Settings**, click **Edit**.
4. In the dialog box that appears, if **Continue the operation** appears, check the message that appears, and then select **Continue the operation**.
5. Select **Link with JP1/NETM/NM - Manager**.
6. Click **OK**.

The JP1/NETM/NM - Manager linkage settings are enabled.

4.7.6 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. 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 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.

4.7.7 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.

For how to set up JP1/NETM/NM - Manager, see the description of operations in the following manual: the *Job Management Partner 1 Version 9 Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide* or the *Job Management Partner 1 Version 10 Job Management Partner 1/NETM/Network Monitor*.

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.

4.8 Settings for building JP1/IM linkage configuration systems

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

You can enable the functionality for linking with JP1/IM of JP1/IT Desktop Management 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-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 linkage with JP1/IM, delete the `JP1IM_EventOption=ON` line that you added to the configuration file or change the setting to `JP1IM_EventOption=OFF`, and then restart the JP1/IT Desktop Management service.

5

Overwrite-installing the product and updating the components

This chapter describes overwrite installation of JP1/IT Desktop Management - Manager and updating of the components (agent, site server program, and network monitor agent).

5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management - Manager

To perform an overwrite installation of JP1/IT Desktop Management - 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 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 - Manager, restart the OS regardless of whether installation was successful. If service `JP1_ITDM_Service` does not start or JP1/IT Desktop Management - 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_ITDM_Service`).
3. Perform overwrite installation again. (The service you stopped will start.)

To perform an overwrite installation of JP1/IT Desktop Management - 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 - 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 - 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 in a single-server configuration](#)

5.2 Procedure for performing an overwrite installation of an agent from the supplied media

To perform an overwrite installation of an agent, you must use a version that is not earlier than the currently installed version. In addition, you must log on to the OS as a user with administrator permissions.

Important 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 an agent:

1. Insert the supplied media in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JPI/IT Desktop Management - Agent**, 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 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 site server program from the supplied media

To perform an overwrite installation of a site server program, you must use a version that is not earlier than the currently installed version.

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 program might not run correctly even if you install it again later.

To perform an overwrite installation of a site server program:

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 - Remote Site Server**, 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 site server program is complete. If a message asking you to restart the computer appears, restart it.

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 - 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 system

There are two ways to upgrade the entire JP1/IT Desktop Management 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 - Manager by overwrite-installing a newer version of the program on the management server and the database server.
2. Update the following components:
 - The agent and the site server program on the computer on which the site server program is installed
 - 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
3. Upgrade the agent on computers on which the site server program or the network access control agent is not installed.

To update the system components by using the function that automatically updates programs registered on the management server:

Important note

To update a component automatically, make sure the site server is operating before attempting to upgrade the management server and database server.

1. Upgrade JP1/IT Desktop Management - Manager by overwrite-installing a newer version of the program on the management server and the database server.
2. Register agent, site server program, 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 - Manager has been upgraded, you must first upgrade the controller.

Tip

If the version of JP1/IT Desktop Management is 10-00 or later, linkage with the MDM system starts after the system's server certificate is validated. Therefore, if you update the version from 09-51 to 10-00 or later, specify the necessary settings as described in [4.6 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 Overview and System Design Guide*.

Related Topics:

- 5.6 Procedure for upgrading JP1/IT Desktop Management - Manager
- 5.7 Updating components

5.6 Procedure for upgrading JP1/IT Desktop Management - Manager

You can upgrade JP1/IT Desktop Management - 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 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 - 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 - 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 JP1/IT Desktop Management - Manager, 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, the network access control agent, and the site server program installed on the user's computer are updated automatically.

Tip

When the agent, the network access control agent, and the site server program are updated automatically, data is sent from the management server to each computer. About 30 megabytes of data is sent to each computer on which an agent is installed. Added to this, about four megabytes of data is sent to a computer on which both a network access control agent and an agent are installed, and about 120 megabytes of data is sent to a computer on which both a site server program and an agent are 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 - Manager is complete.

Tip

If the version of JP1/IT Desktop Management is 10-00 or later, linkage with the MDM system starts after the system's server certificate is validated. Therefore, if you update the version from 09-51 to 10-00 or later, specify the necessary settings as described in [4.6 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 Overview and System Design Guide*.

5.7 Updating components

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

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 - Manager, as in an entire system upgrade, if you set automatic updating of components during the overwrite installation of JP1/IT Desktop Management - Manager, new versions of the agent, site server program, 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 - 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 the distribution functionality:

You can update components by registering a package on the management server, and then 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 the timing due to network load. To not update components automatically, disable updating of programs registered on the management server.

If you upgrade multiple programs, including JP1/IT Desktop Management - Manager, as in an entire system upgrade, and you set components as a package during the overwrite installation of JP1/IT Desktop Management - Manager, new versions of the agent, site server program, 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 - 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-2642-7794_0950_JP1_IT Desktop Management - 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 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 system](#).

Updating the controller:

If the controller is updated when JP1/IT Desktop Management 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 Web browser is Internet Explorer 6.
- The proxy server Internet option is not set correctly in the environment to which you want to connect to JP1/IT Desktop Management 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, site server programs, and network access control 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 - Manager, you can set automatic component updating or package registration during an overwrite installation of JP1/IT Desktop Management - 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, the network access control agent, and the site server program are updated automatically, data is sent from the management server to each computer. About 30 megabytes of data is sent to a computer on which an agent is installed. Added to this, about four megabytes of data is sent to a computer on which both a network access control agent and an agent are installed, and about 120 megabytes of data is sent to a computer on which both a site server program and an agent are 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 - 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 of JP1/IT Desktop Management - Manager in a multi-server configuration system

To perform an overwrite installation of JP1/IT Desktop Management in a multi-server configuration system, perform an overwrite installation on the database server, and then perform an overwrite installation on the management server.

Tip

For details about the task for performing an overwrite installation of JP1/IT Desktop Management - Manager in an environment in which a database server and a management server are used in a cluster configuration, see [5.12 Overview of performing an overwrite installation in a cluster system in a multi-server configuration system](#).

To perform an overwrite installation of JP1/IT Desktop Management - Manager in a multi-server configuration system:

1. On the management server, execute the `stopservice` command.
The management server services stop.
2. Perform an overwrite installation of JP1/IT Desktop Management - Manager on the database server.
If you do not need to upgrade the database, you can skip step 3.
3. On the database server, perform the setup for upgrading the database.
4. On the management server, perform an overwrite installation of JP1/IT Desktop Management - Manager.

Overwrite installation of JP1/IT Desktop Management - Manager in a multi-server configuration system is complete.

Related Topics:

- [8.7 stopservice \(stopping services\)](#)
- [5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management - Manager](#)

5.10 Overview of upgrading JP1/IT Desktop Management - Manager in a multi-server configuration system

You can upgrade JP1/IT Desktop Management - Manager by performing an overwrite installation with a new version of the program on the management server or the database server.

To upgrade JP1/IT Desktop Management in a multi-server configuration system, perform an overwrite installation on the database server, and then perform an overwrite installation on the management server. The version of JP1/IT Desktop Management - Manager on the management server and the version on the database server must be the same.

To upgrade JP1/IT Desktop Management - Manager in a multi-server configuration system:

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. On the management server, execute the `stopservice` command.
 - The management server services stop.
3. On the database server, perform an overwrite installation of JP1/IT Desktop Management - Manager.
 - During installation, at least 2.4 gigabytes of free space is required on the hard disk.
 - If you do not want to upgrade the database, you can skip step 4.
4. Start setup on the database server to upgrade the database.

Tip

When the database upgrade is complete, you can delete the backup you created in step 1.

5. Perform an overwrite installation of JP1/IT Desktop Management - 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 JP1/IT Desktop Management - Manager, 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 an overwrite installation, the agent, site server program, and network access control agent installed on a user's computer are updated automatically.

Tip

When the agent, network access control agent, and site server program are updated automatically, data is sent from the management server to each computer. About 30 megabytes of data is sent to a computer on

which an agent is installed. Added to this, about four megabytes of data is sent to a computer on which both a network access control agent and an agent are installed, and about 120 megabytes of data is sent to a computer on which both a site server program and an agent are installed.

Upgrading JP1/IT Desktop Management - Manager is complete.

Tip

If the version of JP1/IT Desktop Management is 10-00 or later, linkage with the MDM system starts after the system's server certificate is validated. Therefore, if you update the version from 09-51 to 10-00 or later, specify the necessary settings as described in [4.6 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 Overview and System Design Guide*.

5.11 Overview of performing an overwrite installation in a cluster system in a single-server configuration system

To perform an overwrite installation of JP1/IT Desktop Management in a cluster system in a single-server configuration system, first perform an overwrite installation on the primary server, and then perform an overwrite installation on the standby server.

To perform an overwrite installation in a cluster system in a single-server configuration system:

1. Take the service resources of JP1/IT Desktop Management on the primary server offline.
For details about the service resources to be taken offline, see the JP1/IT Desktop Management service resources (generic services) row in the table listing the resources that must be registered in groups. You can find the table in [2.11.3 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 - 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 - 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.

Overwrite installation in a cluster system in a single-server configuration system is complete.

Related Topics:

- [5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management - Manager](#)

5.12 Overview of performing an overwrite installation in a cluster system in a multi-server configuration system

To perform an overwrite installation of JP1/IT Desktop Management in a cluster system in a multi-server configuration system, first perform an overwrite installation on the primary server of a database server, and then perform an overwrite installation on the standby server. Next, perform an overwrite installation on the primary server of the management server, and then perform an overwrite installation on the standby server.

To perform an overwrite installation in a cluster system in a multi-server configuration system:

1. Take JP1/IT Desktop Management service resources on the primary server of the management server offline.
For details about the service resources to be taken offline, see the JP1/IT Desktop Management service resources (generic services) row in the table listing the resources that must be registered in groups. You can find the table in [2.11.3 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 of the database server, take JP1/IT Desktop Management service resources offline.
For details about the service resources to be taken offline, see the JP1/IT Desktop Management service resources (generic services) row in the table listing the resources that must be registered in groups located in [2.11.3 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.
3. On the primary server of the database server, perform an overwrite installation of JP1/IT Desktop Management - Manager.
4. Start setup on the primary server of the database server to upgrade the database.
If you do not need to upgrade the database, you can skip this step.
5. Copy the file that is output when setup finishes on the primary server to the standby server.
6. Move the owner of the group resource on the database server to the standby server.
7. On the standby server of the database server, perform an overwrite installation of JP1/IT Desktop Management - Manager.
8. Start setup on the standby server of the database server to upgrade the database.
If you do not need to upgrade the database, you can skip this step.
9. Move the owner of the group resource on the database server to the primary server.
10. On the database server, bring online the service resource you took offline in step 2.
11. On the primary server of the management server, perform an overwrite installation of JP1/IT Desktop Management.
12. On the standby server of the management server, perform an overwrite installation of JP1/IT Desktop Management.
13. On the management server, bring online the service resources you took offline in step 1.

Overwrite installation in a cluster system in a multi-server configuration is complete.

Related Topics:

- [5.1 Procedure for performing an overwrite installation of JP1/IT Desktop Management - Manager](#)

6

Uninstalling products

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

6.1 Overview of uninstalling the entire system

1. When a site server is installed, uninstall the site server program on the site server. If you are monitoring connection of devices to the network, disable network access control for each network segment. The order in which these operations are performed presents no problem.
2. Uninstall the agent on a computer on which an agent is installed.
3. On the management server, uninstall JP1/IT Desktop Management - 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.

Tip

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

Related Topics:

- [6.4 Procedure for uninstalling the site server program](#)
- [6.5 Disabling the network monitor](#)
- [6.3 Procedure for uninstalling the agent](#)
- [6.2 Procedure for uninstalling JP1/IT Desktop Management - Manager](#)
- [6.6 Uninstalling a controller](#)

6.2 Procedure for uninstalling JP1/IT Desktop Management - Manager

If you want to reinstall JP1/IT Desktop Management - Manager, or want to change the management server, uninstall JP1/IT Desktop Management - 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 - Manager, restart the OS regardless of whether installation was successful.

To uninstall JP1/IT Desktop Management - Manager:

1. In Windows Control Panel, start **Programs and Features**.
2. Select JP1/IT Desktop Management - **Manager**, and then click the **Change** button.
3. In the wizard for installing JP1/IT Desktop Management - 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 - Manager is uninstalled.

Tip

When you uninstall JP1/IT Desktop Management - 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 any more.

Related Topics:

- [6.6 Uninstalling a controller](#)
- [6.7 Procedure for uninstalling JP1/IT Desktop Management - Manager in a cluster system in a single-server configuration system](#)

6.3 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. 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 - **Agent**, and then click the **Uninstall** button.
3. In the confirmation dialog box for uninstallation, click the **Yes** button.

The JP1/IT Desktop Management agent is uninstalled.

Delete the device information on computers that are no longer managed by JP1/IT Desktop Management 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.

6.4 Procedure for uninstalling the site server program

When you want to re-install the site server program, or change the site server, uninstall the site server program.

Important note

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





Important note

Before you can uninstall the site server program in the Device module, the component (site server program) must be registered on the management server.



Tip

Uninstalling the site server program does not delete operation log data. If the data is no longer needed, delete the data manually from the folder that is specified in **Operation log data folder** during site server setup.

To uninstall the site server program:

1. Open the Device module.
2. In the menu area, select a device list from **Device Information** to display the site server you want to uninstall in the information area.
3. In the information area, select one applicable site server.
A site server is a computer for which   or   is displayed for the management type.
4. From **Actions**, select **Uninstall Site Server Program**.
5. In the **Uninstall Site Server Program** dialog box, click the **OK** button.

The site server program on the computer you selected is uninstalled.

When the site server program is uninstalled, the management type icons return to  or  .

Tip




In an environment in which a site server cannot connect to a management server, you can uninstall the site server program on the computer by selecting Windows **Control Panel, Programs and Features**, and then **JPI/IT Desktop Management - Remote Site Server**. However, if you uninstall the site server program by using this method, you must perform the uninstallation procedure in the operation window to change information (the management type of the applicable computer) on the management server.

6.5 Disabling the network monitor

Disable the network monitor if the network monitoring of a specific network segment is not needed or if you want to stop monitoring a network.

To disable the network monitor:

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


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

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

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

Tip

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

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

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

Important note

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

Important note

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

Tip

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

Tip

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

Tip

If a computer has the network monitor agent installed and cannot connect to the management server, you can disable the network monitor by selecting and deleting **JP1/IT Desktop Management - Network Monitor** from **Programs and Features** in the Windows Control Panel on the computer. If you want to disable the network monitor in this way, you must follow the instructions in the operations window for disabling it, and then change the information on the management server (that is, the management type of the target computer).

Related Topics:

- [2.8.2 Enabling the network monitor](#)

6.6 Uninstalling a controller

Uninstall the controllers from the computers that you no longer need to perform remote control with.

To uninstall a controller:

1. In Windows control panel, start **Programs and Features**.
2. Select JP1/IT Desktop Management - RC Manager, and then click the **Uninstall** button.
3. In the displayed dialog box, click the **Yes** button.

The controller is uninstalled.



Tip

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

6.7 Procedure for uninstalling JP1/IT Desktop Management - Manager in a cluster system in a single-server configuration system

If you want to uninstall JP1/IT Desktop Management - Manager in a cluster system in a single-server configuration system, uninstall it first on the primary server, and then uninstall it on the standby server.

To uninstall JP1/IT Desktop Management - Manager in a cluster system in a single-server configuration system:

1. Take the service resources of JP1/IT Desktop Management - Manager on the primary server offline.
For details about the service resources to be taken offline, see the JP1/IT Desktop Management service resource (generic service) row of the table listing the resources that must be registered in groups. You can find the table in [2.11.3 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 - Manager.
3. Move the owner of the group resource to the standby server.
4. On the standby server, uninstall JP1/IT Desktop Management.

Uninstallation in the cluster system in the single-server configuration system is complete.

Related Topics:

- [6.2 Procedure for uninstalling JP1/IT Desktop Management - Manager](#)

6.8 Procedure for uninstalling JP1/IT Desktop Management - Manager in a cluster system in a multi-server configuration system

If you want to uninstall JP1/IT Desktop Management - Manager in a cluster system in a multi-server configuration system on the management server, uninstall it on the primary server first, and then uninstall it on the standby server. Next, on the database server, uninstall it on the primary server and then on the standby server.

To uninstall JP1/IT Desktop Management - Manager in a cluster system of a multi-server configuration system:

1. Take the JP1/IT Desktop Management service resources on the primary server of the management server offline.
For details about service resources to be taken offline, see the JP1/IT Desktop Management service resource (generic service) row of the table listing the resources that must be registered in groups. You can find the table in [2.11.3 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 of the management server, uninstall JP1/IT Desktop Management - Manager.
3. Move the owner of the group resource to the standby server.
4. On the standby server of the management server, uninstall JP1/IT Desktop Management - Manager.
5. Take the JP1/IT Desktop Management service resources on the primary server of the database server offline.
For details about the service resources to be taken offline, see the JP1/IT Desktop Management service resource (generic service) row of the table listing the resources that must be registered in groups. You can find the table in [2.11.3 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.
6. On the primary server of the database server, uninstall JP1/IT Desktop Management - Manager.
7. Move the owner of the group resource to the standby server of the management server.
8. On the standby server of the database server, uninstall JP1/IT Desktop Management - Manager.

Uninstallation in the cluster system of the multi-server configuration system is complete.

Related Topics:

- [6.2 Procedure for uninstalling JP1/IT Desktop Management - Manager](#)

7

Migrating environments

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

7.1 Procedure for replacing a management server in a single-server configuration system

Replacement of a management server means to use a computer on which JP1/IT Desktop Management - Manager is not installed as the new management server.

Important note

The version information of JP1/IT Desktop Management - 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 - Manager while replacing a management server. Accordingly, install the upgrade before or after replacement.

Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

- 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 - 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 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_ITDM_Agent Control
- JP1_ITDM_Service
- JP1_ITDM_Web Container

2. Back up the database.

On the old computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Database Manager**. Start Database Manager for JP1/IT Desktop Management - 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 automatic backup of operation log data is enabled, the backup data is saved in the operations log backup folder that was specified during setup.

To check whether automatic backup is enabled, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup** to start setup for JP1/IT Desktop Management - Manager. In the **Automatic Backup Setting for Operation Logs** view, make sure **Backup Operation logs automatically** is selected. If this item is selected, automatic backup is enabled.

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 - Manager.

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

On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup** to start setup for JP1/IT Desktop Management - Manager, and then perform setup. If you want to enable automatic backup of the operation log, specify the folder in which you stored the backup data in step 4 as the operations log backup folder in the **Automatic Backup Setting for Operation Logs** view.

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 - Manager, Tools**, and then **Database Manager**. Start Database Manager for JP1/IT Desktop Management - Manager, and restore the database.

9. Register the license.

In the Login window of JP1/IT Desktop Management - 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 - Manager that you installed on the new computer. In **Agent Basic Settings** 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. Change the connection destination of the site server.

In the **Server Configuration Settings** view of the Settings module, change the **Management Server** value to the new management server.

12. Make sure that the system operates correctly.

In the JP1/IT Desktop Management - 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 - 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.

13. On the old computer, uninstall JP1/IT Desktop Management - 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 - 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 - Manager](#)
- [1.2.3 Procedure for setting up a management server in a single-server configuration](#)
- [2.11.1 Overview of building a cluster system in a single-server configuration system](#)

7.2 Procedure for replacing a management server in a multi-server configuration system

Replacement of a management server means to use a computer that has not been built as a management server as the new management server.

Important note

The version information of JP1/IT Desktop Management - 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 - Manager while replacing a management server. Accordingly, install the upgrade before or after replacement.

The procedure here describes how to replace a management server. You replace the server by installing JP1/IT Desktop Management - Manager on the new computer and then changing the connection destination of the agent.

To replace a management server:

1. On the management server, stop the JP1/IT Desktop Management - Manager services.
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_ITDM_Agent Control
 - JP1_ITDM_Service
 - JP1_ITDM_Web Container
2. Disconnect the old computer from the network.
3. Install JP1/IT Desktop Management - Manager on the new computer.
4. Set up JP1/IT Desktop Management - Manager as a management server.
On the new computer, from the Windows **Start** menu, select **All Programs**, **JP1_IT Desktop Management - Manager**, **Tools**, and then **Setup**. Start setup for JP1/IT Desktop Management - Manager and perform setup.
5. Register the license.
In the Login window of JP1/IT Desktop Management - Manager installed on the new computer, click the **License** button. In the dialog box that opens, click the **Register License** button to register the license.
6. Change the connection destination of the agent.
Log in to JP1/IT Desktop Management - Manager that you installed on the new computer. In **Agent Basic Settings** in agent setup, select **Basic Settings** and then **Server Name**, and then enter the IP address or 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.
7. Change the connection destination of the site server.

In the **Server Configuration Settings** view of the Settings module, change the setting in **Server Name** to the management server that will be used after migration.

8. Make sure the management server runs correctly.

In JP1/IT Desktop Management - 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** view of the Device module, make sure **Last Alive Confirmation Date/Time** has been updated.

By default, **Last Alive Confirmation Date/Time** is not displayed. To display it, right-click an item in the **Device List** view, such as a host name, and then select **Last Alive Confirmation Date/Time** in the dialog box that opens by selecting **Select Columns**.

If **Last Alive Confirmation Date/Time** has not been updated, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Agent, Administrator Tool**, and then **Setup** on the user's computer. Next, start setup for the agent, and make sure that the new management server is set as the connection destination.

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

Replacement of the management server is complete.

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 migration 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 a 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

If you connect the old management server to a network without uninstalling JP1/IT Desktop Management - 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 - Manager](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)
- [2.11.2 Overview of building a cluster system in a multi-server configuration system](#)

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 site servers

Replacement of a site server means to migrate the site server functionality of a computer on which the site server program is currently installed to another computer. On the new computer, you must build a new site server, and migrate operation log data from the old site server.

Important note

The first four digits of the version information for the site server program that will be installed on the new computer and the first four digits of the version information for the program installed on the old computer must match. For example, if the product version is 09-50-01, the *09-50* portion must match.

Important note

You cannot upgrade the site server program during replacement of the site server. Accordingly, install the update before or after replacement.

To replace a site server:

1. On the old site server, stop the site server service (JP1_ITDM_Remote Site Service).

2. On the new computer, manually copy the operation log data from the old site server.

Copy the data so that the folder structure under the operation log data folder will be the same on both the old and new site servers. The operation log data folder is a folder specified in **Operation log data folder** during setup of each site server.

Tip

The larger the amount of operation log data to be copied in this step, the longer it takes to re-create index information that is performed in step 6. We recommend that you copy only necessary data.

Tip

It is not necessary to manually copy the data used for distribution functionality relay. The data is downloaded automatically from the management server.

3. Install the agent on the new computer.

4. Install the site server program on the new computer, and perform the setup.

5. On the new site server, stop the site server service (JP1_ITDM_Remote Site Service).

6. On the new site server, use the `recreatelogdb` command to re-create index information of the operation log data.

Specify `-all` as the command argument.

7. On the new site server, start the site server service (JP1_ITDM_Remote Site Service).

8. In the operation window, change the server configuration.

In the Settings module, select **Server Configuration**, **Server Configuration Settings**, and then **Site Server Group Settings**. From the site server group that contains the old site server, delete the old site server, and then add the new site server and adjust the priority in the **Edit Site Server Group** dialog box that you open by clicking the **Edit** button.

Tip

If the new site server is not displayed in the **Edit Site Server Group** dialog box, confirm that the computer that will be used as that server is connected to the network, and then wait a while.

9. Uninstall the site server program from the old site server.

Because the operation log data is not deleted, delete it manually from the operation log data folder.

Replacement of the site server is complete.

Important note

When the `recreatelogdb` command finishes and the site server starts, creation of the index information of the operation log data begins. Because the site server is loaded while the index information is being created, it might take a few days to complete the index, depending on the amount of operation log data. Also, operation log data that is generated while the index is being created cannot be checked until the creation of the index information has been completed. Execute the `recreatelogdb` command after taking these issues into consideration.

Related Topics:

- [2.3.2 Procedure for installing the site server program](#)
- [2.3.5 Procedure for setting up a site server](#)
- [4.3.1 Managing server configurations](#)
- [8.6 recreatelogdb \(recreating an operation log index on the site server\)](#)

7.5 Procedure for connecting a site server to another management server

This section describes the necessary operations for the following conditions that can occur after systems are integrated or the administration scope changes.

- You want to change the connection destination of a site server used in a system to a management server in another system.
- You want to change the connection destination of a site server used in a system to a newly built management server[#].

[#]: Does not include new management servers resulting from replacement (a database is restored by using backup data from the management server in the old system).

Some steps vary depending on whether the operation log data stored on a site server is inherited by the destination system during migration or deleted in order to use the site server as a new site server.

To connect a site server to another management server:

1. Change the connection destination of the applicable site server.

You can change the connection destination of the site server by using agent setup. From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Agent, Administrator Tools**, and then **Setup**. In **Connected managing server** of the Setup window that opens, change the IP address of the management server.

Tip

If a password is set for the agent, a dialog box asking for the password opens when agent setup starts.

Tip

If you want to change the connection destination of many site servers, you can add the settings of agents whose destination management server you have changed, and then assign the settings to the applicable computers.

Proceed to step 3 if you do not want to pass the operation log data to the destination computer.

2. If you want to pass the stored operation log data to the destination computer, report the index information for the operation log data to the management server.

On the applicable site server, execute the `recreatelogdb` command with the `-node` argument specified.

In this case, proceed to step 4 after executing the command.

Tip

If the command could not be executed, re-execute it after the period of time set in **Server Connection Interval** of the agent setup elapses (30 minutes is the default setting).

3. If you do not want to pass the operation log data, initialize the database on the site server to delete the data.

From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Remote Site Server**, and then **Setup**. In the Setup dialog box that opens, select **Database Re-creation** to perform the operation. In the dialog box indicating the setup is complete, clear **Store operation log data in the database of the re-created server**.

Also, delete all files and folders under *operation-log-data-folder*.

The folder indicated by *operation-log-data-folder* is the folder specified in **Operation log data folder** during site server setup.

4. Stop the site server service, and delete all data stored for distribution.

On the applicable site server, stop the site server service (JP1_ITDM_Remote Site Service).

In addition, delete all files and folders under the following folder, and then start the site server service:

data-folder\AGC\CDS

The folder indicated by *data-folder* is the folder specified in **Data folder** during site server setup.

5. On the destination system, change the server configuration.

In the Settings module (select **Server Configuration** and then **Server Configuration Settings**), change site server group settings or server configuration settings as needed for the environment. If necessary, change these settings in the source system.

Tip

If the site server whose connection destination you changed is not displayed in the **Edit Site Server Group** dialog box in the destination system, confirm that the computer that is used as that server is connected to the network, and then wait a while.

The connection destination of the site server is changed, and you can use the site server in the destination system.

Related Topics:

- [1.6.10 Procedure for setting up the agent](#)
- [8.6 recreatelogdb \(recreating an operation log index on the site server\)](#)
- [3.10 Procedure for initializing a database](#)
- [4.3.1 Managing server configurations](#)

7.6 Procedure for migrating from a single-server configuration system to a multi-server configuration system

To migrate a management server built in a single-server configuration system to a multi-server configuration system, build a new multi-server configuration system, and then migrate data in the source environment to a database server.

Important note

The version of JP1/IT Desktop Management - Manager to be installed on the destination computer and the version on the source computer must match.

Important note

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

Important note

The operation logs on a management server will no longer be accessible after migration to a multi-server configuration system. However, the operation logs on a site server will be accessible after migration to a multi-server configuration system.

Important note

On a computer that runs Windows 8, do not specify the following folders during installation:

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

To migrate a management server from a single-server configuration system to a multi-server configuration system:

1. Stop the JP1/IT Desktop Management services.

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_ITDM_Service
- JP1_ITDM_Agent Control
- JP1_ITDM_Web Container

2. Back up the database.

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

3. If you migrate the environment to a different computer, disconnect the source computer from the network.

4. If you are using the same computer before and after migration, uninstall JP1/IT Desktop Management - Manager on the computer before migration.

5. Build a database server.

Perform a custom installation of JP1/IT Desktop Management - Manager on the computer that will be used as the database server. After installation, start setup. In the **Server Configuration Settings** view, select **Multi-server configuration**, **Database server** and **16GB**.

Also, set sharing in the **Folder Settings** view, and then specify the folder that can be accessed from a management server in **Data folder**.

6. During database server setup, set the folder specified in **Data folder** as a shared folder that can be accessed from the management server.

7. Build a management server.

On the computer that will be used as the management server, perform a custom installation of JP1/IT Desktop Management - Manager. After installation, start setup. In the **Server Configuration Settings** view, select **Multi-server configuration** and then **Management Server**.

Also, in the **Settings for the Data Folder Shared Between** view, specify the folder you specified as a shared folder in step 6 in **Data folder shared between servers**.

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

Use Database Manager to restore the database.

9. Register the JP1/IT Desktop Management product license.

10. Change the connection destination of the agent.

Log in to JP1/IT Desktop Management - Manager. In **Agent Basic Settings** in agent setup, select **Basic Settings** and then **Management Server** to set the IP address or 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. Change the connection destination of the site server.

In the **Server Configuration Settings** view of the Settings module, change the value in **Management Server** to the management server that will be used after migration.

12. If necessary, change the network access control settings.

In the **Network Access Control Settings** view of the Settings module, delete the IP address of the management server used before migration from **Exclusive Communication Destination for Access-Denied Devices**, and then add the IP address of the management server that will be used after migration.

13. If necessary, change the IP discovery settings.

In the **Configurations** view of the Settings module, select **IP Address Range** and then **Search Node Locations** to change the management server segment setting to the management server network segment that will be used after replacement.

14. Set the storage location for the operation logs.

To manage operation logs, in the **Server Configuration Settings** view of the Settings module, select **Server Configuration Settings** and then **Storage Location for Operation Logs** and change the storage location from the management server to a site server group. The reason for this change is that management servers cannot be specified as the storage location for operation logs in a multi-server configuration system.

15. If the same computer will not be used before and after migration, uninstall JP1/IT Desktop Management - Manager on the computer used before migration.

16. Delete the backup you created in step 2.

Migration from a single-server configuration system to a multi-server configuration system is complete.

Tip

If necessary, delete the backup data you obtained from the source computer after the replacement finishes.

Tip

After the replacement finishes, you can check whether the agent is connected to the management server in the **Device List** view of the Settings 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 migration 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 devices as managed devices.

Important note

If you connect the old management server to a network without uninstalling JP1/IT Desktop Management - 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 - Manager](#)
- [6.2 Procedure for uninstalling JP1/IT Desktop Management - Manager](#)
- [2.4.2 Procedure for setting up a database server](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)
- [2.11.2 Overview of building a cluster system in a multi-server configuration system](#)

7.7 Procedure for migrating JP1/IT Desktop Management 09-51 or earlier in a single-server configuration system to a multi-server configuration system

To migrate JP1/IT Desktop Management 09-51 or earlier in a single-server configuration system to a multi-server configuration system, first upgrade the management server in the single-server configuration system, and then migrate it to the multi-server configuration system.

To migrate JP1/IT Desktop Management 09-51 or earlier in a single-server configuration system to a multi-server configuration system:

1. Upgrade JP1/IT Desktop Management.
2. Perform the migration from the single-server configuration system to the multi-server configuration system.

Important note

The version of the management server and the version of the database server in a multi-server configuration system must match.

Migration of JP1/IT Desktop Management 09-51 or earlier in a single-server configuration to a multi-server configuration system is complete.

Caution applying to the migration procedure

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.

Related Topics:

- [5.6 Procedure for upgrading JP1/IT Desktop Management - Manager](#)
- [7.6 Procedure for migrating from a single-server configuration system to a multi-server configuration system](#)

7.8 Procedure for replacing database servers

Replacement of a database server means to use a computer not built as a database server as the database server.

Important note

The version information of JP1/IT Desktop Management - 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 - Manager while replacing a database server. Accordingly, install the upgrade before or after replacement.

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

To replace a database server:

1. On the database server, stop the JP1/IT Desktop Management - Manager services.
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. You can stop the following services:
 - JP1_ITDM_Agent Control
 - JP1_ITDM_Service
 - JP1_ITDM_Web Container
2. Back up the database.
On the old computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Database Manager**. Start Database Manager for JP1/IT Desktop Management - Manager and back up the database. Leave at least 20 gigabytes of free space on the drive containing the backup folder.
3. Disconnect the old computer from the network.
4. Install JP1/IT Desktop Management - Manager on the new computer.
5. Set up JP1/IT Desktop Management - Manager as a database server.
On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**. Start setup for JP1/IT Desktop Management - Manager and perform setup.
6. Set up the management server again.
On the management server, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**. Start setup for JP1/IT Desktop Management - Manager to set up the management server again.
7. On the management server, stop the JP1/IT Desktop Management - Manager services.
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_ITDM_Agent Control
 - JP1_ITDM_Service

- JP1_ITDM_Web Container
8. On the database server, restore the database you backed up in step 2.
On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Database Manager**. Start Database Manager for JP1/IT Desktop Management - Manager and restore the database.
9. On the management server, start the JP1/IT Desktop Management - Manager services.
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 **Start** to start the service. Start the following services:
- JP1_ITDM_Agent Control
 - JP1_ITDM_Service
 - JP1_ITDM_Web Container
10. On the old computer, uninstall JP1/IT Desktop Management - Manager.

Replacement of the database server is complete.

Tip

If necessary, delete the backup data on the replacement source 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.

Cautions applying to the migration procedure

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 before replacement after replacement, 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 in an environment after replacement, 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 devices as managed devices.

Related Topics:

- [1.2.2 Procedure for installing JP1/IT Desktop Management - Manager](#)
- [2.4.2 Procedure for setting up a database server](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)
- [2.11.2 Overview of building a cluster system in a multi-server configuration system](#)

7.9 Procedure for replacing a management server and a database server in a multi-server configuration system at one time

Replacement of a management server and a database server means to use computers not built as a management server or database server as a management server or database server when computers are replaced or for another reason.

Important note

The version information of JP1/IT Desktop Management - 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 - Manager while replacing a management server. Accordingly, install the upgrade before or after replacement.

The procedure here describes how to replace a management server and a database server at one time. You replace the servers by installing JP1/IT Desktop Management - Manager on the new computer and then migrating data and changing the connection destination of the agent and the site server.

To replace a management server and a database server at one time:

1. On a management server, stop the JP1/IT Desktop Management - Manager services.
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_ITDM_Agent Control
 - JP1_ITDM_Service
 - JP1_ITDM_Web Container
2. Back up the database.
On the old database server computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools, Database Manager**. Start Database Manager for JP1/IT Desktop Management - Manager to back up the database. Leave at least 20 gigabytes of free space on the drive containing the backup folder.
3. Disconnect the old management server and database server computers from the network.
4. On the new computer, install JP1/IT Desktop Management - Manager.
5. Set up JP1/IT Desktop Management - Manager as the database server.
On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**. Start setup for JP1/IT Desktop Management - Manager and perform setup.
6. Set up JP1/IT Desktop Management - Manager as the management server.
On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Setup**. Start setup for JP1/IT Desktop Management - Manager and perform setup.
7. On the management server, stop the JP1/IT Desktop Management - Manager service.
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 service:

- JP1_ITDM_Web Container
8. On the database server, restore the database you backed up in step 2.
On the new computer, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Manager, Tools**, and then **Database Manager**. Start Database Manager for JP1/IT Desktop Management - Manager and restore the database.
 9. On the new management server, start the JP1/IT Desktop Management - Manager service.
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 **Start** to start the service. Start the following service:
 - JP1_ITDM_Web Container
 10. Register the license.
In the Login window of JP1/IT Desktop Management - 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.
 11. Change the connection destination of the agent.
Log in to JP1/IT Desktop Management - Manager that you installed on the new computer. In **Agent Basic Settings** in agent setup, select **Basic Settings** and then **Management Server** to set the IP address or 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.
 12. Change the connection destination of the site server.
In the **Server Configuration Settings** view of the Settings module, change the value set in **Management Server** to the management server that will be used after replacement.
 13. Make sure the server operates correctly.
In JP1/IT Desktop Management - 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** view of the Device module, make sure **Last Alive Confirmation Date/Time** has been updated.
By default, **Last Alive Confirmation Date/Time** is not displayed. To display it, right-click an item in the **Device List** view, such as a host name, and select **Last Alive Confirmation Date/Time** in the dialog box that opens by selecting **Select Columns**.
If **Last Alive Confirmation Date/Time** has not been updated, from the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Agent, Administrator Tool**, and then **Setup** on the user's computer. Next, start setup for the agent and make sure that the new management server is set as the connection destination.
 14. On the old computer, uninstall JP1/IT Desktop Management - Manager.

Replacement of the management server and the database server is complete.

Tip

If necessary, delete the backup data on the old 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 migration procedure

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 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

If you want to manage devices that were managed before replacement after replacement, 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 in an environment after replacement, 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 the 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 devices as managed devices.

Important note

If you connect the old management server to a network without uninstalling JP1/IT Desktop Management - 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 - Manager](#)
- [2.4.3 Procedure for setting up a management server for a multi-server configuration system](#)
- [2.11.2 Overview of building a cluster system in a multi-server configuration system](#)

7.10 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 [6.5 Disabling the network monitor](#), and [2.8.2 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.

8

Commands used for building-related operations

This chapter describes JP1/IT Desktop Management commands that are used to build a system, change settings, and replace devices.

8.1 Executing commands

To execute JP1/IT Desktop Management commands, you can use either the dedicated command prompt (**JP1ITDM Utility Console**) or the Windows command prompt.

JP1ITDM Utility Console is useful when you execute commands on the management server or database server. **JP1ITDM Utility Console** allows you to skip specification of a storage folder for the command execution file when entering a command. By default, when **JP1ITDM Utility Console** starts, the storage folder used by the command is set to the current folder. You can also use the Windows command prompt to execute commands.

Execute commands other than the `getinv.vbs` command as a user who has administrator permissions. In Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, if User Account Control (UAC) is enabled, use a right-click to open **JP1ITDM Utility Console** or the Windows command prompt, and then select **Run as administrator**. Execute the `getinv.vbs` command as a user who has full control permissions over the folder in which the `getinv.vbs` command is stored.

To execute commands on the site server or an agent, use the Windows command prompt.

To execute commands on the management server or database server:

1. From the Windows **Start** menu, select **All programs, JP1_IT Desktop Management - Manager**, and then **Command**.
2. In the window that appears, enter the command that you want to execute.

The command is executed.

To execute commands on the site server or an agent:

1. Open the Windows command prompt.
2. In the window that appears, enter the command that you want to execute.

The command is executed.

Tip

JP1/IT Desktop Management commands can be run as a scheduled task by registering them as a Windows task.

When backing up, restoring, and reorganizing the database with commands, services on the management server and database server must be stopped. Make sure to check which day of the week or time of the day JP1/IT Desktop Management is not running when you register these commands as a Windows scheduled task.

Note

Do not perform the operations listed below on a management server, site server, or database server on which a command is executing. If you perform one of these operations while a command is executing, the command is forcibly terminated. Depending on the timing, the database and important data might be corrupted, the agent control service might be suspended, and the command might output incorrect return values.

- Pressing the **Ctrl + C** keys
- Closing either **JP1ITDM Utility Console** or the Windows command prompt
- Logging out of Windows

- Shutting down Windows

If you perform one of these operations while a command is executing, check the messages in the log file. If a message indicating that the command finished successfully does not appear, re-execute the command as necessary. If a message indicating that the agent control service was suspended appears, restart the agent control service.

Note that the above notes do not apply to the following commands:

- stopservice
- startservice
- getlogs
- getinstlogs
- addfwlist.bat
- resetnid.vbs
- getinv.vbs

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. Copy the downloaded data manually to the management server (in a single server configuration system) or to the database server (in a multi-server configuration system), and execute the command. The latest information will be uploaded to the management server.

Execute this command on the following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

Format

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

Argument

-i support-information-file-name

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

Storage location

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

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

Notes

- This command cannot be executed simultaneously with any of the following commands:
 - `exportdb`
 - `importdb`
 - `ioassetsfieldutil export`
 - `ioassetsfieldutil import`
 - `ioutils exportasset`
 - `ioutils exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils 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 when setup or database manager is running on the management server or database server

Return value

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

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	The specified file is invalid, or the file does not exist.
31	Another command is being executed.
37	The data folders shared among servers cannot be accessed due to the database server being stopped or a network failure.
38	The data folders shared among servers cannot be accessed due to invalid credentials.
51	You do not have the permissions to execute this command.
53	Services on either the management server or database server have not started.
54	The management server or database server has not been set up.
101	Failed to update all or some of the support information.
150	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to upload a support information file called `supportinfo.zip` in `C:\temp`, onto the management server.

```
updatesupportinfo -i C:\temp\supportinfo.zip
```

Related Topics:

- [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 following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

In a multi-server configuration system, execute the commands in the following order:

1. Execute the `stopservice` command on the management server. Alternatively, you can go to the Windows **Start** menu, and select **Administrative Tools** and then **Services** to stop the following services:
 - JP1_DTNAVI_WEBCON
 - JP1_DTNAVI_AGCTRL
 - JP1_DTNAVI_MGRSRV
2. Execute the `stopservice` command on the database server.
3. Execute the `exportdb` command on the database server.

Format

```
exportdb[ -f backup-folder][ -s]
```

Arguments

`-f backup-folder`

Specify the absolute path to the backup storage folder. Only the folders in local drive can be specified. The size of the backup file varies depending on the operational environment and how long JP1/IT Desktop Management has been used. Make sure to keep enough free space for the disk drive in which the backup folder resides. The amount of space required is greater than the sum of the size of the database folder and the data folders that are already taking up capacity.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 135 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If any characters other than above are used for the JP1/IT Desktop Management installation folder, always specify this argument. If this argument is not specified, the following folder is used for the backup folder.

- When this argument is specified:
folder-specified-in-argument\YYYYMMDDhhmmss

- When this argument is omitted:

JP1/IT Desktop Management-installation-folder\mgr\backup\YYYYMMDDhhmmss

Example:

If the command is executed on January 1, 2011 at 2:30:00:

JP1/IT Desktop Management-installation-folder\mgr\backup\20110101023000

-s

Specify this argument to stop management server services (`stopservice` command), exporting data backup (`exportdb` command), and start management of the server service (`startservice` command) automatically.

Storage location

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

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

Notes

- Execute this command in the following state:
 - In a single-server configuration system: When the management server is already set, and the server is stopped
 - In a multi-server configuration system: When the database server is completed, and the services on the management server and the database server are not running
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
 - `importdb`
 - `ioassetsfieldutil export`
 - `ioassetsfieldutil import`
 - `ioutils exportasset`
 - `ioutils exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils 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 or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

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

Return value	Description
0	The command finished normally.
1	The backup was exported successfully, but the automatic starting of the management server failed.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid or the folder does not exist.
31	Another command is being executed.
32	A backup storage folder that was created at the same time exists.
33	The disk does not have enough space.
34	Failed to start the database.
35 [#]	The management server or the database server was in a starting process when the command is executed.
36	The database was in a shutdown process when the command is executed.
51	You do not have the permissions to execute this command.
52	The argument <code>-s</code> is specified in a cluster environment or in a multi-server configuration system.
53	The management server has not stopped in a single-server configuration system. The management server or database server has not stopped in a multi-server configuration system.
54	The management server or database server has not been set up.
55	The default backup storage folder cannot be used.
61	Cannot connect to the backup folder for the operation logs.
62	Cannot log in to the backup folder for the operation logs.
63	The operation log-related folder does not have enough free space.
64	The backup of the operation log was interrupted due to some other error.
101	Failed to export backup data.
102	Failed to automatically stop the management server.
110	The command execution failed due to a problem with a license.
150	The command execution was interrupted due to some other error.

[#]: The value to be returned when argument `-s` is specified

Example

The following example shows use of this command to export backup data to `C:\tmp\backup`, stop the management server services, export data backup, and start the management server service automatically.

```
exportdb -f C:\tmp\backup -s
```

Related Topics:

- [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 following servers:

- In a single-server configuration system: Management server
- In a multi-server configuration system: Database server

In a multi-server configuration system, execute the commands in the following order:

1. Execute the `stopservice` command on the management server. Alternatively, you can go to the Windows **Start** menu and select **Administrative Tools** and then **Services**, to stop the following services:
 - JP1_DTNAVI_WEBCON
 - JP1_DTNAVI_AGCTRL
 - JP1_DTNAVI_MGRSRV
2. Execute the `stopservice` command on the database server.
3. Execute the `importdb` command on the database server.

Format

```
importdb [ -f data-storage-folder-name] [ -w work-folder-name] [ -s]
```

Argument

-f data-storage-folder-name

Specify the absolute path to the folder in which the backup file of the target restore point resides. Only a folder in a local drive can be specified.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If any characters other than above are used for the JP1/IT Desktop Management installation folder, always specify this argument.

The following data storage folders are used during command execution for restoring data, when this argument is specified or omitted.

When this argument is specified:

The data storage folder specified in the argument is used.

When this argument is omitted:

The most up-to-date data storage folder available under the path below is chosen by name.

JP1/IT Desktop Management-installation-folder\mgr\backup

For example, if the folder has three data storage folders, \20110101023000, \20110102023000, and \20110103023000, then \20110103023000 will be chosen to be used for restoring.

-w *work-folder-name*

Specify the absolute path to the work folder to be used for restoring to the backup point. Only the folders in a local drive can be specified. 10 GB or more is required for the drive where the work folder resides, in order to manage 10,000 devices.

To specify a path containing a space, enclose the strings with double quotation marks ("). Specify a folder name that is 150 bytes or fewer in length, and exclude the backslash (\) at the end of the folder name. Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), .(period), @, \

If characters other than above are used for the JP1/IT Desktop Management installation folder, always specify this argument. If the specified folder does not exist, an error is returned.

When this argument is omitted, the folder below is used as a work folder.

JP1/IT Desktop Management-installation-folder\mgr\temp

-s

Specify if you want to automatically run a set of commands for stopping the management server services (the `stopservice` command), restoring the database with a backup (the `importdb` command), and starting the management server services (the `startservice` command).

Storage location

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

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

Notes

- Execute this command in the following state:
 - In a single-server configuration system: When the management server setup is completed and the management server is not running
 - In a multi-server configuration system: When the database server is completed, and the services on the management server and the database server are not running
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
 - `exportdb`
 - `ioassetsfieldutil export`
 - `ioassetsfieldutil import`
 - `ioutils exportasset`
 - `ioutils exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils 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 or in a multi-server configuration system. If you specify this argument, the command fails.

Return value

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

Return value	Description
0	The command finished normally.
1	Restoration from a backup was successful, but a failure occurred with automatically starting the management server.
11	The format for specifying the command arguments is invalid.
12	The specified data storage folder is invalid, or the folder does not exist.
13	A backup file does not exist in the specified data storage folder.
14	The specified work folder is invalid, or the folder does not exist.
15	The disk does not have enough space.
31	Another command is being executed.
34	The starting of the database failed.
35 [#]	The management server or the database server was in a start process when the command is executed.
36	The database was in a shutdown process when the command was executed.
51	You do not have the permissions to execute this command.
52	The argument <code>-s</code> is specified in a cluster environment or in a multi-server configuration system.
53	The management server has not stopped in a single-server configuration system. The management server or database server has not stopped in a multi-server configuration system.
54	The management server or database server has not been set up.
55	The default data storage folder and the work folder are not usable.
56	A backup of an older version was specified.
61	Cannot connect to the backup folder for the operation logs.
62	Cannot log in to the backup folder for the operation logs.

Return value	Description
63	The operation log-related folder does not have enough free space.
64	The backup of the operation log was interrupted due to some other error.
101	A restoration using a backup failed.
102	Failed to automatically stop the management server.
110	Command execution failed due to a problem with the license.
150	Command execution was interrupted due to some other error.

#: The value to be returned when argument `-s` is specified

Example

The following example shows use of this command to stop the management server services, restore data using a backup acquired on January 3rd, 2011, 2:30:00 (in the backup data folder `C:\tmp\backup\20110103023000`), and start the management server services automatically.

```
importdb -f C:\tmp\backup\20110103023000 -s
```

Related Topics:

- [8.1 Executing commands](#)

8.6 recreatelogdb (recreating an operation log index on the site server)

This section describes the `recreatelogdb` command, which re-creates indexes to view the operation logs stored on the site server.

Functionality

This command re-creates indexes to be used for referring to the operation logs stored on the site server. It also reports the list of agent-operated logs managed by the site server up onto the management server.

Indexes are created on each site server and reported to the management server. When viewing the distributed operation logs from the operation window, the operation logs are searched through using the index information and thus the logs on the site server can be reached.

Operation logs stored on the site server cannot be viewed correctly if an inconsistency is introduced between the operation log data and the indexes on the site server due to the operation log data being manually added or removed, or if index information is corrupted due to a system failure. In such cases, you can use the `recreatelogdb` command. An operation log index will be re-created and the operation logs on the site server will be properly referred to.

Execute the `recreatelogdb` command in cases like the following:

- When operation log data is deleted from its own storage folder on the site server
- When backup data for the operation log is restored (added) to the site server
- When operation log data is copied or moved from an another site server
- When the operation log database on the site server is corrupted
- When the database on the management server is corrupted

This command must be executed on the site server.

Format

```
recreatelogdb{ -all| -add| -node}
```

Argument

-all

Re-creates indexes of the operation logs stored in the site server. Indexes are recreated after the command is completed, when the site server is started. Specify this argument to re-create indexes in such cases as when operation log data is moved or the database on the site server is corrupted.

If this command is executed with this argument when the site server is started, the server stops during command execution. The site server starts again when the command is completed. If this command is executed when the site server is stopped, the server remains stopped after the command is completed.

-add

Creates additional operation log indexes. Indexes are created after the command is completed, when the site server is started. Specify this argument when additional operation logs are added to the site server. For example, specify when operation log data is moved from another site server.

If the command is executed with this argument when the site server is started, the server stops during command execution. The site server starts again when the command is completed. If this command is executed when the site server is stopped, the server remains stopped after the command is completed.

-node

Reports the list of agent-operated logs managed by the site server up onto the management server. An index is not recreated. Specify this argument in the following cases:

- There is no defect in the database on the site server, but database on the management server is corrupted. The operation logs cannot be searched correctly.
- When the site server connection destination is changed to a management server in another system
- When the database is rebuilt (the `updatesupportinfo` command is executed) on the management server

Storage location

`site-server-installation-folder\mgr\bin\`

Notes

- When an argument other than `-node` is specified with the `recreatelogdb` command, the site server stops during command execution. Operation logs generated during the command execution cannot be viewed until the command is completed. Once the `recreatelogdb` command is completed, index creation begins when the site server starts. As the index creation process increases your server load, it might take a couple of days for the process to complete, depending on the size of the data. Operation logs generated during index creation cannot be viewed until index creation is completed. Keep these considerations in mind when executing the `recreatelogdb` command.
- If the job status recording file for the `deletelog` command (`deletelog_lasttime.txt`) exists in the work folder, the `recreatelogdb` command fails. In such a case, re-execute the `deletelog` command to complete deletion of the operation logs, and then execute the `recreatelogdb` command.
- If you moved operation logs to the data folder, and then re-created operation log indexes with the argument `-all` or `-add` specified, always execute the `recreatelogdb` command with the argument `-node`. By executing this command, a list of agent-operated logs is reported to the management server. If the logs are not reported to the server, a search through the operation logs might not be performed correctly.
- Execute this command when the site server setup is completed.
- This command cannot be simultaneously executed by multiple users.

Return value

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

Return value	Description
0	The command finished normally.
1	A warning was raised during command execution. The command stopped.
11	The specified format for the argument is incorrect.
31	Another command is being executed.
51	You do not have the permissions to execute this command.
54	The site server has not been set up.
58	Failed to connect to the management server.
62	A file access error occurred.
67	A job status recording file for the <code>deletelog</code> command exists.
101	Command execution failed because there is not enough memory, or due to some other reason.
102	Failed to automatically stop the site server.

Return value	Description
120	A database access error occurred.

Example

The following example shows use of this command to re-create indexes of the operation logs, in case the database on the site server has been corrupted.

```
recreatelogdb -all
```

Related Topics:

- [8.1 Executing commands](#)

8.7 stopservice (stopping services)

Functionality

This command stops the services associated with the management server or the database server to stop the management server or the database server.

Execute this command on the management server in a single-server configuration system.

In a multi-server configuration system, execute the commands in the order below. It might take some time before the service stops, or an error might occur if the commands are executed in a wrong order.

1. Execute the `stopservice` command on the management server.
2. Execute the `stopservice` command on the database server.

Format

```
stopservice
```

Arguments

No arguments are available for this command.

Storage location

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

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

Notes

- Execute this command when the management server and the database server setup is completed.
- This command cannot be simultaneously executed by multiple users.
- This command cannot be executed simultaneously with any of the following commands:
 - `exportdb`
 - `importdb`
 - `ioassetsfieldutil export`
 - `ioassetsfieldutil import`
 - `ioutils exportasset`
 - `ioutils exportdevice`
 - `ioutils exportdevicedetail`
 - `ioutils exportfield`
 - `ioutils exportfilter`
 - `ioutils 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 or database server has already stopped.
31	Another command is being executed.
35	The management server or database server was in a startup process when the command is executed.
37	Failed to access to the data folder shared between servers. The database server was stopped, or a network failure has occurred.
38	Invalid credentials. The data folders shared between servers cannot be accessed.
51	You do not have the permissions to execute this command.
52	This command cannot be executed in a cluster environment.
54	The management server or database server has not been set up.
101	Failed to stop the services of the management server or database server.
150	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to stop services of the management server.

```
stopservice
```

Related Topics:

- [8.1 Executing commands](#)

8.8 getlogs (collecting troubleshooting information)

Functionality

This command collects troubleshooting information required by the support service in batch when you encounter a problem with an unknown cause or unresolved issues.

The troubleshooting information is output to two files: `tsinf_1st.dat` for primary use, and `tsinf_2nd.dat` for secondary use.

In a single-server configuration system, execute this command on the management server. In a multi-server configuration system, execute this command on the management server or database server.

Format

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

Argument

-f troubleshooting-information-storage-folder

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

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

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

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

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

Storage location

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

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

Notes

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

Return value

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

Return value	Description
0	The command finished normally.
1	Collecting troubleshooting information partially failed.
11	The format for specifying the command arguments is invalid.
12	The specified folder is invalid, or the folder does not exist.
51	You do not have the permissions to execute this command.
101	Command execution was interrupted due to some other error.

Example

The following example shows use of this command to collect troubleshooting information into C:\tmp\troubleshoot.

```
getlogs -f C:\tmp\troubleshoot
```

Related Topics:

- [8.1 Executing commands](#)

8.9 getinstlogs (collecting troubleshooting information about installation)

This section describes the `getinstlogs` command, which collects troubleshooting information regarding product installation on the management server or database server.

Functionality

This command collects troubleshooting information required by the support service from the administrator in batch, when an administrator encounters a problem with an unknown cause or unresolved issues in installing JPI/IT Desktop Management.

In a single-server configuration system, execute this command on the management server. In a multi-server configuration system, execute this command on the management server or database server.

Format

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

Argument

-f troubleshooting-information-storage-folder

Specify the absolute path to the storage folder for troubleshooting information. You can specify a network drive as well as a local drive.

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

If this argument is not specified, the troubleshooting information file will be stored on the Desktop.

Storage location

root-directory-of-JPI/IT-Desktop Management-distribution-media_PPDIR\P064274A\DISK1

Notes

- If the storage folder for troubleshooting information already contains a folder or a file named JDNINST, the command cannot be executed until the folder or the file is deleted.
- Select an existing folder to specify a storage folder for troubleshooting information.

Return value

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

Return value	Description
0	The command finished normally.
1	The collecting of troubleshooting information partially failed.
11	The format for specifying the command arguments is invalid.
12	The specified folder cannot be accessed, or the folder does not exist.
13	Cannot write the backup file to the specified data storage folder.
51	You do not have the permissions to execute this command.

Return value	Description
101	The command execution was interrupted due to some other error.

Example

The following example shows use of this command to collect troubleshooting information about the installation process, into C:\tmp\troubleshoot\install.

```
getinstlogs -f C:\tmp\troubleshoot\install
```

Related Topics:

- [8.1 Executing commands](#)

8.10 resetnid.vbs (resetting the host ID)

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

Functionality

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

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

Tip

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

When the `resetnid.vbs` command is executed on a computer that was once identified by JP1/IT Desktop Management, the host IDs assigned to the computer before and after the command execution are both registered to JP1/IT Desktop Management. Accordingly, two instances of the device information are displayed per computer. However, you can update the view by deleting both device information instances in the Settings module by selecting **Discovery**, and then **Managed Nodes**. After this operation, only the latest device information will be displayed.

Tip

To reset the host ID on the computer on which the site server is installed, perform the procedure described below. If you do not perform this procedure, the operation logs managed on the site server cannot be searched.

1. Execute the `resetnid.vbs` command.
2. Restart the site server service (JP1_ITDM_Remote Site Service).
3. Specify the `-node` option, and then execute the `recreatelogdb` command.

Important note

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

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

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

Format

```
resetnid.vbs /nodeid [ /i]
```

Argument

`/nodeid`

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

`/i`

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

Storage location

agent-installation-folder\bin

Notes

When the `resetnid.vbs` command is executed, the time required is equal to the shortest time of the intervals set for the fields before a new host ID is created. The time intervals are defined in the agent configuration menu **Basic Settings**, under **Agent Basic Settings**.

- Monitoring interval (security items) (minutes)
- Monitoring interval (other than security items) (minutes)
- Interval for acquiring information from the management server (minutes)

Return value

The following table shows the return values of the `resetnid.vbs` command.

Return value	Description
0	The command finished normally.
10001	Command execution was canceled on the user's computer.
10011	The argument syntax is incorrect.
10051	You do not have permission to execute the command.
10101	Failed to reset the host ID.
10150	Failed to reset the host ID.

Example

The following example shows use of this command to reset the host ID.

```
resetnid.vbs /nodeid
```

Related Topics:

- [8.1 Executing commands](#)

9

Troubleshooting

This section describes what actions to take when a problem occurs in JP1/IT Desktop Management.

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 message (databases excepted).

FPH

Indicates that the message is related to JP1/IT Desktop Management databases.

nnnn

Indicates a serial number identifying the message. The serial numbers of messages related to JP1/IT Desktop Management 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 during building of a basic 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 site server
- 9.6 Troubleshooting during building of a multi-server configuration system
- 9.7 Troubleshooting during building of a support service linkage configuration system
- 9.8 Troubleshooting during building of an Active Directory linkage configuration system
- 9.9 Troubleshooting during building of an MDM linkage configuration system
- 9.10 Troubleshooting during building of a network monitoring configuration system
- 9.11 Troubleshooting during building of a cluster system

9.2 Troubleshooting during building of a basic 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 - Manager on the management server, make sure of the following:

- The OS supports JP1/IT Desktop Management - Manager.
- You have logged on to Windows as a user account with Administrative privileges.

If necessary, you can obtain troubleshooting information during installation by using the `getinstlogs` command. For details about the `getinstlogs` command, see [8.9 getinstlogs \(collecting troubleshooting information about installation\)](#).

Log type you can obtain

Log type	Output destination	File name	Description
Installer trace log file	<ul style="list-style-type: none">• When JP1/IT Desktop Management - Manager is installed correctly: <i>JP1/IT Desktop Management - Manager\installation-folder\log</i>• When JP1/IT Desktop Management - 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 - 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:

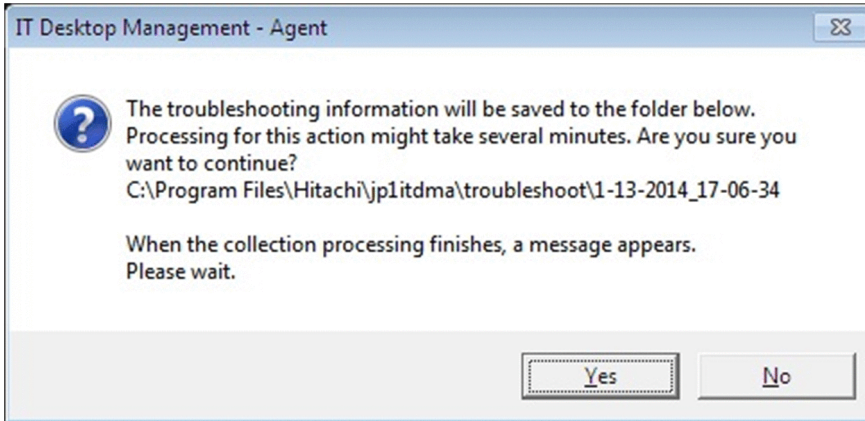
Collect troubleshooting information on the computer on which the problem occurred. Perform this operation as a user with administrator permissions.

1. Double-click `getlogs.vbs`.

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

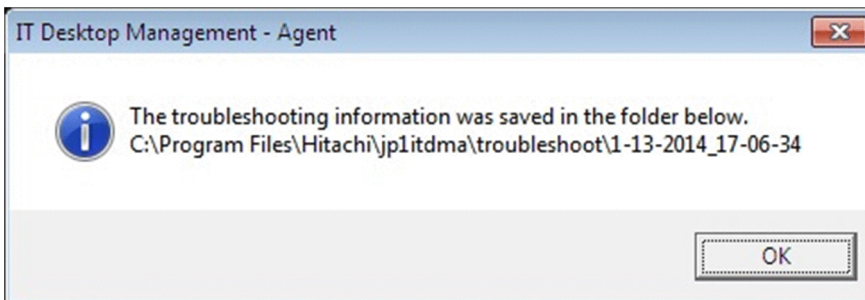
`\bin` in the `JPI/IT Desktop Management - Agent` installation folder

The dialog box asking you whether collection of troubleshooting information can be started appears.



2. Click the **Yes** button.

The collection of troubleshooting information starts. When the troubleshooting information has been obtained, a dialog box indicating this opens with the storage location of the troubleshooting information displayed.



The collected troubleshooting information is stored in the following location:

`JPI/IT Desktop Management - Agent-installation-folder\troubleshoot\YYYY-MM-DD_hh-mm-ss#`
 #: Where *YYYY* is year, *MM* is month, *DD* is day, *hh* is hour, *mm* is minute, and *ss* is second.

3. Click the **OK** button.

The dialog box indicating that the collection of troubleshooting information is complete closes.

The following table shows the troubleshooting information that can be collected by using this method.

Troubleshooting information	Information collected
Agent log	<code>JPI/IT Desktop Management - Agent-installation-folder\log</code>
System information	<ul style="list-style-type: none"> • System information Result of <code>msinfo32/nfo</code> execution • Environment variable Result of <code>SET</code> command execution • Registry information Registry information under <code>HKEY_LOCAL_MACHINE_SOFTWARE\Hitachi</code>

Troubleshooting information	Information collected
System information	<ul style="list-style-type: none"><li data-bbox="472 181 655 203">• File information A list of subfolders and files under the <i>JPI/IT Desktop Management - Agent-installation-folder</i><li data-bbox="472 248 940 311">• Event log Application, system, and security information

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 specified incorrect agent configurations on the computer whose site server and network access control you want to enable, take action as follows according to the settings:

To take action when the agent configuration that clears **Connect to the management server** is assigned:

1. Switch the management status from offline management to online management.
2. Manually start the site server and network access control services.

To take action when the agent configuration that clears **Regularly send information collected from a computer to the management server** is assigned:

1. In the agent configuration, select **Agent Basic Settings** then and **Basic Settings**, and then select **Regularly send information collected from a computer to the management server**.

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 **Agent Basic Settings** view for the agent configuration, select **Connect to the management server**, and then click **OK**.

After you have changed the agent configuration, perform a setup on the user computer.

To switch to online management (setting up on the user computer):

1. Log in to a computer that has the agent installed.
2. From the Windows **Start** menu, select **All Programs, JP1_IT Desktop Management - Agent, Administrator Tool**, and then **Setup**.
3. In the **Setup** dialog box, select **Connect to the management server**, and then click **OK**.
4. In the displayed confirmation dialog box, click **OK**.

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

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 **Agent Basic Settings** view for the agent configuration, clear the **Connect to the management server** check box, and then click **OK**.
2. In the displayed dialog box, click **OK**.

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

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 site server

If you cannot install the site server program on a computer, make sure of the following:

- The OS is a prerequisite OS for the site server.
- You have logged on to Windows as a user account with Administrative privileges.
- You are not trying to install a site server program that is older than the agent that is already installed.

If necessary, you can obtain troubleshooting information during installation by using the `getlogs.vbs` command. The `getlogs.vbs` command is stored in the following folder:

JP1/IT Desktop Management - Agent-installation-folder\bin

Log type you can obtain

Log type	Output location	File name	Description
Installer trace log file	<ul style="list-style-type: none">• When the site server program is installed correctly <i>site-server-program-installation-folder\log</i>• When the site server program is not installed correctly <code>%WINDIR%\Temp</code> <code>\JDNINST</code>	JDNINS01.log	The trace log file of the installer. It is output when the site server program is installed.

Also, obtain troubleshooting information for the site server if necessary. Troubleshooting information for the site server is included in the troubleshooting information for the agent on the same computer. For details about how to collect the information, see [9.2.2 Troubleshooting during agent installation](#).

9.6 Troubleshooting during building of a multi-server configuration system

If you cannot install JP1/IT Desktop Management - Manager, make sure of the following:

- The OS supports JP1/IT Desktop Management - Manager.
- You have logged on to Windows as a user account with Administrative privileges.

If necessary, you can obtain troubleshooting information during installation by using the `getinstlogs` command. For details about the `getinstlogs` command, see [8.9 getinstlogs \(collecting troubleshooting information about installation\)](#).

Log type you can obtain

Log type	Output destination	File name	Description
Installer trace log file	<ul style="list-style-type: none">• When JP1/IT Desktop Management - Manager is installed correctly <i>JP1/IT Desktop Management - Manager-installation-folder\log</i>• When JP1/IT Desktop Management - Manager is not installed correctly <code>%WINDIR%\Temp\JDNINST</code>	JDNINS01.log	The trace log file for the installer. It is output when JP1/IT Desktop Management - Manager is installed.

If you cannot set the data folder that is shared by servers during management server setup, make sure of the following:

- The value set for the data folder shared by servers during management server setup is correct.
- A network failure has not occurred between the management server and the database server.
- The database server has been set up.

If you cannot log in immediately after building an environment, make sure of the following:

- The database server is running.
- A network failure has not occurred between the management server and the database server.

9.7 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.

9.8 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.

9.9 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.

9.10 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.

9.11 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 - 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.

9.12 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 troubleshooting information.

For details about how to collect error information, see the description of the action to be taken if a problem occurs in the *Job Management Partner 1 Version 9 Job Management Partner 1/Network Monitor - Manager Description, User's Guide and Operator's Guide* or the *Job Management Partner 1 Version 10 Job Management Partner 1/NETM/Network Monitor - Manager*.

Appendix

A. Miscellaneous Information

This appendix provides miscellaneous information about using JP1/IT Desktop Management.

A.1 Port number list

This section describes the port numbers used by JP1/IT Desktop Management.

JP1/IT Desktop Management - Manager port number list

Single-server configuration:

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
31080	←	Administrator computer [ephemeral]	TCP	Used for communication from an administrator computer to a management server when the operation window is either referenced or used
31000	←	<ul style="list-style-type: none">• Agent [ephemeral]• Site server [ephemeral]	TCP	Used for communication from either an agent or a site server to a management server
31006 to 31012	None	None	TCP	Used for internal processing of JP1/IT Desktop Management.

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

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

Multi-server configuration:


Management server

Port number for management server	Connection direction	Connected to [port number]	Protocol	Use
31080	←	Administrator computer [ephemeral]	TCP	Used for communication from an administrator computer to a management server when the operation window is either referenced or used
31000	←	<ul style="list-style-type: none">• Agent [ephemeral]• Site server [ephemeral]	TCP	Used for communication from either an agent or a site server to a management server
31006	←	Database server [ephemeral]	TCP	Used for communication from a database server to a management server
31007 to 31009, 31011, 31012	None	None	TCP	Used for internal processing of JP1/IT Desktop Management.

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

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

Database server

Port number for database server	Connection direction	Connected to [port number]	Protocol	Use
31010		Management server [ephemeral]	TCP	Used for communication from a management server to a database server
31007	None	None	TCP	Used for internal processing of JP1/IT Desktop Management.

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

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

Specify settings to enable the following ports for networks between JP1/IT Desktop Management - Manager and agentless computers.

Ports used for shared files and printers:

- Protocol: TCP and UDP, Port number: 445
- Protocol: TCP, Port number: 139
- Protocol: UDP, Port number: 137 and 138


Ports used for SNMP protocol:

- Protocol: UDP, Port number: 161

Follow the steps below to specify protocol ports.

1. From the Windows Control Panel, select **Windows Firewall** and then **Advanced**.
2. In the displayed dialog box, select **Inbound Rules**, and then in the operation window, select **New Rule**. Follow the displayed **New Inbound Rule Wizard** to specify protocol ports.

Port number list for a site server

Port number for site server	Connection direction	Connected to [Port number]	Protocol	Use
31000		Agent or management server [ephemeral]	TCP	Used for a communication from an agent or management server to a site server
31010	None	None	TCP	Used for internal processing of a site server

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

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

Specify settings to enable the following ports for the networks between JP1/IT Desktop Management - Remote Site Server and agentless computers.

Ports used for shared files and printers:

- Protocol: TCP and UDP, port number: 445
- Protocol: TCP, port number: 139
- Protocol: UDP, port number: 137 and 138

Ports used for SNMP protocol:

- Protocol: UDP, port number: 161

Follow the steps below to specify the protocol ports.

1. From the Windows Control Panel, select **Windows Firewall** and then **Advanced**.
2. In the dialog box that appears, select **Inbound Rules**, and then in the operation window, select **New Rule**.
Follow the displayed **New Inbound Rule Wizard** to specify the protocol ports.

Port number list for a controller and remote control agent

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

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

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

- Port number for a controller
Specify port numbers in the **Options** dialog box of the controller.

- Port number for a remote controller agent
Specify port numbers in **Remote Control Settings** in the agent configurations.
- Port number for the chat functionality
In the **Chat** window, select **Options**, and in the displayed dialog box, in the **Connect** tab, specify the port numbers.

JP1/IT Desktop Management - Agent port number list

Agent port number	Connection direction	Connected server [port number]	Protocol	Use
31001	←	Management server [ephemeral]	TCP	Used for communication from a management server to the agent
16992	←	Management server [ephemeral]	TCP	Used for controlling the power source of a computer that uses AMT

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

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

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

Port numbers for agentless devices

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

A.2 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 10-01

- 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 `resetnid.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 `resetnid.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 177
- Active Directory
 - searching for devices registered in 107
- Active Directory linkage configuration system
 - building 57
 - overview of building 57
- adding, agent configurations 99
- adding, site server group 101
- adding agent configurations 99
- adding network monitor settings 112
- adding product license 21
- adding site server groups 101
- agent
 - automatically installing 39
 - 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 28
 - planning installation 27
 - procedure for setting up 37
- agent installation
 - disk copy 35
 - distributing agent by email 33
 - distributing media 32
 - logon script 34
 - uploading to file server 31
 - uploading to Web server 30
- agentless configuration system
 - building 47
 - overview of building 47
- automatically deploying agent (network search) 40

B

- basic configuration system
 - building 15
 - overview of building 16
- building JP1/Network Monitor - Manager linkage configuration systems 62

C

- changing
 - setting 75
- changing assignment of network monitor settings 113
- changing default password 23
- checking
 - agent installation status 39
 - discovered device 42
 - excluded device 43
 - latest discovery status 41
 - managed device 42
- cluster system
 - building 65
- collecting troubleshooting information, getlogs command 190
- collecting troubleshooting information about installation, getinstlogs command 192
- command
 - used for building-related operation 171
- command description format 174
- components
 - updating 117
- controller, uninstalling 142
- creating
 - installation set 28
- 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

- database server
 - procedure for setting up 53
- 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 25
- disabling the network monitor 140

- discovered device
 - checking 42
- discovery status
 - checking latest status 41

E

- editing
 - network control settings file 114
- editing, automatic update settings for network control list 112
- editing, site server group information 102
- editing devices in the network control list 112
- editing site server group information 102
- enabling
 - JP1/NETM/NM - Manager linkage settings 113
- enabling the network monitor 59
- excluded device
 - checking 43
- executing commands 172
- exportdb command 177

G

- getinstlogs command 192
- getlogs command 190
- Getting Started** wizard
 - searching Active Directory 107
 - searching network 25
- group resource
 - procedure for creating on primary server 67

I

- identifying
 - all devices used in organization 25
- importdb command 181
- installation set
 - creating 28
- installing
 - agent automatically 39
 - agent manually 28
 - agent on computer 29
- installing agent
 - disk copy 35
 - distributing agent by email 33
 - distributing media 32
 - from supplied media 36
 - logon script 34

- uploading to file server 31
- uploading to Web server 30
- installing product (overwrite installation) 117

J

- JP1/IM linkage configuration system
 - overview of building 63
- JP1/IT Desktop Management
 - setting up on primary server 71
 - setting up on standby server 74
- JP1/IT Desktop Management - Manager
 - installation type 17
 - procedure for installing 17
- JP1/NETM/NM - Manager
 - troubleshooting during linkage with 212
- JP1/NETM/NM - Manager linkage configuration system
 - overview of building 62
- JP1/NETM/NM - Manager linkage settings
 - enabling 113
- JP1/Network Monitor - Manager linkage configuration systems, building 62

L

- license
 - registering 21
- logging in 22
- logging in to operation window 22

M

- mail notification, discovery from IP address 97
- mail notification, searching Active Directory 108
- managed device
 - checking 42
- management server
 - procedure for replacing in single-server configuration system 146
 - setting up (in single-server configuration) 19
- management server environment
 - creating 17
- management server for multi-server configuration system
 - procedure for setting up 54
- managing, server configuration 101
- managing server configurations 101
- MDM linkage configuration system
 - building 58

- overview of building 58
- message
 - output format 197
- migrating
 - environment 145
- miscellaneous information 214
- multi-server configuration system
 - building 52
 - overview of building 52, 66

N

- network
 - searching for devices connected to 25
- network control appliance
 - replacing computer by network control appliance (when network monitor is enabled) 115
- network control list
 - editing automatic update settings 112
- network control list, editing devices in 112
- network control settings file
 - editing 114
- network monitoring configuration system
 - building 59
 - overview of building 59
- network monitor settings, adding 112

O

- offline management configuration system
 - building 46
 - overview of building 46
- operation window, logging in 22
- overview of building
 - JP1/NETM/NM - Manager linkage configuration system 62
- overview of building cluster system
 - single-server configuration system 65
- overview of performing overwrite installation
 - in cluster system in multi-server configuration system 134
 - in cluster system in single-server configuration system 133
 - JP1/IT Desktop Management - Manager in multi-server configuration system 130
- overview of troubleshooting
 - during building of environment 197
- overview of uninstalling
 - entire system 136

- overview of upgrading
 - entire JP1/IT Desktop Management system 123
 - JP1/IT Desktop Management - Manager in multi-server configuration system 131
- overwrite installation
 - in cluster system in multi-server configuration system 134
 - in cluster system in single-server configuration system 133
 - JP1/IT Desktop Management - Manager in multi-server configuration system 130
- overwrite-installing product 117

P

- planning installation
 - agent 27
- port number list 214
- procedure for changing
 - currency unit 92
 - data folder shared by servers 79
 - folders used 78
 - port number 87
 - setting for connection to database 76
- procedure for connecting
 - site server to another management server 156
- procedure for controlling
 - network bandwidth used for distribution 90
- procedure for initializing
 - database 95
- procedure for migrating
 - from single-server configuration system to multi-server configuration system 158
 - JP1/IT Desktop Management 09-51 or earlier in single-server configuration system to multi-server configuration system 162
- procedure for performing overwrite installation
 - agent from supplied media 120
 - JP1/IT Desktop Management - Manager 118
 - network access control agent from supplied media 122
 - site server program from supplied media 121
- procedure for recording operation log
 - on management server in single-server configuration system 81
- procedure for registering
 - component 129
- procedure for replacing
 - computer for which network access control enabled 170

- computer on which agent installed 153
- database server 163
- management server in multi-server configuration system 150
- management server in single-server configuration system 146
- replacing management server and database server in multi-server configuration system at one time 166
- site server 154
- procedure for replacing management server in single-server configuration system 146
- procedure for uninstalling
 - agent 138
 - JP1/IT Desktop Management - Manager 137
 - site server program 139
- procedure for uninstalling JP1/IT Desktop Management - Manager
 - in cluster system in multi-server configuration 144
 - in cluster system in single-server configuration system 143
- procedure for upgrading
 - database 94
 - JP1/IT Desktop Management - Manager 125
- product license
 - adding 21
 - registering 21

R

- recognition procedure
 - when agent environment is changed 217
- recreatelogdb command 185
- recreating operation log index on the site server, recreatelogdb command 185
- registering
 - product license 21
- removing, site server group 102
- removing site server groups 102
- resetnid.vbs command 194
- resetting host ID, resrtnid.vbs command 194
- restoring data using a backup, importdb command 181

S

- searching
 - devices connected to network 25
 - devices registered in Active Directory 107
- Setting additional management item, information acquired from Active Directory 106
- setting for building

- Active Directory linkage configuration system 106
- agentless configuration system 100
- basic configuration system 97
- MDM linkage configuration system 110
- network monitoring configuration system 112
- site server configuration system 101
- support service linkage configuration system 104
- setting management target 108
- setting up management server (in single-server configuration) 19
- setting user account information 23
- site server
 - procedure for setting up 51
- site server configuration system
 - building 48
 - overview of building 48
- site server program
 - procedure for installing 48
 - procedure for installing from supplied media 49
 - procedure for installing in operation window 50
- SNMP credentials 98
- specifying an update interval, agentless 100
- specifying search conditions, discovery from IP address 97
- specifying search conditions, searching Active Directory 108
- specifying search conditions for Active Directory 108
- specifying search conditions for IP address range 97
- specifying server configurations 101
- specifying settings for connecting to Active Directory 106
- specifying settings for connecting to the support service 104
- specifying settings to link with an MDM system 110
- stopping services, stopservice command 188
- stopservice command 188
- support service linkage configuration system
 - building 56
 - overview of building 56
- switching from offline management to online management 202
- switching from online management to offline management 203
- system configuration
 - building 45

T

- troubleshooting 196

- during agent installation 199
- during building of Active Directory linkage configuration system 208
- during building of agentless configuration system 204
- during building of basic configuration system 199
- during building of cluster system 211
- during building of management server 199
- during building of MDM linkage configuration system 209
- during building of multi-server configuration system 206
- during building of network monitoring configuration system 210
- during building of offline management configuration system 202
- during building of site server 205
- during building of support service linkage configuration system 207
- during linkage with JP1/NETM/NM - Manager 212
- troubleshooting information
 - agent 200

U

- uninstalling
 - in cluster system in single-server configuration system 143
 - JP1/IT Desktop Management - Manager 137
 - product 135
- uninstalling controllers 142
- unlocking user account 24
- updatesupportinfo command 175
- updating
 - component 127
 - components 117
- upgrading JP1/IT Desktop Management - Manager, overview of 131
- uploading support service information 175
- user account, unlocking 24

W

- wizard
 - Getting Started** wizard, searching Active Directory 107
 - Getting Started** wizard, searching network 25