HITACHI
Inspire the Next

Job Management Partner 1/IT Desktop Management

Setup Guide

3020-3-S99(E)

Relevant program product

P-2642-739L Job Management Partner 1/IT Desktop Management - Manager 09-50(for Windows 7 Professional,Windows 7 Enterprise,Windows 7 Ultimate,Windows Server 2008 Enterprise,Windows Server 2008 Standard,Windows Server 2003)

Trademarks

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

Apple is a registered trademark of Apple Computer, Inc.

Firefox is a registered trademark of the Mozilla Foundation.

HP-UX is a product name of Hewlett-Packard Development Company, L.P. in the U.S. and other countries.

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

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

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

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

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

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

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

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

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

Windows 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/).

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.

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.

Printed in Japan.

Issued

May. 2012: 3020-3-S99(E)

Contents

Preface

This manual provides the prerequisites for Job Management Partner 1/IT Desktop Management, and explains how to install and set up Job Management Partner 1/IT Desktop Management.

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

- Intended readers
- Organization of this manual
- Microsoft product name abbreviations
- Conventions: Fonts and symbols

Intended readers

- Knowledge on how to install and uninstall JP1/IT Desktop Management, and how to migrate its environment
- Knowledge on how to configure a JP1/IT Desktop Management system and knowledge of the procedures.

Organization of this manual

This manual is organized into the following chapters:

Chapter 1 Overview

This chapter provides an overview of JP1/IT Desktop Management.

Chapter 2 Setup and installation

This chapter describes the prerequisites and provides the procedure for intalling JP1/IT Desktop Management.

Chapter 3 Logging in and activating a license

This chapter describes the procedure for displaying the JP1/IT Desktop Management login window, provides an overview of product licenses, and describes how to register a product license.

Chapter 4 Completing the initial setup

This chapter describes how to log in to JP1/IT Desktop Management, how to manage user accounts, and the procedure for setting up a connection to the support service.

Chapter 5 Preparing for management

This chapter describes the procedure for searching the network to discover nodes.

Chapter 6 Setting up system configurations

This chapter provides an overview of system configurations for using JP1/IT Desktop Management, and provides the procedures for setting up the configurations.

Chapter 7 Re-installing products

This chapter describes the procedure for re-installing JP1/IT Desktop Management and its components.

Chapter 8 Migrating an environment

This chapter describes the procedures for replacing the management server and site server and connecting a site server to another management server.

Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation			Product name
Active Directory			Microsoft(R) Active Directory(R)
AppLocker			Microsoft(R) AppLocker(TM)
Internet Explorer	Microsoft Internet Explorer		Microsoft(R) Internet Explorer(R)
	Windows Internet Explorer		Windows(R) Internet Explorer(R)
Microsoft.NET			Microsoft(R).NET
Microsoft Cluster Service			Microsoft(R) Cluster Service
Microsoft Outlook			Microsoft(R) Outlook(R)
Microsoft Outlook Express			Microsoft(R) Office Outlook(R)
MS-DOS			Microsoft(R) MS-DOS(R)
Windows	Windows 2000	Windows 2000 Advanced Server	Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Windows 2000 Professional	Microsoft(R) Windows(R) 2000 Professional Operating System
		Windows 2000 Server	Microsoft(R) Windows(R) 2000 Server Operating System
	Windows 7		Microsoft(R) Windows(R) 7 Enterprise
			Microsoft(R) Windows(R) 7 Home Basic
			Microsoft(R) Windows(R) 7 Home Premium
			Microsoft(R) Windows(R) 7 Professional
			Microsoft(R) Windows(R) 7 Starter
			Microsoft(R) Windows(R) 7 Ultimate
	Windows Server 2003	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
			Microsoft(R) Windows Server(R) 2003, Standard Edition
			Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
		Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003, Standard x64 Edition

Abbreviation			Product name
			Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
			Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows Server 2008	Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 Enterprise
			Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Windows Server 2008 Foundation	Microsoft(R) Windows Server(R) 2008 R2 Foundation
		Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 R2 Standard
			Microsoft(R) Windows Server(R) 2008 Standard
			Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V
	Windows Vista		Microsoft(R) Windows Vista(R) Business
			Microsoft(R) Windows Vista(R) Enterprise
			Microsoft(R) Windows Vista(R) Home Basic
			Microsoft(R) Windows Vista(R) Home Premium
			Microsoft(R) Windows Vista(R) Ultimate
	Windows XP	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
		Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System
Windows 95			Microsoft(R) Windows(R) 95 Operating System
Windows 98			Microsoft(R) Windows(R) 98 Operating System
Windows Live Mail			Windows Live(TM) Mail
Windows Me			Microsoft(R) Windows(R) Millennium Edition Operating System
Windows Media Player			Windows Media(R) Player

Abbreviation	Product name
Windows NT 4.0	Microsoft(R) Windows NT(R) Server Enterprise Edition Version 4.0
	Microsoft(R) Windows NT(R) Server Network Operating System Version4.0
	Microsoft(R) Windows NT(R) Workstation Operating System Version4.0
Windows Mail	Windows(R) Mail

Conventions: Fonts and symbols

The following table explains the fonts used in this manual:

Font	Convention
Bold	**Bold** type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italics	*Italics* are used to indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` *Italics* are also used for emphasis. For example: • Do *not* delete the configuration file.
`Code font`	A `code font` indicates text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
|	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example:

Symbol	Convention
	`A|B|C` means A, or B, or C.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of A, or B, or C.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
`...`	In coding, an ellipsis (...) indicates that one or more lines of coding are not shown for purposes of brevity. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify`A, B`, you can specify `B` as many times as necessary.

Icon	Description
	Caution: Indicates a situation that requires caution from the user.
	WARNING: Indicates a situation that requires immediate user action.
	Note: Indicates important useful information for the user.
	Tip: Indicates a useful tip for the user.

Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00*, but the same version number would be written in the program as *02-00*.

1

Overview

This chapter provides an overview of the tasks that you need complete to install, configure, and begin using JP1/IT Desktop Management.

Overview of the getting started process

The following steps outline the processes involved in initial setup and discovering nodes:

1. **Prepare for the installation:**

   To prepare for installation, make sure you have the required system and OS requirements in your environment. For details, see JP1/IT Desktop Management system requirements on page 2-2. Refer to the List of Port Numbers on page 2-14. You may need to change the firewall settings for JP1/IT Desktop Management to communicate with the network. For details, Allowing communication through Windows firewalls on page A-2.

2. **Install JP1/IT Desktop Management:**

   Install the software on a server running a supported operating system. See Requirements for the management server on page 2-3 for details. This document refers to the server as your management server. An **Installation Wizard** with **Quick Install** and **Custom Install** options helps you to install JP1/IT Desktop Management.

3. **Register a product license:**

   Register a valid product license. You can register a product license from the login panel.

4. **Login and complete initial setup:**

   After registering a product license, use the default login credentials to log in to JP1/IT Desktop Management. Afterwards, for security reasons, you will be prompted to change your user ID and password. After that, you set up user accounts for other administrators.

5. **Discover nodes and install agents:**

   JP1/IT Desktop Management's management process involves communication between the management server and nodes connected to the network. The management server collects data for management from agents installed on the discovered nodes. From the **Getting Started Wizard**, you will discover nodes, install agents for management or start managing the discovered nodes without agents.

6. **Begin management:**

   After discovering the nodes install agents to start managing your IT operations environment. You can define and implement security policies; manage software, hardware assets, contracts and licenses; manage software and file distribution, get alerts for security events and generate reports.

2

Setup and installation

This chapter outlines the system requirements and the installation instructions.

It includes the following key topics:

- Overview
- Flow of setting up a basic system
- JP1/IT Desktop Management system requirements
- List of Port Numbers
- JP1/IT Desktop Management - Manager installation types
- Installing JP1/IT Desktop Management
- Custom installation

Overview

To install JP1/IT Desktop Management on your management server, you must first set up the client computer and make sure your target computers meet the agent and agentless requirements. This section outlines the complete system requirements and the list of port numbers.

- **System requirements**: Make sure your environment meets the system requirements that are detailed in JP1/IT Desktop Management system requirements on page 2-2.
- **Port Numbers**: Gather access protocol credentials for each management target in List of Port Numbers on page 2-14.

Flow of setting up a basic system

To set up a basic system, first set up the management server, and then install an agent on each computer to be managed.

1. Set up the management server.
2. Register a product license for JP1/IT Desktop Management, log in to the system, and then specify the user account information.
3. Install an agent on each computer to be managed by JP1/IT Desktop Management.

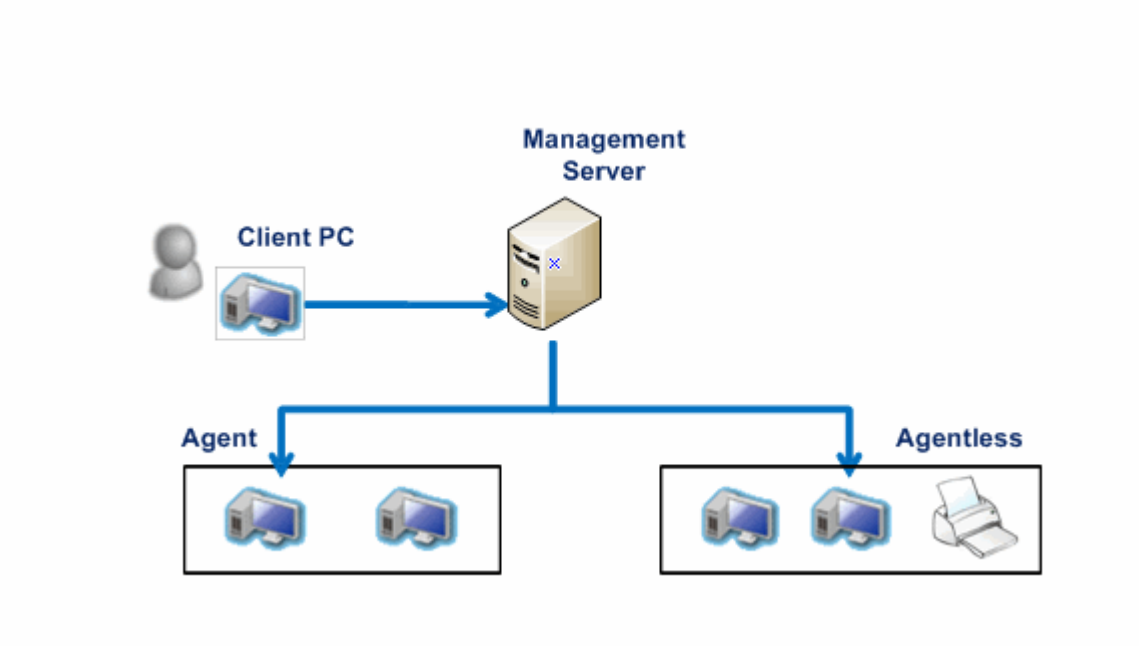
Setup of the basic system is completed.

Related Topics:

- Registering licenses on page 3-4
- Launching the login panel on page 3-2
- Installing agents on page 5-8

JP1/IT Desktop Management system requirements

Working with JP1/IT Desktop Management includes the Management server, Client computer and Agent/Agentless devices.



System requirements for JP1/IT Desktop Management include the hardware and software requirements for the following:

- Management server
- Agent computers
- Agentless computers
- Client computer
- Optional settings - AMT
- Remote control
- Network access control

Requirements for the management server

JP1/IT Desktop Management is installed on the management server. JP1/IT Desktop Management uses a client computer to communicate with both agent and agentless computers.

Network communication environment

- **Management server and client computer**: Environment must allow HTTP communication through browser.
- **Management server and agent**:
  - Configure the network setting so the management server and agent can directly reference to each other's host name and IP address. See List of Port Numbers on page 2-14 for Port Number specifications.
  - JP1/IT Desktop Management uses the TCP/IP protocol for communication. So you must create exceptions in Windows Firewall settings to allow communication between the management server and

managed devices through the ports. See Allowing communication through Windows firewalls on page A-2 for details.

- **Management server and agentless computer**: Each managed target computers must have Administrative Share (Admin$) and IPC$ permission. All managed target computers without an agent must have common access accounts.

Hardware

The following table lists the hardware requirements for the management server.

Item	Requirements
Computer	PC/AT-compatible
CPU Recommended system requirements for Windows Server 2008.	• 2.0 GHz or faster 32-bit (x86) processor • 2.0 GHZ or faster 64-bit (x64) processor
Hard Disk	2.4 GB or more (Main program)
	35.0 GB or more (Database)
	500 MB (on the system drive (for the work area))
Memory	2.0 GB or more

The following table lists the additional free space required to use the distribution facility.

Item	Required environment
Drive on which JP1/IT Desktop Management - Manager is installed	Free space equal to at least twice the size of the package (before compression to a ZIP file)
Drive that contains the data folder	Free space equal to at least twice the size of the package (before compression to a ZIP file)
System drive	Free space equal to the size of the package (before compression to a ZIP file)

The following table lists the free space required to automatically update components.

Item	Required environment
Drive on which JP1/IT Desktop Management - Manager is installed	500 MB
Drive that contains the data folder	
System drive	

Operating System

The following table lists the requirements for the management server's operating system.

OS	Details
Windows 7[#1]	Windows 7 Enterprise[#2]
	Windows 7 Professional[#2]
	Windows 7 Ultimate[#2]
Windows Server 2008[#3]	Windows Server 2008 Enterprise[#4]
	Windows Server 2008 Enterprise without Hyper-V[#4]
	Windows Server 2008 R2 Enterprise[#2]
	Windows Server 2008 Standard[#4]
	Windows Server 2008 Standard without Hyper-V[#4]
	Windows Server 2008 R2 Standard[#2]
Windows Server 2003	Windows Server 2003, Enterprise Edition[#2, #4]
	Windows Server 2003, Enterprise x64 Edition[#2, #4]
	Windows Server 2003 R2, Enterprise Edition[#4]
	Windows Server 2003 R2, Enterprise x64 Edition[#4]
	Windows Server 2003, Standard Edition[#2, #4]
	Windows Server 2003, Standard x64 Edition[#2, #4]
	Windows Server 2003 R2, Standard Edition[#4]
	Windows Server 2003 R2, Standard x64 Edition[#4]

#1: XP mode is not supported.

#2: Including Service Pack 1.

#3: Server Core cannot be used as an installation option.

#4: Including Service Pack 2.

Requirements for agent computers

The management server communicates with managed nodes through agents. Following are the requirements for JP1/IT Desktop Management - Agent.

Hardware

The following table lists the hardware requirements for agent computers:

Item	Requirements		
Computer	PC/AT-Compatible		
Hard Disk	20 MB (40 MB or more is recommended)		
Virtual memory	40 MB or more		
CPU/Physical Memory	**Windows**	**CPU**	**Physical Memory**
	2000	133 MHz or faster 32-bit (x86) processor	64 MB + 20 MB or more
	XP	300 MHz or faster 32-bit (x86) processor	128 MB + 20 MB or more
	Server 2003	133 MHz or faster 32-bit (x86) or 64-bit (x64) processor	128 MB + 20 MB or more
	Vista	800 MHz or faster 32-bit (x86) or 64-bit(x64) processor	512 MB + 20 MB or more
	Server 2008	• 1.0 GHz or faster 32-bit (x86) processor • 1.4 GHz or faster 64-bit (x64) processor	512 MB + 20 MB or more
	7	1.0 GHz or faster 32-bit (x86) or 64-bit (x64) processor	1 GB + 20 MB or more

The following table lists the additional free space required to use the distribution facility.

Item	Required environment
Drive on which an agent is installed	Free space equal to at least twice the size of the package (before compression to a ZIP file)
System drive of a computer on which an agent is installed	Free space equal to the size of the package (before compression to a ZIP file)

The following table lists the free space required to automatically update an agent.

Item	Required environment
Drive on which an agent is installed	50 MB
System drive of a computer on which an agent is installed	

Operating System

The following table lists the OS requirements for agent computers:

OS	Details
Windows 7[#1]	Windows 7 Enterprise[#2]
	Windows 7 Home Basic[#2]
	Windows 7 Home Premium[#2]
	Windows 7 Professional[#2]
	Windows 7 Starter[#2]
	Windows 7 Ultimate[#2]
Windows Server 2008[#3]	Windows Server 2008 Enterprise[#4]
	Windows Server 2008 Enterprise without Hyper-V[#4]
	Windows Server 2008 R2 Enterprise[#2]
	Windows Server 2008 Standard[#4]
	Windows Server 2008 Standard without Hyper-V[#4]
	Windows Server 2008 R2 Standard[#2]
Windows Vista	Windows Vista Business[#2, #4]
	Windows Vista Enterprise[#2, #4]
	Windows Vista Home Basic[#2, #4]
	Windows Vista Home Premium[#2, #4]
	Windows Vista Ultimate[#2, #4]
Windows Server 2003	Windows Server 2003, Enterprise Edition[#2, #4]
	Windows Server 2003, Enterprise x64 Edition[#2, #4]
	Windows Server 2003 R2, Enterprise Edition[#4]
	Windows Server 2003 R2, Enterprise x64 Edition[#4]
	Windows Server 2003, Standard Edition[#2]
	Windows Server 2003, Standard x64 Edition[#2, #4]
	Windows Server 2003 R2, Standard Edition[#4]
	Windows Server 2003 R2, Standard x64 Edition[#4]
Windows XP	Windows XP Home Edition Operating System (Service Pack 2, 3)
	Windows XP Professional Operating System (Service Pack 2, 3)
Windows 2000	Windows 2000 Advanced Server Operating System (Service Pack 4)
	Windows 2000 Professional Operating System (Service Pack 4)
	Windows 2000 Server Operating System (Service Pack 4)

#1: XP mode is not supported.

#2: Including Service Pack 1.

#3: Server Core cannot be used as an installation option.

#4: Including Service Pack 2.

Web browser and e-mail applications

To collect Operation Logs on user's activities such as sending/receiving e-mail attachments and file upload/download from a Web browser, check that your environment adheres to the Web browser and e-mail application requirements.

The following table lists the agent requirements that support tracking e-mail attachments and file upload/download activity from the Web browser.

Type	Product Name	Version
E-mail application	Microsoft Outlook Express	6
	Microsoft Outlook	2002
		2003
		2007
		2010
	Windows Mail	6
	Windows Live Mail	2009
		2011
Web Browser	Microsoft Internet Explorer	6.0
	Windows Internet Explorer	7.0
		8.0
		9.0
	FireFox	3.5
		3.6
		4.0
		5.0

Requirement for agentless computers

If you decide to manage some of the discovered nodes without agents, after discovering nodes you can set up an **Auto Monitoring Schedule** for the selected nodes. Agentless management has certain management limitations. See Agent and Agentless management capacity on page A-7 for details on agentless management capacity. The agentless computers should have the following prerequisites:

- Windows must have Administrative Share.

- If you want to discover using Active Directory discovery, the system must be registered as a domain computer.
- SNMP agent is required for Network Devices and Printers.

The following table shows the system specifications for agentless management:

Device	OS Category	Operating System	Machine Type
System Device	Windows	Windows 7	PC
		Windows Server 2008 R2	
		Windows Server 2008	
		Windows Vista	
		Windows Server 2003	
		WindowsXP Professional	
		WindowsXP Home	
		WindowsMe	PC#
		Windows2000 Professional	PC
		Windows2000 Server	
		Windows98	PC#
		WindowsNT 4.0	
		WindowsNT 3.51	
	Unix	HP-UX	PC
		Other than the above UNIX	PC#
	Linux	RedHat Linux	PC
		Other than the above Linux	PC#
	Mac OS	Mac OS X	PC
		Other than the above Mac OS	PC#
Network Device Except PC	Printer	-	Printer
	Network Device	Router	Network Device
		Bridge	
		Repeater	
	Other IP Device	-	Other Device

Note: Legend: #: JP1/IT Desktop Management may determine these devices as "Other PC devices."

Requirements for Client computers

You will use a client computer's Web browser to connect to JP1/IT Desktop Management's management server. The following table shows the requirements for client computers.

Item	Requirements	
	Product Name	Version
Web Browser	Microsoft™ Internet Explorer	6.0
	Windows Internet Explorer	7.0
		8.0
		9.0
	Firefox™	3.5 or later
Web browser plug-in	Adobe™ Flash Player	10.3 or later

Requirements for optional settings

If you do not have JP1/IT Desktop Management's Agent installed in the managed target computers, but still want to monitor and remotely access the agentless computer, you can use Intel AMT to access the target computers. To setup AMT functionality, see Setting up AMT functionality on page A-2.

The following table shows the requirements for using Intel AMT:

Product	Item	Details
Common (manager, agent)	Required software	.NET Framework 2.0 or later
Agent	Required hardware	PC equipped with Intel vPro technology
		PC equipped with Intel Centrino Pro technology
	Required drivers	Intel Management Engine Interface
		Intel AMT
	AMT BIOS settings	Set to "Small Business"
		Enable DHCP mode
	Network environment	DHCP environment

Using Intel AMT has the following restrictions.

- If a local area network and wireless local area network are connected to the same subnet, the AMT functionality will not get activated.

- If a computer gets disconnected from wireless local area network connection, AMT will not function and you cannot start the machine using AMT. If connection fails, Wake on LAN is re-executed.
- If the computer is running on battery and stops due to battery failure, AMT will not function and you cannot start the machine from AMT.

Requirements for remote control

To use the remote control feature, the following configuration is required to support the controller.

Software requirements:

You can connect remote control both in agent and agentless management environment. When you manage the computers with an agent, the remote control OS requirement is the same as your agent OS requirement.

- **Agent remote control**: You should have JP1/IT Desktop Management Agent, installed in the agent computers.
- **Agentless remote control**: You should have client software, RFB protocol to support remote control connection to VNCClient, Apple Remote Desktop, Intel vPro6.0 Hardware KVM

Hardware requirements for remote controller:

The following table lists the hardware requirements for remote controller:

Item	Requirement		
Computer	PC/AT - Compatible		
Hard Disk	20 MB or more		
CPU/Physical Memory	**Windows**	**CPU**	**Physical Memory**
	7	1.0 GHz or faster 32-bit (x86)or 64-bit (x64) processor	1GB +#1
	Server 2008	• 1.0 GHz or faster 32-bit (x86) processor • 1.4 GHz or faster 64-bit(x64) processor	512 MB +#1
	Vista	800 MHz or faster 32-bit (x86)or 64-bit (x64) processor	512 MB +#1
	Server 2003	133 MHz or faster 32-bit (x86)or 64-bit (x64) processor	128 MB +#1
	XP	300 MHz or faster 32-bit (x86)processor	128 MB +#1

Note: Legend: #1 indicates the required physical memory for the following functions:

- Temporary buffer for drawing - 5 MB in Agents.
- Temporary buffer for file transfer - 2 MB
- Buffer for chat server - 2+ MB (0.1 per connection)
- Buffer for chat client - 2+ (0.1 per connection)

Requirements for network access control

To use the network access control feature, your agent computers should have the following software and hardware requirements.

Software requirements: The network access controller requires V 3.0 JP1/IT Desktop Management - Agent and the software and hardware specified in this section.

Hardware requirements:

The following table lists the hardware requirements for network access control:

Item	Requirement		
Computer	PC/AT - Compatible		
Hard Disk	20 MB or more.(Recommended 40 MB or more)		
Virtual Memory	32 MB or more		
CPU/Physical Memory	**Windows**	**CPU**	**Physical Memory**
	Server 2008	• 1.0 GHz or faster 32-bit (x86) processor • 1.4 GHz or faster 64-bit(x64) processor	512 MB + 20 MB more
	Server 2003	133 MHz or faster 32-bit (x86)processor	128 MB + 20 MB more

Operating systems requirements:

The following table lists the operating system requirements for using JP1/IT Desktop Management's network access control in your environment.

Item	Requirement
Windows Server 2003	Windows Server 2003, Standard Edition
	Windows Server 2003, Enterprise Edition
	Windows Server 2003 R2, Standard Edition
	Windows Server 2003 R2, Enterprise Edition

Item	Requirement
Windows XP	Windows XP Professional Operating System (Service Pack 2/3)

Requirements for the site server

This subsection describes the hardware, OS, and software requirements for the site server.

Hardware

The following table lists the hardware requirements for the site server.

Item	Requirements
Computer	PC/AT-compatible
CPU Recommended system requirements for Windows Server 2008.	• 2.0 GHz or faster 32-bit (x86) processor • 2.0 GHZ or faster 64-bit (x64) processor
Hard Disk	2.4 GB or more.(Recommended 3.0 GB or more) (Main program)
	4.0 GB or more (Database)
Memory	2.0 GB or more

OS

The following table lists the OS requirements for the site server.

OS	Details
Windows 7[#1]	Windows 7 Enterprise[#2]
	Windows 7 Professional[#2]
	Windows 7 Ultimate[#2]
Windows Server 2008[#3]	Windows Server 2008 Enterprise[#4]
	Windows Server 2008 Enterprise without Hyper-V[#4]
	Windows Server 2008 R2 Enterprise[#2]
	Windows Server 2008 Standard[#4]
	Windows Server 2008 Standard without Hyper-V[#4]
	Windows Server 2008 R2 Standard[#2]
Windows Server 2003	Windows Server 2003, Enterprise Edition[#2, #4]
	Windows Server 2003, Enterprise x64 Edition[#2, #4]

OS	Details
	Windows Server 2003 R2, Enterprise Edition#4
	Windows Server 2003 R2, Enterprise x64 Edition#4
	Windows Server 2003, Standard Edition#2, #4
	Windows Server 2003, Standard x64 Edition#2, #4
	Windows Server 2003 R2, Standard Edition#4
	Windows Server 2003 R2, Standard x64 Edition#4

#1: XP mode is not supported.

#2: Including Service Pack 1.

#3: Server Core cannot be used as an installation option.

#4: Including Service Pack 2.

Software

An agent must be installed.

List of Port Numbers

The following tables have a list of Port Numbers that are used by JP1/IT Desktop Management and JP1/IT Desktop Management Agent.

Management Server [port number]	Connection direction	Connection Target [port number]	Protocol	Usage
Management Server [31000]	<-	Computer[ephemeral]	TCP	Connect to Management Server from computer
Management Server [31001]	->	Computer[ephemeral]	TCP	Connect to computer from Management Server
Management Server [31080]	<-	Client[ephemeral]	TCP	Connect to Management Server from each browser
Management Server [16992]	->	Computer[ephemeral]	TCP	Control power on/off by using AMT
Management Server 31002 ~ 31013	None	None	TCP	For internal process of JP1/IT Desktop Management

Each port number is set by default at delivery of the product. If the port number (given in the list above) is already used in your system environment, specify a different port number at the time of setting up of JP1/IT Desktop Management. In addition, if you control the ports in the network between JP1/IT Desktop Management and JP1/IT Desktop Management Agent by firewall, please enable the connection to pass through the ports (given in the list above).

To set a protocol port:

1. From the Windows **Control Panel**, select **Windows Firewall** > **Advanced Settings**.
2. From the tree in the dialog box that appears, select **Inbound Rules**, and then select **New Rule** in the operation window.
   Follow the instructions displayed in the **New Inbound Rule Wizard** panel to set a protocol port.

Note: You can use **`netstat -a`** command to see used ports. If you find default port numbers in the returned list, change the default port number during installation.

As for the network between JP1/IT Desktop Management and agentless computers, please make sure the following ports are available to pass through.

Port Number	Connection direction	Connection Target[Port Number]	Protocol	Usage
Agentless[445]	<-	Management Server[ephemeral]	TCP or UDP	To connect to File and Printer from Management Server.
Agentless[139]	<-	Management Server[ephemeral]	TCP	To connect to File and Printer from Management Server.
Agentless[137 and 138]	<-	Management Server[ephemeral]	UDP	To connect to File and Printer from Management Server.

Port Number	Connection direction	Connection Target[Port Number]	Protocol	Usage
Agentless[161]	<-	Management Server[ephemeral]	UDP	To connect with SMTP server.

Agent (Port Number)	Connection direction	Connection Target [Port Number]	Protocol	Usage
Agent [31000]	->	Management Server [ephemeral]	TCP	Connect to Management Server from computer
Agent[31001]	<-	Management Server [ephemeral]	TCP	Connect to computer from Management Server
Agent [16992]	<-	Management Server [ephemeral]	TCP	Control power on/off by using AMT

Each port number is set by default at delivery of the product. If the port number (given in the list above) is already used in your system environment, please specify a different port number. Also, if you control the ports in the network between JP1/IT Desktop Management and JP1/IT Desktop Management Agent by firewall, please enable the connection to pass through the ports (given in the list above).

Note: You can set up the Protocol to allow communication through the Windows firewall from Windows **Control Panel > Windows Firewall > Exceptions** panel.

Agent (Port Number)	Connection direction	Connection Target [Port Number]	Protocol	Usage
Controller [31016]	->	Remote Control Agent	TCP	Remote Control
Controller [31017]	->	Remote Control Agent	TCP	File Transfer from Controller to agent
Controller [31018]	-> <-	Remote Control Agent	TCP	Chat
Controller [31019]	<-	Remote Control Agent	TCP	Connection request from agent to Controller
Controller [31020]	<-	Remote Control Agent	TCP	File Transfer from agent to Controller

All port numbers are set to their default values when the product is shipped. If a default port number (shown in the list above) is already used in your system environment, specify a different port number as described below.

- Port number for Controller
  Use the **Options** dialog box in Controller.
- Port number for Remote Control Agent

Use the dialog box that opens by clicking **Remote Control Settings** in the agent settings.

- Port number for the chat facility
  Use the **Connect** tab in the **Options** dialog box in the **Chat** window.

List of port numbers for the site server

The following table lists the port number used by the site server.

Site Server (Port Number)	Connection direction	Connection Target [Port Number]	Protocol	Usage
31010	None	None	TCP	For internal processing of the site server

All port numbers are set to their default values when the product is shipped. If a default port number (shown in the list above) is already used in your system environment, specify a different port number during setup of the site server.

JP1/IT Desktop Management - Manager installation types

There are two installation methods for JP1/IT Desktop Management - Manager. Select the method that best suits your situation.

Quick installation
: This requires minimal effort for installation and setup. Default values are used during installation and setup. We recommend this method unless special settings are required.

Custom installation
: You must specify the settings during the installation. After installation is completed, you need to perform the setup procedure to create a database. We recommend this method if you want to set non-default values during installation and setup.

Installing JP1/IT Desktop Management

Make sure to log into the management server with your administrative permission. Run the setup executable, **setup.exe**, from the provided media to launch the JP1/IT Desktop Management's InstallShield Wizard. After you agree to the terms and conditions, you can select two options to install JP1/IT Desktop Management.

To install JP1/IT Desktop Management:

1. The **setup.exe** launches the **InstallShield Wizard** and displays **Welcome** panel.

2. Click **Next**. The **License Agreement** panel opens with information on software license terms.

Note: To print the license agreement, click **Print**.

3. Read the agreement and select **I accept the terms of license agreement** and click **Next**. Select one of the following two options to install JP1/IT Desktop Management:
    - Quick Installation
    - Custom Installation
4. If you selected **Quick Installation**, follow the instructions and complete the requirements in all six panels of the **InstallShield Wizard**.
5. For information on the **Custom Installation** option, refer to the Custom installation on page 2-18.

Note: You have to create exceptions for JP1/IT Desktop Management and Agent to communicate with each other, in the Windows Firewall settings. If you installed JP1/IT Desktop Management with your Windows Firewall settings Off, make sure you execute **Allow Communication through Windows Firewall** settings command. See Allowing communication through Windows firewalls on page A-2 for details.

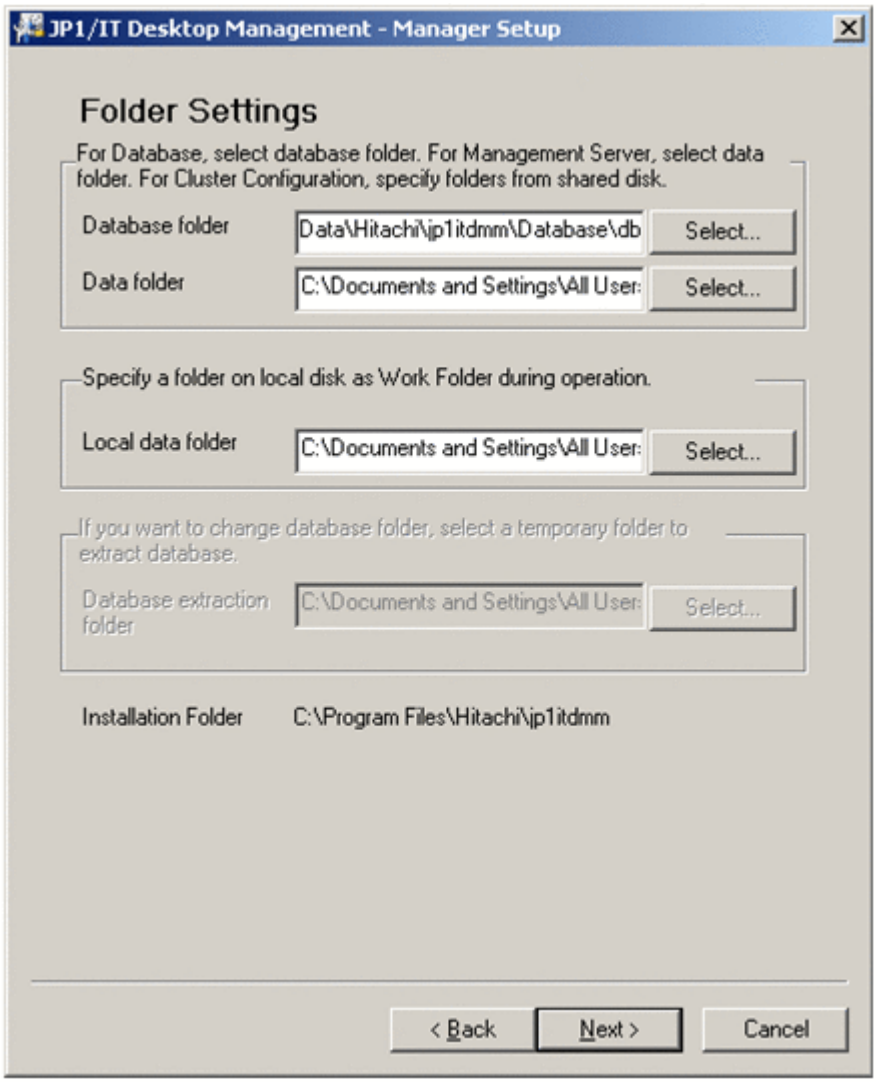
Custom installation

If you selected custom installation, you can customize JP1/IT Desktop Management's setup and environment based on your company's management requirements. You can customize the following settings:

- Specify cluster environment, see Configuring cluster environments on page 2-20.
- Specify folder settings
- Change Operations Log settings
- Change port numbers
- Control network bandwidth
- Change currency unit

Specify Folder Settings

Do the following in the primary server's folder setup window to set up JP1/IT Desktop Management in a cluster environment.



Specify the path for the shared disk in the following items:

- Database folder
- Data folder

Specify the other items (except the ones specified in the window above) in the same way as you would specify other setups.

Changing Operation Logs settings

During Custom installation, you can specify or change the Operation Logs settings such as:

- The number of computers that are used to collect Operation Logs
- Maximum retention period for collected Operation Logs
- Required capacity
- Operation Logs database folder

After installing the product, you can refer to the online help for more details on changing Operation Logs settings.

Changing Port Numbers

During custom installation, **Port Number Settings** Window prompts give you the option to change management server connection and management server's port numbers. You can also change Port Numbers any time after installing the software. Refer to Online Help for detailed information on changing port numbers after installation.

Note:

- The port number you specify here will be used for the URL of the Web Console.
- The first 12 number starting from the specified number will be reserved for management server. For example if you specify 31000, than 31000 to 31012 will be used.
- See List of Port Numbers on page 2-14.

Changing the currency unit and controlling network bandwidth

During custom installation, you can also change the Currency Unit setting in **Currency Unit Setting** and set the maximum transmission speed for distribution in **Control Network bandwidth from a management server**. You can perform all custom installation options even while you are working on JP1/IT Desktop Management.

Configuring cluster environments

Custom installation on page 2-18 also has an option to install JP1/IT Desktop Management in cluster environment.

To configure cluster environment:

1. Select **Custom Installation** and install JP1/IT Desktop Management in **Primary Server** and **Secondary Server**.

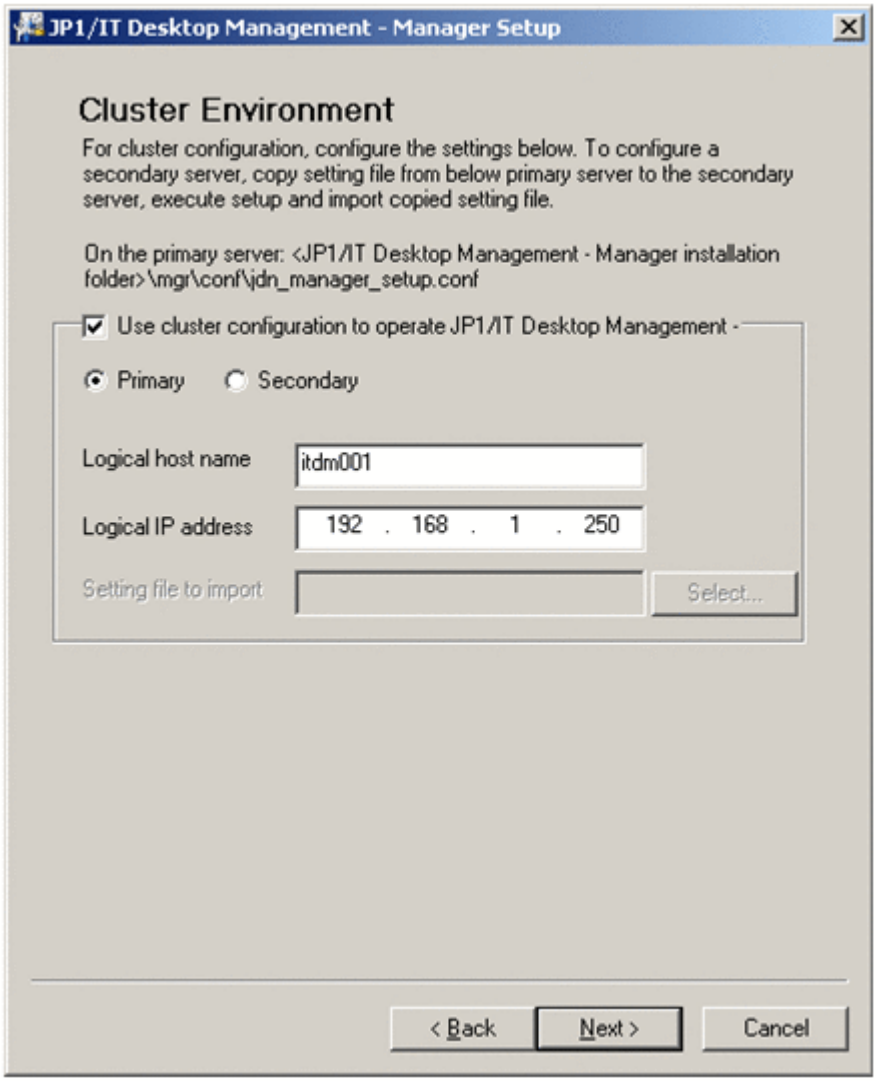
WARNING: Do not run setup.exe after installation completes.

2. Create groups of resources in the **Primary Server**. See Creating group resource in primary server on page A-3 for details.
3. After creating the groups, execute set up on the **Primary Server**.
4. Copy the output file after set up completion from the **Primary Server** to the **Secondary Server**.
5. Move the groups of resources from **Primary Server** to **Secondary server** to execute set up in **Secondary Server**.
6. Move the groups of resources to Primary server to start operations in a clustered environment.
7. Specify online service resources for JP1/IT Desktop Management.

JP1/IT Desktop Management starts operating in a cluster environment.

Setting up JP1/IT Desktop Management in primary server

Setup JP1/IT Desktop Management in the primary (active) server. To operate the cluster system and setup the primary server complete the following:



- Select the check box **Use cluster configuration to operate [ProductName]**.
- Select **Primary**.
- Specify **Logical host name** and **Logical IP address**.
- **Setting file to import** is inactive, you need not select file now.

As you finish the setup, the file will be created in the path shown below. Copy the file to the Secondary server.Installation Folder of JP1/IT Desktop Management\mgr\conf\jdn_manager_setup.conf

After setting up JP1/IT Desktop Management in primary server, you can set it up in the secondary server to operate in cluster environment.

Setting up JP1/IT Desktop Management on a secondary server

To operate JP1/IT Desktop Management in a cluster environment, you can setup JP1/IT Desktop Management in the secondary server (standby) in the same way as the primary server.

Specify the following in the Cluster Environment Window during setup:

- Select [**Use cluster configuration to operate [ProductName]**].
- **Select Secondary**
- In **Setting file to import**, select the file copied from Primary server Setup.

Setting the folder windows settings are the same as other setup tasks. But you cannot specify the following items that are inactive in secondary server.

- Database folder
- Data folder
- Database extraction folder

Note: You are not required to register agents in the secondary server.

JP1/IT Desktop Management's management operations will automatically move to the secondary server in case of any problem in the primary server.

3

Logging in and registration a license

After installing JP1/IT Desktop Management, you need to register a license. If your company has more than one management server, each machine requires a separate license.

Overview

JP1/IT Desktop Management uses the *one-license-per-managed-node* method to control the number of licenses used. In this method, one license is used for a managed device regardless of the device type. This means that as many devices as the number of licenses registered in JP1/IT Desktop Management can be managed. Note that licenses are used for only managing devices, and not used for registering assets.

To register licenses, use the product license key file that was provided when you purchased JP1/IT Desktop Management. If the number of licenses used has reached the maximum number of registered licenses, no more devices can be added. Confirm in advance that you have a sufficient number of licenses.

If the number of devices you want to manage exceeds the number of registered licenses, you need to add more licenses. To add licenses, purchase product licenses and register them.

Launching the login panel

To register a product license, access the login panel.

Figure 3-1 Login panel

Use the host name and port data that you entered during the installation, to specify the JP1/IT Desktop Management URL.

1. Launch your browser.

2. Use this format to go to login panel: *http://hostname:portnumber/jp1itdm/jp1itdm.jsp*

   For example, if your host name is host ITDM and port number 31080, type *http://host ITDM:31080/jp1itdm/jp1itdm.jsp*

   JP1/IT Desktop Management panel opens.

You can also launch login panel from Windows. From the Windows **Start** menu, select **All Programs** > **JP1/IT Desktop Management - Manager** > **Login**. The login panel opens. You have to register your license to login and start using your software.

Note: If you have installed JP1/IT Desktop Management using the **Custom Installation**, specify the port number in the web browser. If you have used **Quick Installation** the default value becomes the port number for the browser.

Overview of product licenses

JP1/IT Desktop Management uses the *one-license-per-managed-node* method to control the number of licenses used. In this method, one license is used for a managed device regardless of the device type. This means that as many devices as the number of licenses registered in JP1/IT Desktop Management can be managed. Note that licenses are used for only managing devices, and not used for registering assets.

To register licenses, use the product license key file that was provided when you purchased JP1/IT Desktop Management. If the number of licenses used has reached the maximum number of registered licenses, no more devices can be added. Confirm in advance that you have a sufficient number of licenses.

If the number of devices you want to manage exceeds the number of registered licenses, you need to add more licenses. To add licenses, purchase product licenses and register them.

If devices are automatically registered as managed devices during discovery and there are not enough licenses, the devices are handled as *discovered nodes*. Although the discovered nodes are displayed on the **Discovered Nodes** panel displayed by selecting **Discovery** in the **Settings** panel, they are not management targets (no licenses are used). You can reduce the number of licenses in use by excluding nodes from management or by deleting nodes.

Tip: In an OS muiltiboot environment, because the information reported to the management server is different for each OS, each OS is handled as a separate device.

Tip: To use the network access control facility, register all computers permitted to connect to the network as management targets. Devices other than computers do not need to be registered as management targets.

Tip: To use the remote control facility, register the devices that will be subject to remote control as management targets.

Registering licenses

By registering licenses in JP1/IT Desktop Management, you can manage devices up to the number of registered licenses.

To register a license:

1. Open the login panel.
2. Click the **License** button.
3. In the dialog box that opens, click the **Register License** button.
4. In the dialog box that opens, select the license key file and click the **Open** button.

License registration has finished.

Tip: Except for the initial registration, you can also register licenses in the **License Details** panel that is opened by selecting **Product Licenses** in the **Settings** panel. Click the **Register License** button. In the dialog box that opens, select the license key file and then click the **Open** button to finish license registration.

Tip: Except for the initial registration, you can also register licenses in the **License Details** dialog box that is opened by clicking **Help** in the top-left corner of the screen, and then clicking **About**. After that, click **Register License**. In the dialog box that opens, select the license key file and then click the **Open** button to finish license registration.

4

Completing the initial setup

After the registration of a product license has finished, you can log in to the application using the default user account credentials. The first time you log in, be sure to create a new user ID and password for yourself.

Overview

JP1/IT Desktop Management includes a built-in user account. You will use the built-in user account credentials for initial login. At your first log in you will be prompted to change the password. After changing the password, you can set up your own user account and user accounts for any other administrative users who will use the software.

The built-in user account cannot be deleted. Following are the built-in user account credentials:

- **User ID**: *system*
- **Password**: *manager*

Notes on passwords

Following are important points to remember on password specification for any user account you create in JP1/IT Desktop Management:

- Passwords are valid for 180 days. You get password change notification at log in time during the last 7 days.
- Passwords are case sensitive and should have the following:
  - Upper case or lower case alphabet, numbers or English symbols.
  - Should be 8 to 32 characters long.

Note:

- Do not use a character string with all same characters (11111111111 or aaaaaa)
- The User ID cannot be used for the password.
- When changing passwords, do not reuse the existing password.

Setting up user accounts

If you have more than one administrator who will be working on the management process in JP1/IT Desktop Management, you have to create separate user accounts for each user. You have the flexibility to add, edit or remove any user accounts, except the built-in account, at any time.

Note: Built-in user account and administrative user accounts are different. You can add/edit and delete any of the administrative user accounts. But built-in user account remains in the system with administrative permission. See User Management - Default account values on page A-7 for default account values. For more details on built-in user account refer to online help

To add an user account:

1. Click on **Settings** to go to **Settings Menu> User Management> Account Management** and click **Add New User**.

   Add New User dialog box opens.

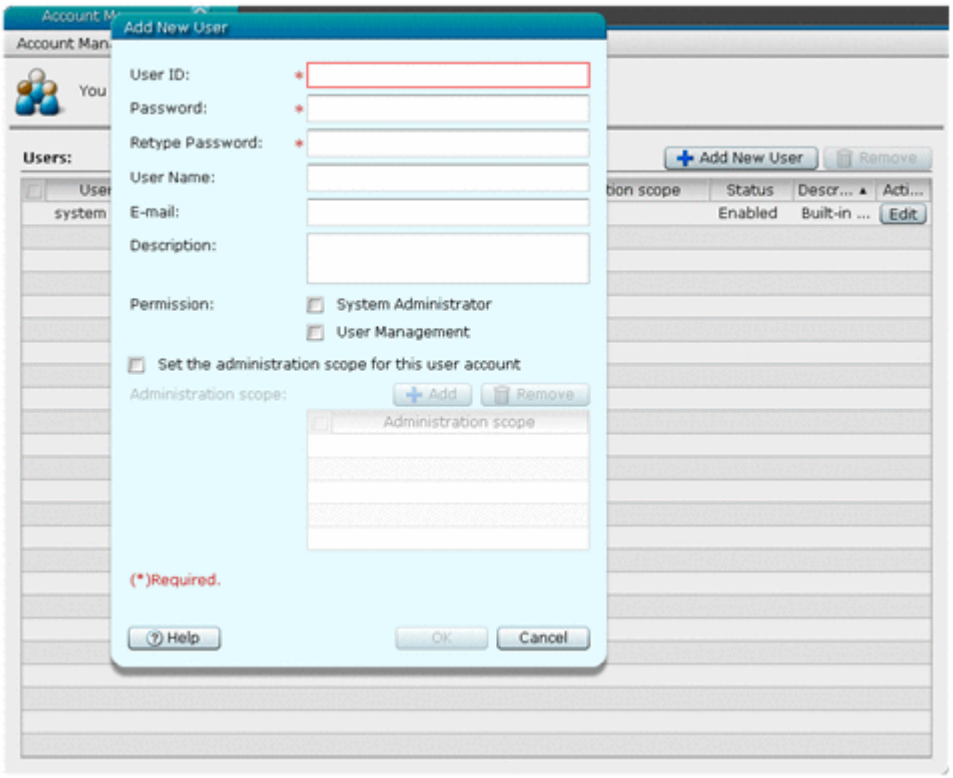


Figure 4-1 Add New User dialog box

2. Enter the user details, such as **User ID**, **Password**,**User Name**, **E-mail** and select appropriate permission in the check box.
3. Click **OK**.

   JP1/IT Desktop Management saves the user information to the users list and displays the details. Added users can access information or start managing devices in JP1/IT Desktop Management.

Assigning user permissions

While registering or adding new user accounts, assign access permission based on user role. Administrative users and Business users will have different set of access permissions. Administrative access permissions will vary based on roles of system administrator or business managers. System administrator will have the most access permissions.

- **System Administrator permission**: Permission for performing all operations except registering, editing and deleting user accounts.
- **User Management permission**: Permission for only registering, editing and deleting user accounts.
- **View permission**: Permission for viewing and outputting (printing) all information except system setting information.

The following table explains the types of users and their access permission:

User	Access Permission
System administrator	• **System Administrator** permission. • **User Management** permission.
Business user	**View** permission

Note:

- If you do not select any user permission (**System Administrator** and **User Management**) for the user account, in **Permissions** field, the created user will have only View permission.
- Business managers with View permission will only have access to **Home** and **Reports** modules in JP1/IT Desktop Management.
- You can create an user account with only **User Management** permission.

Setting up automatic product updates

JP1/IT Desktop Management gives you an option to enable automatic product updates. When you enable automatic product update, you can receive up to date information on judging security policy adherence and receive new Windows updates from Microsoft Corporation. To enable product update, the Proxy server settings is also required.

To specify settings automatic product updates:

1. From **Settings > Settings menu > General > Product Update**, select the **Enable Product Update** check box. Fill in required information in the given fields.

Note: Product Update provides you the ability to collect patch information to monitor individual, selected patch information in **Security Policy**. If you do not want to monitor the patch information automatically, you can uncheck the **Enable Product Update** check box, to disable monitoring automatic patch updates.

2. Select **Use Proxy Server** check box. Fill in required information in the given fields.
3. Click **Test** to check the connectivity.
4. **Apply** button gets enabled after filling in the details. Click **Apply** to apply the settings.

   After enabling proxy server settings, you can select the required **Windows Updates** from **Security** module. For more information on setting up Windows Updates, refer to online help.

JP1/IT Desktop Management automatically gets product update information and determines security status of each managed target computer based on it.

Tip: After information is acquired from the Support Service site and the security policy is updated, the security status of each device is evaluated.

Introducing JP1/IT Desktop Management

After you login, you will see JP1/IT Desktop Management's **Home** module dashboard. At every login you go to **Home** module by default. At your first login, you see the **Getting Started Wizard** option open. Clicking on **Getting Started**, takes you to **What is this Wizard?** panel. You can continue clicking through this wizard to start the first step for management, the discovery process.

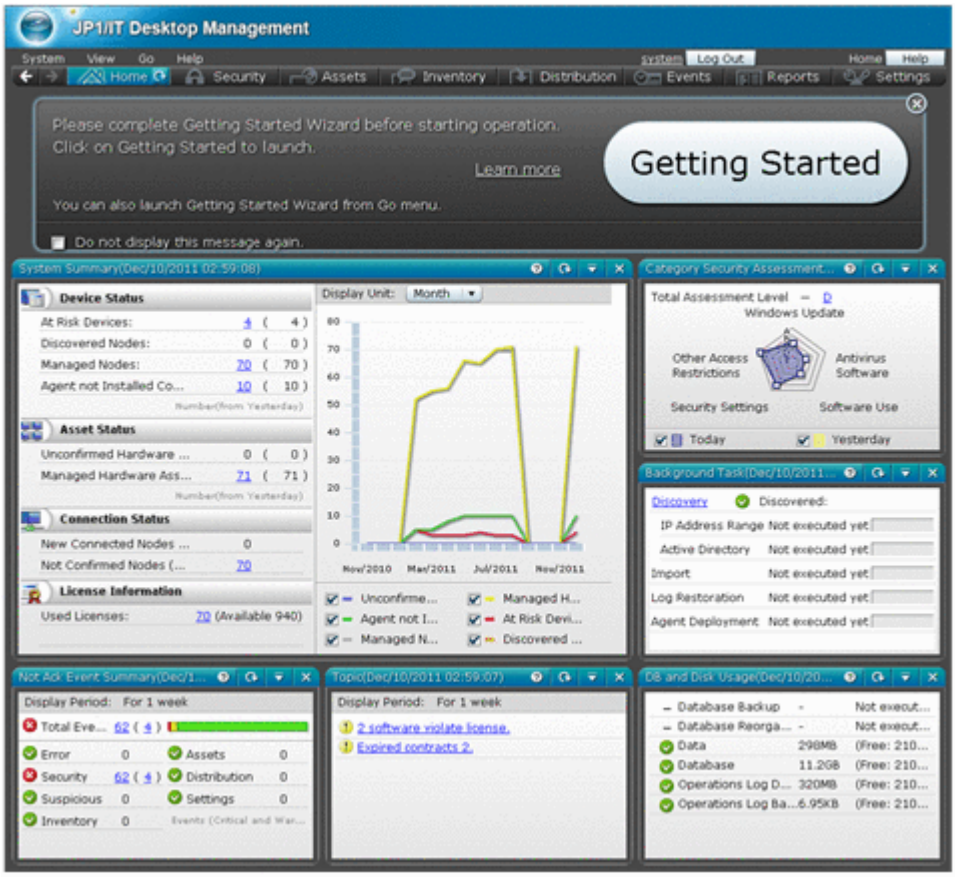


Figure 4-2 JP1/IT Desktop Management Home page

Desktop components

Your JP1/IT Desktop Management's desktop is designed in such a way that it is easy to navigate, manage and access required information at any given time in the management process. The image below introduces some of the terms referred frequently in this document and online help when referring to JP1/IT Desktop Management's navigation components.

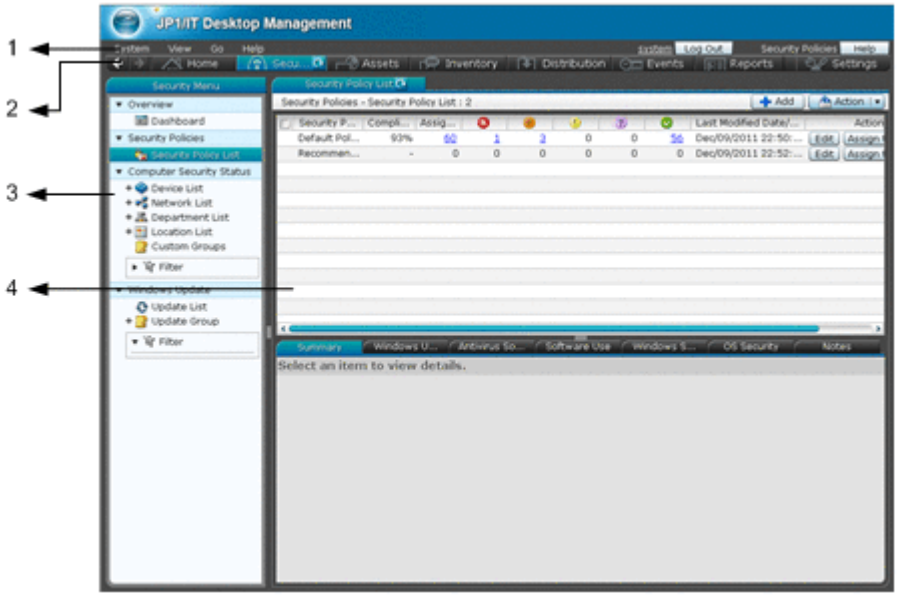


Figure 4-3 JP1/IT Desktop Management Desktop components

Desktop components

Item	Name
1	**Menu bar**: This menu bar has the following options: • **System**: Contains **Logout** option to end the session. • **View**: Lists the **Panel Layout** to select panels view, **Option** with **History** and **Selection Item** and **Change View Default** options. • **Go**: Lists the options to navigate to **Getting Started Wizard** and **Change Profile** dialog box. • **Help**: Lists the **JP1/IT Desktop Management Help**, **JP1/IT Desktop Management Site Map**, **Update**, **About**, and**Version Information** options.
2	**Module**: Contains the active navigation buttons for the JP1/IT Desktop Management modules **Home**, **Security**, **Assets**, **Inventory**, **Distribution**, **Events**, **Reports** and **Setting**.
3	**Module menu**: This area shows the key resources that are associated with the selected module. When you make a selection from the menu, details about it are displayed in the information area.
4	**Information area**: This area changes depending on the selected module and your selection from the module menu. Depending on your permissions and the options that are available based on the selected menu item, you may also be able to add, edit, or delete data.

For more detailed information about navigating in JP1/IT Desktop Management, refer to online help.

Referring to online help

JP1/IT Desktop Management's **Help** system provides you a comprehensive overview of all available functionalists and detailed procedures to perform all related tasks. The online help gives you detailed procedures and related information with active links to go back and forth based on your requirements while performing any task. Also an active **Help** button within the panels and dialog boxes provides you context sensitive help. Context sensitive help gives you the specific information related to the task you perform in the dialog box or panel.

5

Preparing for management

The Getting Started wizard provides options to discover the nodes you want to manage with JP1/IT Desktop Management.

After discovery, you can manage the nodes with or without an agent in JP1/IT Desktop Management. When you manage with an agent, you can utilize all available aspects of management from JP1/IT Desktop Management. To manage with an agent, you will install an agent in the discovered nodes.

Overview

When you log into JP1/IT Desktop Management for the first time, you will see the **Getting Started** button in the **Home** module.

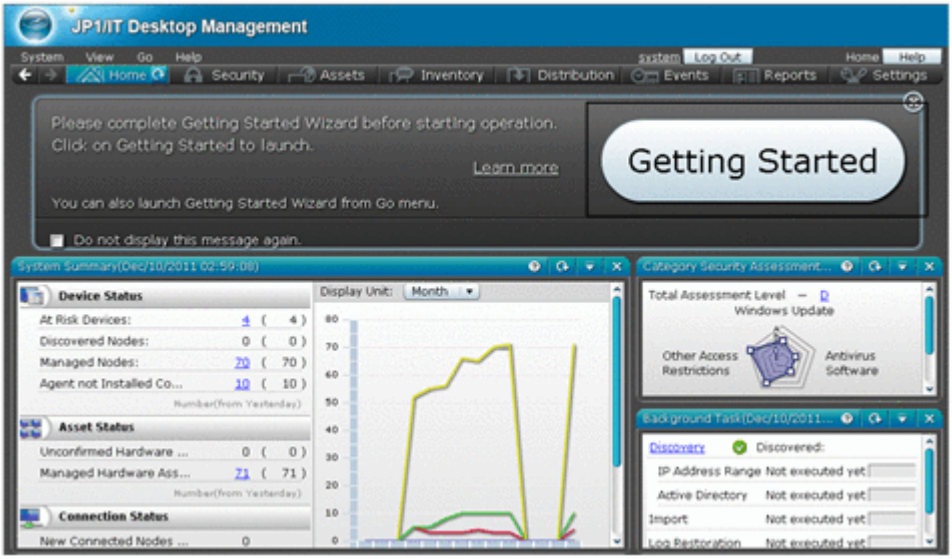


Figure 5-1 Getting Started

The **Getting Started Wizard** with self explanatory panels, will guide you through configuring the discovery process. When you configure the discovery for the first time, you can use the default agent configuration to install agent in the discovered devices. You can also create a new agent installer. But, if you only want to discover the nodes and not install agents now, when you specify the discovery configurations, in **Specify Discovery Option** panel, do not select **Auto-Manage Discovered Nodes** or **Auto-Install Agent** options. You can install agents on the nodes later.

Notes on discovery prerequisites

The following information provides you the explanation about the Active Directory and IP address range discovery prerequisites.

Active Directory discovery

In Active Directory discovery, the credential information, **User ID** and **Password**, are used to authenticate computer. So, to discover all computers, make sure you do the following:

- Define the credential information in all computers.
- Specified user should have Administrator privileges.

JP1/IT Desktop Management must be able to resolve address for computer's host name that is obtained from Active Directory by discovery, at management server. There are two ways to resolve the address:

- Resolve the address for computer's host name that is obtained from Active Directory at the DNS where JP1/IT Desktop Management manager is connected.
- Make sure the JP1/IT Desktop Management Management server belongs to the Active Directory domain.

IP Address Range discovery

In the IP Address Range discovery, JP1/IT Desktop Management can discover devices only by using ARP and ICMP. To collect the device details from discovered devices, JP1/IT Desktop Management should access the discovered devices using SNMP or Windows Administrative share.

Discovery credential information specified in IP address range discovery is also used to deploy agents to the discovered devices. If you want to deploy agent after discovery, specify the Windows Administrative Share credential information for target IP address range in **Settings > Discovery > Configurations > IP Address Range**.

Windows computers

- **Windows firewall setting**: If Windows Firewall is enabled in target computers, in Windows Firewall setting, make sure **File and Printer Sharing** is selected in Exceptions tab.
- **Simple file sharing (for XP)**: Simple file sharing should be disabled. You can see this option from target computer's **Explorer > Tools > Folder Options > View** tab. Make sure the **Use simple file sharing (Recommended)** is not selected.
- **Administrative share**: ADMIN$ is enabled. You can check whether ADMIN$ is enabled using net share command at the Windows command prompt. To enable ADMIN$, execute **`netshareADMIN$`** at the Windows command prompt.

  At the time of discovery, if the log on authentication with Administrative right is specified, JP1/IT Desktop Management can find the device type and collect most of the device details. You can also deploy and install agent in these computers.
- **Shared resource**: IPC$ is enabled. You can check whether IPC$ is enabled using net shared command at the Windows command prompt. Usually IPC$ is enabled.

SNMP nodes

- **IP Address**: This is the address of the SNMP node.
- **Port Number**: The port number where the SNMP node waits for the communication. The default setting is UDP/161.
- **Community Name**: This is the Community name used for SNMP nodes. The default setting is public.

  At the time of discovery, if the specified Community Name matches, JP1/IT Desktop Management can find the device type and collect part of device information.

Notes on discovery credential information

After discovering the devices, JP1/IT Desktop Management collects the device details for management purposes. To collect device details JP1/IT Desktop Management should access the devices using the credential information. So you have to specify the credential information for the target devices when you specify the discovery schedule.

Note: Both in Active Directory Discovery and IP Address Range discovery, if target computer's OS is Windows Me, Windows 98, Windows 95, or Windows NT 4.0, its device type could become Unknown when discovered.

Discovering nodes by Active Directory

Active Directory discovery collects the device information based on devices that are registered in the Active Directory domain. Discovering nodes by using Active Directory domain information is one of the two options to discover the status of all IT devices before agent installation.

To discover nodes by Active Directory domain information:

1. Click **Go > Getting Started Wizard**. The **What is this Wizard?** panel opens.
2. Click **Next** to open **Select How to Get Started** panel.
3. **Select Discover Nodes** and click **Next** to open **Select How to Discover Nodes** panel.
4. **Select Discovery from Active Directory** and Click **Next** and go to **Specify Active Directory Domains** panel.
5. Enter information in the required fields, about the **Active Directory domain** which you want to discover the status and click **OK**.

Note:

- **Domain Name:** This is the Domain name of Active Directory.
- **Host name:** This is the Active Directory host name.
- **User ID:** User who is registered to Active Directory and has Domain Administrator right.
- **Password:** This is the password that is associated with the User ID.
- **Root OU:** Root OU (Organization Unit) of Department information in Active Directory. Computers existing under this root OU will be the discovery target. Specify the Root OU in the following format: <Domain Name>/<OU>/<OU>

  For example: If the domain name is **hitachi.com** and the OU is **Unit 1**, the root OU will be **hitachi.com/Unit 1**

Also if you have a built-in folder as **Computers**, you cannot use it to connect as Root OU.

6. Click **Next** to open **Specify Discovery Schedule** panel.

Note: If you check mark **Discover Immediately** check box, the discovery process starts immediately, right after completing the **Discovery Wizard**.

Specify the date, time and day, and click **Next**, and open **Specify Discovery Option** panel.

7. Check mark **Auto-Manage Discovered Nodes** and if necessary **Auto-Install Agent** check boxes ON and click **Next**.
8. In **Set Discovery Notifications** panel, enter e-mail address to receive discovery completion notification, specify **SMTP Server Settings** and click **Next**.
9. In **Confirm Content and Finish Settings** panel, verify the settings and click **Complete**. The **Discovery Settings Configured** panel appears.
10. Click **Discovery Log**. you can view the discovered devices and select to manage devices from the displayed list.

    Or you can Click **Close** to close and exit the **Discovery from Active Directory Wizard** and start the discovery process.

    You will receive an e-mail notification when discovery process is completed. If you have selected **Auto-Install Agent** in **Specify Discovery Option** panel, JP1/IT Desktop Management will install the assigned agent in the discovered device for management.

You can view the **Active Directory** discovery log in **Settings >Settings Menu > Discovery > Last Discovery Log > Active Directory**. From here you can select **Go to Discovered Nodes** for further management options.

Discovering nodes by IP address range

Discovering nodes using IP address range is another option to determine the status of devices connected to your network. IP address range discovery discovers and collects information from the nodes based on the specified IP address range. JP1/IT Desktop Management discovers all IT devices, including file servers, PCs, printers, and network switches, that are within a specified address range and that are connected to the network.

Prerequisites for performing IP address range discovery:

- Network IP range.
- Node credentials.

To discover nodes by specified IP address range:

1. On the menu bar, click **Go > Getting Started Wizard**. The **What is this Wizard?** panel opens.
2. Click **Next** to open **Select How to Get Started** panel.
3. **Select Discover Nodes** and click **Next** to open the **Select How to Discover Nodes** panel.
4. Select **Discovery from IP Address Range** and click **Next** to go to **Discovery from IP Address Range** panel.

5. Click **Add IP Address Range** to launch **Add IP Address Range** dialog box.
6. Enter **Discovery Range Name** and **IP address range** and click **OK.**
   JP1/IT Desktop Management adds the IP address range to discovery list.
7. Click **Next**. The **Specify Credentials** panel opens. See Notes on discovery credential information on page 5-4 for details on the credential information.
8. Click **Add Credential** to launch **Add Credential** dialog. Enter credential information and click **OK**.
   Your credential information is included in Discovery list.
9. Click **Next**. The **Associate Credentials** panel opens.
10. Assign the credential information for each IP address range and click **Next**.

WARNING: Make sure to assign credential information for each IP address range. Some target computers might have account lock enabled, to lock the account after few successive unsuccessful log on. If you select **Any**, JP1/IT Desktop Management will try to authenticate the target computers with all credentials and the account in the target computer might get locked without the user's knowledge.

Caution: If you select **All**, JP1/IT Desktop Management attempts to access the device by using each authentication information item. This increases the number of transmissions and the load on the network. Be sure to consider the extra load on the network before selecting this option.

11. In **Specify Discovery Schedule** panel set discovery schedule and click **Next.**

Caution: If you select the **Intensive Discovery** check box, the next discovery starts immediately after the current discovery ends. As a result, a heavy load is put on the network during the discovery phase. Be sure to consider the extra load on the network before selecting this option.

Note: If you check mark **Discover Immediately** check box, the discovery process starts immediately, right after completing the **Discovery Wizard**. If you want to repeat discovery, you can check mark **Intensive Discovery**.

12. In **Specify Discovery Option** panel check mark **Auto-Manage Discovered Nodes** and if necessary **Auto-Install Agent** check boxes **ON** and click **Next**.
13. In **Set Discovery Notification** panel, enter your e-mail to get discovery completion notification, specify **SMTP Server Settings** and click **Next**.
    You see **Confirm and Finish Settings** panel.
14. Make sure the entered settings are right and click **Complete**. The **Discovery Settings Configured** panel opens.
15. Click **Discovery Log**. you can view the discovered devices and select to manage devices from the displayed list.

Or you can click **Close** to close and exit the **Discovery from IP Address Range** wizard and start the discovery process. If you have selected **Auto-Install Agent** option in **Specify Discovery Schedule** panel, JP1/IT Desktop Management installs agent in the discovered devices.

You can view the **IP Address Range** discovery log in **Settings >Settings Menu > Discovery > Last Discovery Log > IP Address Range**. From here you can select **Go to Discovered Nodes** for further management options.

After discovery

Discovery process takes place based on the specified schedule. After the discovery, you can view a list of the discovered nodes from **Settings** module, **Discovery > Discovered Nodes**.

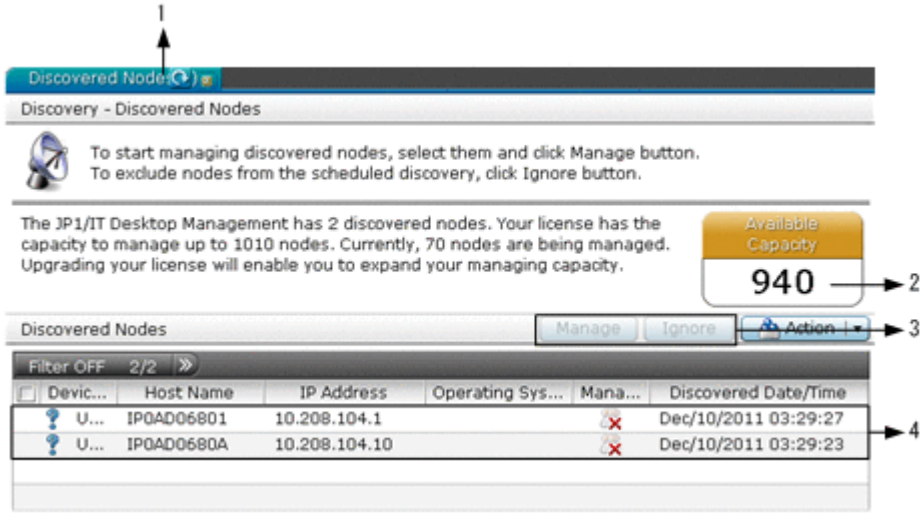


Figure 5-2 Discovered Nodes panel

Discovered Nodes panel

Item	Description
1	Displays the total number of discovered nodes in the current discovery.
2	Shows available management capacity for your software license.
3	You can select the nodes and select the option to **Manage** or **Ignore** the nodes.
4	List of discovered nodes with discovery details.

For more detailed options that you can perform in this panel, refer to the Online Help.

Agent and agentless management

After discovering devices, you can begin management with or without an agent. For JP1/IT Desktop Management's agent and agentless management capacity, refer to Agent and Agentless management capacity on page A-7 in Appendix.

Installing agents

JP1/IT Desktop Management's Agent gives you complete management capacity. With an agent in the managed nodes you can define and apply security policies, distribute, install and uninstall software and remote control computers for troubleshooting and management. To install agent in the discovered nodes, you have to do the following:

- Create an agent installer
- Deploy and install agent in the selected nodes

Creating agent installer

Agent installer is the combination of agent configuration and installation command. You can either use the default agent configuration or specify a customized configuration based on your management requirements.

To create an agent installer:

1. From the **Menu** bar, click **Go > Getting Started Wizard**. You see **What is this Wizard?**
2. Click **Next** to open **Select How to Get Started** panel.
3. Select **Create Agent Installer** and click **Next**.
4. In **Select Agent Configuration**, set **Agent Configuration Name**, specify **Installation Folder** and click **Create**.

Note: You can also specify the account to install agent in target devices.

You get a pop up window with a message that prompts you to save the Agent Installer file and close that window after saving.

5. Click **Save**, to save agent installer on your desktop. Now you see **Complete Agent Installer** wizard.
6. Click **Close** to close the wizard.

You have created the agent installer to distribute agent to the devices you want to manage with JP1/IT Desktop Management.

Agent deployment and installation

After configuring your agent, you can deploy and install the agent to the target devices in the following two ways:

Automatic installation: You can push install agent in the selected nodes. To install agent automatically in the selected nodes, select the **Auto-Install**

Agent check box in **Specify Discovery Option** panel while specifying discovery schedule in Discovery Wizard. JP1/IT Desktop Management automatically installs agent after discovery and starts managing the nodes.

Manual installation: To install agent manually, you will create an agent installer set and then follow one of the following five methods to install agents in discovered nodes:

- **Installing agents by domain**: Distribute and install agent by selected active directory domains.
- **Installing agent by user**: E-mail agent installer to the users and request them to download and install agents in their computers.
- **Installing agent by department**: Contact each department's system administrators and instruct them to distribute agent within their departments.
- **Distributing agent by web portal**: Upload agent configuration in the web portal and instruct the users to download and install.
- **Installing agent by CD**: In special circumstances, copy agent configuration in CD ROM and install in target devices.

For further details on agent deployment and distribution, refer to Online help.

Agentless management

You can manage the discovered nodes without an agent. But in agentless management you will have certain limitations. Automatic enforcement of security policies and software or file data distribution is not possible without an agent installed on managed devices. Refer to Agent and Agentless management capacity on page A-7 for the limitations on Agentless management.

Brief introduction to JP1/IT Desktop Management's features

JP1/IT Desktop Management allows an administrator to take charge of the IT environment by delivering an easy to use, integrated solution for tracking assets, distributing or removing software, and managing security. The combination of these features in a single package is what allows the software to efficiently provide protection and control in an IT environment. With JP1/IT Desktop Management, you can efficiently manage security policies, network access, IT assets, distribution and generate management reports. The following table lists the major features and functions available in JP1/IT Desktop Management.

Feature	Functions
Security management	• Assign, define and customize security policies • Monitor security status • Review operations log • Acquire and distribute Windows Updates • Control the network access

Feature	Functions
Assets management	• Hardware assets • Software licenses • Software assets • Contracts (hardware and software license contracts)
Inventory management	• Device inventory • Software inventory • Remote control
Distribution Management	• Distribute software packages • Distribute file data • Uninstall software
Monitor and manage events	**Events** module provides list of all security and error events captured by the management system with appropriate status message such as: • **Critical** • **Warning** • **Information**
Generate management reports	Generate reports under the following categories for viewing and printing: • **Summary Reports** • **Security Diagnosis Reports** • **Security Details Report** • **Inventory Details Report** • **Assets Details Reports**

Other notable features

With JP1/IT Desktop Management in your IT Operations management you can

- Specify settings to receive email alerts or critical issues and fix security violations
- Save cost and time with remote control to troubleshoot agent computers from anywhere
- Record and play back remote sessions and covert the recording to AVI file to use for training purposes
- Use chat, when the remote control user's phone is busy, to share information

6

Setting up system configurations

This chapter describes how to set up each system configuration.

Setting up an agentless system

This section describes how to set up an agentless system.

Flow of setting up an agentless system

To set up an agentless system, you must first set up the management server, perform discovery, and then register the discovered nodes as management targets.

1. Set up the management server.
2. From the operation window, perform discovery for the network to find nodes.

   If you want to manage all devices, you can specify the discovery settings so that discovered nodes are automatically registered as management targets. In this case, go to step 4.
3. Register the discovered nodes as management targets.
4. Specify the settings to periodically update device information.

Setup of the agentless system is completed.

Tip: If you want to set up a system in which a computer containing an agent and a computer without an agent co-exist, set up the basic system and then start the above procedure from step 2.

Related Topics:

- After discovery on page 5-7

Setting up a site server system

This section describes how to set up a site server system.

Flow of setting up a site server system

To set up a site server system, you must first set up the basic system, set up the site server, and then configure the server for the system.

1. Set up the basic system.
2. Install the site server program on the computer on which an agent has been installed, and then set up the program.
3. In the operation window, configure the server.

Setup of the site server system is completed.

Related Topics:

- Setting up the site server on page 6-5

Installing a site server program

There are two installation methods for a site server program. Select the method that best suits your situation.

Installation from the provided media

You must specify settings on the target computer to proceed with the installation. After installation, you need to perform the setup procedure. We recommend this method if you want to set non-default values during installation and setup.

Installation from the operation window

From the operation window displayed on the administrator's computer, select a computer and then install the program. The default values are set during installation and setup. We recommend this method unless special settings are required.

Tip: When the site server program is installed, a message appears at the top of the home window and on the **Notice** panel.

Installing the site server program from the provided media

To install the site server program, you need to log on to a computer containing an agent as a user with Administrator permissions.

Caution: When you install the program on a Windows computer that supports user account control (UAC), a dialog box that prompts you to promote your permissions might appear. If this dialog box appears, promote your permissions.

Caution: Do not shut down the OS during installation. If you do so and try to re-install the program later, the program might not run normally.

Tip: The site server program cannot be installed on the management server.

To install the site server program from the provided media:

1. Insert the provided media into 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 for starting 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, specify the installation folder, and then click the **Next** button.
6. A confirmation dialog box opens. Confirm that there are no problems with the installation settings, and then click the **Install** button.

Installation is performed. If you find a problem in the installation settings, click the **Back** button and correct the settings.

7. When the installation process is completed, click the **Finish** button.

Installation of the site server program is completed. If a message that prompts you to restart your computer appears, restart the computer.

After installation is completed, you need to perform the setup procedure to create a database. If you have selected the **Setup** check box upon completion of the installation, the setup process is automatically started after installation is completed.

Installing the site server program from the operation window

From the **Device** window, you can select a computer on which an agent is installed, and then install the site server program.

Caution: Do not shut down the OS during installation. If you do so and try to re-install the program later, the program might not run normally.

Tip: To install the site server program from the **Device** window, the component (site server program) must be registered with the management server in advance.

Tip: The site server program cannot be installed on the management server.

To install the site server program from the operation window:

1. Display the **Device** window.
2. From **Device Information**, select the list of devices that contains the computer you want to install the site server program on. The list of devices is displayed in the Information area.
3. In the Information area, select a computer on which an agent is already installed.
4. Select **Install Site Server Program** from **Action**.
5. In the **Install Site Server Program** dialog box, click **OK**.

The site server program is installed on the selected computer. To install site server programs on multiple computers, repeat the above steps.

For the computer on which the site server program is installed,  is displayed for the management type.

Tip: For the computers on which the site server program is installed, access denial by network access control is suppressed. A site server computer is also automatically registered as an exclusive communication target. However, if you install the site server program on a computer whose connection is already blocked, the computer is not permitted to be connected to the network.

Setting up the site server

After installing the site server program from the provided media, you need to set up the site server by creating a database and specifying environment settings.

To set up the site server:

1. From the Windows **Start** menu, select **All Programs** > **JP1_IT Desktop Management - Remote Site Server** > **Setup**.
2. In the **Setup** window, click the **Next** button.
3. In the **Select a Setup** window, select the type of setup, and then click the **Next** button.

   This window is not displayed for the initial setup after installation.
4. In the **Folder Settings** window, specify the folder types that the site server program will use, and then click the **Next** button.
5. In the **Port Number Settings** window, specify the port number that the site server program will use, and then click the **Next** button.
6. In the **Other Settings** window, specify whether to enable flow control when the distribution facility is used, and then click the **Next** button.
7. In the **Confirm Setup Settings** window, confirm that there are no problems with the setup settings, and then click the **Next** button.

   Setup is performed. If you find a problem in the setup settings, click the **Back** button and correct the settings.
8. When the setup process is completed, click **OK**.

Setup is completed and the site server runs with the specified settings.

Tip: If you run the setup program immediately after installation, a database will be created during setup.

Setting up a Windows update management system

This section describes how to set up a Windows update management system.

Flow for setting up a Windows update management system

To set up a Windows update management system, you must first set up the basic system, and then specify the information necessary for connecting to the Support Service site.

1. Set up the basic system.
2. Enter the information necessary for connecting to the Support Service site into the window.

Tip: To determine whether Windows updates are applied and automatically take action according to determination results, you need to specify the security policy settings.

Setup of the Windows update management system is completed.

Related Topics:

- Setting up automatic product updates on page 4-4

Setting up an Active Directory linkage system

This section describes how to set up an Active Directory linkage system.

Flow for setting up an Active Directory linkage system

To set up an Active Directory linkage system, you must connect Active Directory to the network and the computers registered with Active Directory as management targets.

1. Set up the management server within the system in which Active Directory has been installed.
2. Specify the information necessary for connecting JP1/IT Desktop Management to Active Directory.
3. If necessary, specify the settings so that the information items managed by Active Directory are acquired as additional management items.
4. Perform discovery to find the computers registered in Active Directory.
   If you want to manage all devices, you can specify the discovery settings so that discovered nodes are automatically registered as management targets. Similarly, it is also possible to simultaneously perform discovery and automatic agent deployment. Perform steps 5 and 6, if necessary.
5. Register the discovered computers as management targets.
6. Install an agent on each computer that is to be managed.

Setup of the Active Directory linkage system is completed.

Related Topics:

- Discovering nodes by Active Directory on page 5-4

7

Re-installing products

Installing a program that has the same version number but a revision number that is different from the revision number of the installed program is called *re-installation*.

This chapter describes how to re-install JP1/IT Desktop Management - Manager, agents, the site server program, and network access control agents.

Re-installing JP1/IT Desktop Management - Manager

JP1/IT Desktop Management - Manager can only be overwritten if the version number of the product to be installed is the same as, and the revision number is the same as or later than, the existing installed product. Re-installation requires at least 2.4 GB of free space on the hard disk.

Caution: Before starting re-installation, log out of JP1/IT Desktop Management and close the operation window. If you start re-installation with the operation window open, the operation window might not be displayed correctly after installation.

Caution: When you install the product on a Windows computer that supports user account control (UAC), a dialog box that prompts you to promote your permissions might appear. If this dialog box appears, promote your permissions.

Caution: Do not shut down the OS during installation. If you do so and try to re-install the program later, the program might not run normally.

To re-install JP1/IT Desktop Management - Manager:

1. Insert the provided media into 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 for starting installation, click the **Next** button.
4. After checking the information displayed in the **License Agreement for Usage** dialog box, select **Accept the conditions of license agreement for usage**, and then click the **Next** button.
5. In the dialog box indicating that the installation is ready, check the displayed information and then click the **Install** button.

   Installation is performed. For a cluster configuration, if necessary, a dialog box that prompts you to stop the services appears. Follow the instructions shown in the dialog box.
6. In the dialog box indicating the completion of the installation, specify the settings related to component updates, and then click the **Finish** button.

Tip: If upgrading the database is required, the **Setup** check box for starting the setup process is displayed in the dialog box that indicates the completion of re-installation. Select this check box or start the setup process from the **Start** menu. After doing so, component-related settings are displayed in the dialog box that indicates the completion of setup.

Re-installation of JP1/IT Desktop Management - Manager is completed. If a message that prompts you to restart your computer appears, restart the computer.

Related Topics:

- How to update components on page 7-5

- Custom installation on page 2-18

Re-installing agents from the provided media

An agent can only be overwritten if the version number of the product to be installed is the same as, and the revision number is the same as or later than, the existing installed product.

Caution: When you install the product on a Windows computer that supports user account control (UAC), a dialog box that prompts you to promote your permissions might appear. If this dialog box appears, promote your permissions.

Caution: Do not shut down the OS during installation. If you do so and try to re-install the program later, the program might not run normally.

To re-install an agent:

1. Insert the provided media into the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/ IT Desktop Management - Agent** and then click the **Install** button.
3. In the dialog box for starting installation, click the **Next** button.
4. In the dialog box indicating that installation is ready, click the **Install** button.

   Installation is performed.
5. In the dialog box indicating the completion of installation, click the **Finish** button.

Re-installation of the agent is completed. If a message that prompts you to restart your computer appears, restart the computer.

Re-installing a site server program from the provided media

A site server program can only be overwritten if the version number of the product to be installed is the same as, and the revision number is the same as or later than, the existing installed product.

Caution: When you install the program on a Windows computer that supports user account control (UAC), a dialog box that prompts you to promote your permissions might appear. If this dialog box appears, promote your permissions.

Caution: Do not shut down the OS during installation. If you do so and try to re-install the program later, the program might not run normally.

To re-installation a site server program:

1. Insert the provided media into 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 for starting installation, click the **Next** button.
4. In the dialog box indicating that installation is ready, click the **Install** button.

   Installation is performed.
5. In the dialog box indicating the completion of installation, click the **Finish** button.

Re-installation of the site server program is completed. If a message that prompts you to restart your computer appears, restart the computer.

Re-installing a network access control agent from the provided media

A network access control agent can only be overwritten if the version number of the product to be installed is the same as, and the revision number is the same as or later than, the existing installed product. You also need to log on to the OS as a user with Administrator permissions.

Caution: When you install the product on a Windows computer that supports user account control (UAC), a dialog box that prompts you to promote your permissions might appear. If this dialog box appears, promote your permissions.

Caution: Do not shut down the OS during installation. If you do so and try to re-install the program later, the program might not run normally.

To re-install the network access control agent:

1. Insert the provided media into 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 for starting installation, click the **Next** button.
4. In the dialog box indicating that installation is ready, click the **Install** button.

   Installation is performed.
5. In the dialog box indicating the completion of installation, click the **Finish** button.

Re-installation of the network access control agent is completed. You do not need to restart the computer.

How to update components

Components are agents, site server programs, and network access control agents. The following methods are available for updating these programs.

Automatic update by registering programs on the management server

Components are updated by registering new versions of programs on the management server and automatically distributing them.

To update multiple programs including JP1/IT Desktop Management - Manager, such as when upgrading the entire system, specify that components are to be automatically updated during re-installation of JP1/IT Desktop Management - Manager. This enables new versions of agents, site server programs, and network access control agents to be automatically registered on the management server, and distributed to target computers.

To update individual programs separately, manually specify that components are to be automatically updated and register each program. By doing so, the new versions of programs will be distributed automatically.

To specify that components are to be automatically updated or to register programs on the management server, you can use the dialog box that indicates that the overwrite of JP1/IT Desktop Management - Manager has completed, or the **Component Registration** dialog box that is opened from the **Start** menu of the management server.

Update by using the distribution facility

Components are updated by registering a package on the management server, creating a task, and then distributing the package. This method is useful if you do not want to automatically update components because, for example, you want to control the time when a load is put on the network (by updates).

To update multiple programs including JP1/IT Desktop Management - Manager, such as when upgrading the entire system, during re-installation of JP1/IT Desktop Management - Manager, specify the settings to register components as packages. This allows new versions of agents, site server programs, and network access control agent to be registered automatically as packages on the management server.

To update individual programs separately, manually specify the settings for registering components as packages for distribution, and then register the programs that need updates. This allows the packages to be registered automatically.

To specify the registration of components as packages or to register programs on the management server, you can use the dialog box that indicates that the overwrite of JP1/IT Desktop Management - Manager has completed, or the **Component Registration** dialog box that is opened from the **Start** menu of the management server.

The names of automatically registered packages follow the format *program-name_version-number_program-name-of-each-component* (example: P-2642-739L_0950_JP1_IT Desktop Management - Agent). Add a task with such a package specified, and distribute it.

Tip: If a package of the same version has already been registered, the existing package is not overwritten.

Updates using provided media

You can update components by re-installing programs from a new version of the provided media. This causes the existing version to be overwritten.

To upgrade the entire system, you need to upgrade JP1/IT Desktop Management - Manager, the agents, and then other components. It does not matter whether the site server programs or network access control agents are upgraded first.

8

Migrating an environment

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

Replacing the management server

Replacing the management server means configuring a computer on which JP1/IT Desktop Management - Manager is not installed so that the computer can be used as a new management server.

WARNING: The first four digits of the product version information (for example, *03-00* in product version 03-00-01) for JP1/IT Desktop Management - Manager to be installed on the replacement-target computer must be the same as that for the product on the replacement-source.

WARNING: You cannot upgrade the version of JP1/IT Desktop Management - Manager when replacing the management server. Upgrade the version after replacement is completed, or replace the management server after upgrading the version.

The following describes how to replace the management server. You can replace the management server by installing JP1/IT Desktop Management - Manager on the replacement-target computer and moving data from the replacement-source computer.

To replace the management server:

1. Stop the JP1/IT Desktop Management services.

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

   - `JP1_ITDM_Agent Control`
   - `JP1_ITDM_Service`
   - `JP1_ITDM_Web Container`

2. Back up the database.

   Use Database Manager to back up the database. As a general guideline, make sure that the drive for the backup folder has at least 20 GB of free space.

   If automatic backup of the operation logs is enabled, save the backup data from the operation log backup folder specified during setup.

3. Store the operation log backup data on the replacement-target computer.

   If you have saved the operation log backup data in step 2, store the data in the folder that you want to specify as the *operation-log-backup-folder* on the replacement-target computer before installation. In this folder, do not store any data other than the operation log backup data.

4. Disconnect the replacement-source computer from the network.
5. Install JP1/IT Desktop Management - Manager on the replacement-target computer.
6. Set up JP1/IT Desktop Management - Manager.

If automatic backup of the operation logs is enabled, specify, as the operation log backup folder, the folder in which you stored the backup data in step 3.

7. Restore the database you have backed up in step 2.

   Use Database Manager to restore the database.

   If you have saved the data from the operation log backup folder, store the data in the folder specified during setup.

8. Register a license.

   Register a license from the operation window for JP1/IT Desktop Management - Manager installed on the replacement-target computer.

9. Change the connection destination of the agent.

   Log in to JP1/IT Desktop Management - Manager. Select **Agent Basic Settings** in the **Agent Configurations** window. Then, specify the IP address or host name for the replacement-target computer in the **Management Server** text box under **Basic Settings**.

10. Uninstall JP1/IT Desktop Management - Manager from the replacement-source computer.

11. Delete the backup you created in step 2.

Replacement of the management server is completed.

Tip: To confirm that agents connect to the new management server after replacement, use the **Device List** window in the **Device** window to check whether the value of **Last Modified Date/Time** has been updated. If theagents are not connecting to the new server, check whether the connection destination is correctly specified in the **Setup** window for the agents on the users' computers.

Tip: For a cluster environment, perform the following after restoring the database (step 7) and before registering a license (step 8):

1. Set up the primary management server.

   Select **Modify settings**, and then complete the setup process without changing the settings.

2. Set up the secondary management server.

   Select **Modify settings**, specify the following file for **Setting file to import** in the **Cluster Environment** window, and then complete the setup process.

   primary-management-server-installation-folder`\mgr\conf\jdn_manager_setup.conf`

Notes on replacement

Caution: You need to change the connection destination of the agent (step 9) only when the management server's IP address or host name before and after the replacement has changed.

Caution: If you want to change the connection destination of the agent because the IP address of the replacement-target computer is different from that of the replacement-source computer, you need to ensure that the network is configured so that the replacement-target management server and the agents can directly reference each other. This network configuration must allow the management server and the agent to communicate using each other's host name and IP address via ICMP communication. You also need to permit communication between the TCP protocol ports used by the management server and agents.

Caution: To allow the management server to inherit the system configuration from the replacement-source, the IP addresses of managed devices must be the same before and after replacement.
For example, if the location and IP address of any managed computer changes during the replacement of the management server, that managed computer will not connect to the replacement-target management server. In such a case, create an installation set for the replacement-target management server, and then install the agent on that computer. This will enable the computer to connect to the management server. To allow the management server to inherit the system configuration from the replacement-source, the IP addresses of managed devices must be the same before and after replacement.

Caution: If you want the connection settings between the management server and the agent to be inherited, you need to back up the database and restore it to the replacement-target computer (steps 2 and 7). If you do not back up and restore the database, the replacement-target management server will not connect to the agent.
If you do not want the connection settings between the management server and the agent to be inherited, there is no need to back up or restore the database. However, if you want to connect to the same agents, after replacement is completed, you need to re-create the environment by re-installing the agents and re-specifying the security policies.

Caution: If you connect the replacement-source management server to the network without uninstalling JP1/IT Desktop Management - Manager, the replacement-target management server will not be able to manage the agents correctly.
This is because the replacement-source management server and replacement-target management server can both connect to the agents. If each management server issues different instructions, the agents might not respond to administrator commands. In addition, information reported by agents connected to the replacement-source management server will not be reported to the replacement-target management server. This causes differences in information managed by each management server.

Related Topics:

- Installing JP1/IT Desktop Management on page 2-17
- Custom installation on page 2-18

Replacing a site server

Replacing a site server means transferring the function of the site server from the computer on which the site server is currently installed to another computer. On the replacement-target computer, you need to set up a site server and migrate the operation log data from the replacement-source site server.

Caution: The first four digits of the product version information (for example, *09-50* in product version 09-50-01) of the site server program to be installed on the replacement-target computer must be the same as that for the product on the replacement-source computer.

Caution: You cannot upgrade the site server program when replacing the site server. Upgrade the program after replacement is completed, or replace the site server after upgrading the program.

To replace the site server:

1. Install the agent on the replacement-target computer.
2. Install the site server program on the computer indicated in step 1, and then perform the setup procedure.
3. Stop the site server service (`JP1_ITDM_Remote Site Service`) on the computer indicated in step 2.
4. Manually copy the operation log data from the replacement-source site server to the computer indicated in step 3.

   When copying data, make sure that the folder structure below the operation log data folder is the same between the replacement-source site server and the replacement-target site server. The operation log data folder is the folder specified in **Operation log data folder** during the setup of each site server.

Tip: The larger the operation log data, the longer it takes to re-create the index information for the data in later steps. We recommend only copy the data that is necessary.

Tip: You do not need to manually copy the data relayed by the distribution functionality. This data is automatically downloaded from the management server.

5. Change the server configuration in the operation window.

   In the **Settings** window, select **Server Configuration** and then **Server Configuration Settings**. In the **Site Server Group Settings** area, click the **Edit** button for the site server group that contains the replacement-source site server. In the **Edit Site server Group** dialog box that opens, delete the replacement-source site server, add the replacement-target site server, and then adjust the priorities.

Tip: If the replacement-target site server is not displayed in the **Edit Site server Group** dialog box, confirm that the target computer is connected to the network, and then wait a while.

6. Use the `recreatelogdb` command on the replacement-target site server to re-create the operation log index information.
   Specify `-all` for the command argument.
7. Start the site server service (`JP1_ITDM_Remote Site Service`) on the replacement-target site server.
8. Uninstall the site server program from the replacement-source site server.
   Because the operation log data is not automatically deleted, manually delete it from the operation log data folder.

Replacement of the site server is completed.

Caution: After the `recreatelogdb` command ends, creation of operation log index information is started when the site server is started. Because the site server is under a heavy load during creation of the index information, it might take several days to complete the creation of the index, depending on the amount of operation log data. In addition, because operation logs generated during creation of the index information cannot be checked until the creation process is completed, detection of suspicious operations might be delayed. Be sure to take these issues into consideration before executing the `recreatelogdb` command.

Related Topics:

- Installing a site server program on page 6-3
- Setting up the site server on page 6-5

Connecting the site server to another management server

This section describes the operations required, if any, if the following occurs due to system integration, a change in the administration scope, or for any other reason:

- If the connection destination for the site server used on a system must be changed to the management server on another system.
- If the connection destination for the site server used on a system must be changed to a newly configured management server.#

#: This does not apply to a replaced management server whose database has been restored from backup data of the management server of the original system.

Operations differ depending on whether the operation log data is to be inherited from the site server, or the operation log data is to be deleted and the site server is to be used as a new site server.

To connect the site server to another management server:

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

You can change the connection destination of the site server in the **Setup** window for the agent. From the Windows **Start** menu, select **All Programs** > **JP1_IT Desktop Management - Agent** > **Administrator Tool** > **Setup**. In the **Setup** window that opens, change the IP address for the management server displayed for **Connected management server**.

Tip: If password protection is enabled for the agent, the password entry window appears when the agent setup process is started. The default password is `manager`.

Tip: If you want to change the connection destinations for many site servers, add the agent settings containing new connection destination management servers to the migration source system and assign the information to the target computer.

If you do not want the migration destination to inherit the operation log data, go to step 3.

2. If you want the migration destination to inherit the stored operation log data, report the operation log index information to the management server.

   Execute the `recreatelogdb` command with the `-node` argument specified on the target site server.

   Go to step 4 after execution of the command.

Tip: If an attempt to execute the command fails, wait until the period specified for **Server Connection Interval** in the agent settings (default: 30 minutes) has elapsed, and then execute the command again.

3. If you do not want the operation log data to be inherited, initialize the site server database and delete the operation log data.

   From the Windows **Start** menu, select **All Programs** > **JP1_IT Desktop Management - Remote Site Server** > **Setup**. In the **Setup** window that opens, select **Database Recreation** to re-create the database. In the dialog box that indicates the completion of the setup, clear the **Store operation log data in the re-created database** check box.

   Delete all files and folders in the *operation-log-data-folder*.

   The *operation-log-data-folder* is the folder specified for **Operation log data folder** during setup of the site server.

4. Stop the site server service and delete the distribution data stored in the site server.

   Stop the site server service (`JP1_ITDM_Remote Site Service`) on the target site server.

   Delete all files and folders in the following folder, and then start the site server service.

   data-folder`\AGC\CDS`

   data-folder is the folder specified for **Data folder** during setup of the site server.

5. Change the server configuration in the migration-destination system.

In the **Settings** window (select **Server Configuration** and then **Server Configuration Settings**), change the site server group settings and server configuration according to the environment. If necessary, also change the settings for the migration-source system.

Tip: If a site server connection destination change is not displayed in the **Edit Site server Group** dialog box for the migration destination system, confirm that the target computer is connected to the network, and then wait a while.

The connection destination of the site server is changed. The site server can now be used on the migration-destination system.

Appendix A

This Appendix provides you topics that you need to refer to in the process of installation, setup and getting started.

This appendix includes the following key topics:

- ☐ Setting up and installation
- ☐ User Management - Default account values
- ☐ Agent and Agentless management capacity
- ☐ Communication between the management server and a site server
- ☐ Communication between a site server and an agent
- ☐ Reference Material for This Manual

Setting up and installation

This sections provides you details and procedures for optional tasks during the installation process.

Allowing communication through Windows firewalls

While Installing JP1/IT Desktop Management, if you have the Windows Firewall settings turned ON, the software is automatically added to exceptions. If you have the firewall settings Off when installing JP1/IT Desktop Management, and if you want to turn the firewall settings ON after the installation, use **`addfwlist.bat`** to allow JP1/IT Desktop Management to communicate through Windows firewall. After completing installation, make sure to allow communication through Windows firewall for JP1/IT Desktop Management's management operation.

Note:

- You must have administrative privileges to execute this command.
- Execute the firewall command **`addfwlist.bat`** when Windows Firewall Service is running.

Return values for **`addfwlist.bat`** command:

Returned value	Description
0	The command ended successfully.
-1	The command ended abnormally.

Example: To configure Windows Firewall to allow communication from JP1/IT Desktop Management, use the following command:

```
addfwlist.bat
```

Setting up AMT functionality

Follow the steps provided below to setup AMT functionality.

To use AMT functions:

1. Install the AMT driver.
2. Set up AMT from the BIOS.
3. Perform assembly registration for the AMT functionality DLLs (**`jdngamt.dll`**, **`jdnagcamt.dl`**l).

   The following is an example of command execution using the default installation destination for the product.

   Agent

   Regasm.exe /register /codebase "*C:\Program Files\Hitachi\jp1itdmm\mgr\bin\jdngamt.dll*"

   Manager

Regasm.exe /register "*C:\Program Files\Hitachi\jp1itdmm\mgr\bin\jdnagcamt.dll*Files\Hitachi\jp1itdmm\mgr\bin\jdnagcamt.dll"

Creating group resource in primary server

After installing JP1/IT Desktop Management, create the group and register the resources required for it in Microsoft Cluster Service or Windows Server Failover Cluster. You should have administrative privileges to create group resources in primary server.

Tip: Refer to Microsoft Cluster Service/Windows Server Failover Cluster manuals to learn how to create group resources.

To create group resource in management server:

1. Create another group apart from the Cluster Group that is already registered in Microsoft Cluster Service or Windows Server Failover Cluster.
2. Create the resources required for the created group. Refer to Group Resource to view the required resources to be registered for group.
3. Set the running server as the primary (active) server.
4. Make the Generic resources offline and the other service resources of JP1/IT Desktop Management online.
5. If you have Windows Server 2008, Run the command for in the command prompt, given below.
   "cluster *res*"JP1/IT Desktop Management Web Service"*/priv*StartupParameters="""

Note: Legend: * symbol means a single-byte space.

For setting items and values for each resources, see the following topics:

- JP1_ITDM_DB Service settings on page A-3
- JP1_ITDM_DB Cluster Service settings on page A-4
- JP1_ITDM_Web Container settings on page A-5
- JP1_ITDM_Agent Control settings on page A-6
- Other service resource settings on page A-7

JP1_ITDM_DB Service settings

The following table shows the settings and value for JP1_ITDM_DB Service.

Resource name	Item	Value
JP1_ITDM_DB Service	Name	Specify a name
	Resource type	Specify "Generic Service "

Resource name	Item	Value
	Group	Specify a group name for the management server
	Possible owners	Specify the two, primary (active) and secondary (standby) servers.
	Dependencies	Specify Network Name resource and Shared disk (Physical disk) Resource.
	Service Name	Specify "HiRDBEmbeddedEdition_JE1".
	Registry Replication	Do not specify
	Failover threshold	0 (Fix)
	Failover period (seconds)	0 (Fix)
	Pending timeout (seconds)	300 (recommended value)

JP1_ITDM_DB Cluster Service settings

The following table shows the settings and value for JP1_ITDM_DB Cluster Service.

Resource name	Item	Value
JP1_ITDM_DB Cluster Service	Name	Specify a name
	Resource type	Specify "Generic Service "
	Group	Specify a group name for the management server
	Possible owners	Specify the two primary (active) and secondary (standby) servers.
	Dependencies	Specify the resource of "JP1_ITDM_DB Service"
	Service Name	Specify "HiRDBClusterService_JE1".
	Registry Replication	Do not specify.
	Failover threshold	1 (recommended value)
	Failover period (seconds)	900 (recommended value)
	Pending timeout (seconds)	300 (recommended value)

JP1_ITDM_Service settings

The following table shows the settings and value for JP1_ITDM_Service.

Resource name	Item	Value
JP1_ITDM_Service	Name	Specify a name
	Resource type	Specify "Generic Service "
	Group	Specify a group name for the management server
	Possible owners	Specify the two primary (active) and secondary (standby) servers.
	Dependencies	Specify the resource of "JP1_ITDM_DB Cluster Service".
	Service Name	Specify " JP1_DTNAVI_MGRSRV".
	Registry Replication	Do not specify.
	Failover threshold	1 (recommended value)
	Failover period (seconds)	900 (recommended value)
	Pending timeout (seconds)	300 (recommended value)

JP1_ITDM_Web Container settings

The following table shows the settings and value for JP1_ITDM_Web Container settings.

Resource name	Item	Value
JP1_ITDM_Web Container	Name	Specify a name
	Resource type	Specify "Generic Service "
	Group	Specify a group name for the management server
	Possible owners	Specify the two primary (active) and secondary (standby) servers.
	Dependencies	Specify the resource of " JP1_ITDM_DB Cluster Service".
	Service Name	Specify "JP1_DTNAVI_WEBCON".
	Registry Replication	Do not specify.
	Failover threshold	1 (recommended value)
	Failover period (seconds)	900 (recommended value)
	Pending timeout (seconds)	300 (recommended value)

JP1_ITDM_Web Server settings

The following table shows the settings and value for JP1_ITDM_Web Server settings.

Resource name	Item	Value
JP1_ITDM_Web Server	Name	Specify a name
	Resource type	Specify " Generic Service "
	Group	Specify a group name for the management server
	Possible owners	Specify the two primary (active) and secondary (standby) servers.
	Dependencies	Specify the resource of "Network Name resource ".
	Service Name	Specify "JP1_DTNAVI_WEBSVR".
	Registry Replication	Do not specify.
	Failover threshold	1 (recommended value)
	Failover period (seconds)	900 (recommended value)
	Pending timeout (seconds)	300 (recommended value)

JP1_ITDM_Agent Control settings

The following table shows the settings and value for JP1_ITDM_Agent Control settings.

Resource name	Item	Value
JP1_ITDM_Agent Control	Name	Specify a name
	Resource type	Specify "Generic Service "
	Group	Specify a group name for the management server
	Possible owners	Specify the two primary (active) and secondary (standby) servers.
	Dependencies	Specify the resource of " JP1_ITDM_DB Cluster Service".
	Service Name	Specify "JP1_DTNAVI_AGCTRL".
	Registry Replication	Do not specify.
	Failover threshold	1 (recommended value)
	Failover period (seconds)	900 (recommended value)

Resource name	Item	Value
	Pending timeout (seconds)	300 (recommended value)

Other service resource settings

The following table shows required resources for setting resource settings for resources other than service resources.

Resource name	Item	Value
-IP Address resource -Network Name resource -Shared disk (Physical disk) Resource	Failover threshold	1 (recommended value)
	Failover period (seconds)	900 (recommended value)
	Pending timeout (seconds)	300 (recommended value)

User Management - Default account values

The following table provides the details of built-in account values.

Item	Initial Value	Notes
User ID	system	Cannot be changed.
Password	manager	At initial login, change password and specify email in user management window.
Permissions	System Management and User Account Management	N/A
Username	None	N/A
E-mail	None	N/A
Description	Built-in account	N/A
User profile	None	This item is not created at initial registration.

Agent and Agentless management capacity

The following table compares JP1/IT Desktop Management's management capabilities with Agent and without Agent.

Category	Agent Management	Agentless Management
Device information collection[#1]	Y	P

Category		Agent Management	Agentless Management
Security status diagnosis	Security policy allocation	Y	Y[#2]
	Security status diagnosis	Y	P
Security management	Policy allocation	Y	Y
	Track security status and enforce security compliance	Y	P
	Collect operation logs	Y	N
	Notification messages to end users	Y	N
	Prevent following unauthorized actions: • Printing • External Device • Software	Y	N
	Power On/Off	Y	N
Asset management	Device information collection[#3]	Y	P
	Hardware management	Y	P
	Software license management	Y	Y
	Software management	Y	Y
	Contract management	Y	Y
Software/file distribution	Software distribution	Y	N
	File distribution	Y	N
	Windows update distribution	Y	N
	Software uninstallation	Y	N
Remote control	Computer operation	Y	Y[#4]
	Troubleshoot	Y	P
	Chat	Y	N
	File transfer	Y	N
Network Access Control	Enable access control	Y	N
	Network connection control	Y	Y
Report creation		Y	P

Note: Legend:

- Y - Yes, Management possible.
  N - No, Management not possible.

P - Partial Management possible. (Cannot perform all management tasks, but you can perform part of the tasks)

- #1 - The device information that can be collected depends on whether the agent is present.
- #2 - If you want to diagnose the security status for an agentless computer, use Windows Administrative Share. For individual agentless computers, the security status of the screensaver cannot be determined.
- #3 - Collecting device information depends on the presence of agent and credential settings.
- #4 - You can operate computers as long as they are connected via RFB.

Communication between the management server and a site server

In many cases, JP1/IT Desktop Management provides communication between the management server, a site server, and an agent by sending and receiving data. For each function, the following describes when communication between the management server and a site server occurs.

Device management

- When device discovery is performed

Security management

- When security policies are created or edited
- When security policies are assigned
- When an operation log stored in the site server is searched or viewed

Distribution management

- When a package is created
- When software is installed or files are distributed

Others

- When agent settings are changed
- When an agent program is registered with the management server
- When an agent is deployed on a computer
- When a site server program is registered with the management server
- When a site server is installed on a computer in the operation window
- When server configuration management settings are changed
- When a network access control agent program is registered with the management server

- When a network access control agent is installed on a computer in the operation window

Communication between a site server and an agent

In many cases, JP1/IT Desktop Management provides communication between the management server, a site server, and an agent by sending and receiving data. For each function, the following describes when communication between a site server and an agent occurs.

Security management

- When security policies are assigned
- When an operation log is acquired

Distribution management

When software is installed or files are distributed

Others

- When an agent is deployed on a computer
- When a site server is installed on a computer in the operation window
- When a network access control agent is installed on a computer in the operation window

Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

Conventions: Abbreviations for product names

This manual uses the following acronyms:

Abbreviation	Full name or meaning
AMT	Intel(R) Active Management Technology
Firefox	Firefox(R)
Intel	Intel(R)
Linux	Linux(R)
Mac OS	MAC OS(R)
VMWare	VMWare(R)

The following table shows the function names written in this manual.

Abbreviation	Full name
Programs and Features	Add/Remove Applications
	Add/Remove Programs
	Programs and Features

Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Full name or meaning
ARP	Address Resolution Protocol
AVI	Audio Video Interleaving
BIOS	Basic Input / Output System
CD	Compact Disc
DVD	Digital Versatile Disc
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
ID	IDentification
IP	Internet Protocol
KVM	Keyboard Video Mouse
LAN	Local Area Network
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
RFB	Remote Framebuffer
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UAC	User Account Control
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VNC	Virtual Network Computing

Conventions: KB, MB, GB, TB, and PB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1,024^2$ bytes.
- 1 GB (gigabyte) is $1,024^3$ bytes.
- 1 TB (terabyte) is $1,024^4$ bytes.
- 1 PB (petabyte) is $1,024^5$ bytes.

Glossary

This glossary defines the special terms used in this document. Click the desired letter below to display the glossary entries that start with that letter.

A

Access Permission
JP1/IT Desktop Management user accounts have three permissions levels; user management permission, administrator permission and view only permission. The user's access to the application is defined by the assigned user permission.

AD Discovery
Active Directory discovery collects the device information based on devices that are registered in the Active Directory domain.

Administration Scope
Administration scope, which is set for a user account, is the range that the organization administrator controls.

Agent Configuration
Agent configuration is the package that contains agent's installation parameters along with the agent program to install in target computers. You can customize the configuration to suit the management requirement for target computers.

Agent Installer
Agent Installer is the package with Agent Configuration, Installation Folder, and Installation command. You can deploy the installer set and install an agent in target computers for managing the devices with the agent.

Agentless Management
Managing devices connected to the network without installing an agent in them.

| # | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Agents
JP1/IT Desktop Management agents are specialized programs that run on managed target computers and communicate with the management server. These agents allow IT managers to monitor file and network activity, enforce security settings, and distribute software and files to managed PCs.

Auto Discovery
Based on specified discovery schedule, JP1/IT Desktop Management executes discovery automatically to find new devices in the management system.

Auto-Install Agent
This is an option in the Discovery Wizard > Specify Discovery Option panel. When you select this option, JP1/IT Desktop Management installs agent on the discovered node, right after discovery.

B

Built-in user account
The software application has a built-in user account called "system" with administrative permission.

C

Chat
The ability to chat with end users on an agent computer during a remote session.

Client machine
This is a computer that is used to access the management server.

Cluster Configuration
Configuring JP1/IT Desktop Management's operation settings in primary and secondary server setup. The secondary server works as a Failover Server. If JP1/IT Desktop Management's management system has an interruption or failure, the secondary server takes over for uninterrupted management process.

Controller
The computer from which you operate a remote session on the agent computer. You can download the controller from JP1/IT Desktop Management and install it on your computer before starting remote control.

Credential
Credentials are user login authentication for nodes in the discovery process. The credential information, enables JP1/IT Desktop Management to collect device details from the discovered nodes, after discovery.

D

Default Agent Configuration
JP1/IT Desktop Management provides a default agent configuration. If you do not specify the agent configuration, JP1/IT Desktop Management assigns the default agent configuration to the target devices. You can customize the default configuration to suit your specific management targets.

Deployment
This is a function to transfer the software (agent) to managing-target devices and make it executable. Also, this is a function to remove executable software from managing-target devices.

Discovered Nodes
This is a tab within the Setting module that shows all the discovered and rediscovered nodes that were identified by the JP1/IT Desktop Management. Administrators use this view to select which discovered nodes they want to manage, or ignore.

Discovery
This is a function to search nodes that are connected to networks, in a specified network range.

Discovery Log
A log that displays discovered nodes, discovery process and the related details of discovered nodes.

Discovery Notification
E-mail that notifies recipients that the discovery process is complete.

Discovery Process
A process used to identify nodes on a network.

Discovery Status
Shows the status of discovery process.

Discovery Wizard
A Windows wizard that allows system administrators to configure settings (such as IP address range or Active Directory domain information) for initiating the discovery process that identifies nodes connected to a network.

Distributed Operation Log
Distributed operation logs are stored on site servers. From the operation window, you can view the distributed operation logs separately from the operation logs stored on the management server.

E

E-mail notification
JP1/IT Desktop Management generates automatic e-mail notifications for system events. You can specify the e-mail notification settings for discovery notification. JP1/IT Desktop Management uses the built-in user account as the from address for system generated e-mails.

H

Home module
Home module provides an overview of system status in dynamic panes view. Each pane displays a summary of the managed environments. Links within each pane allow you to navigate to the specific modules for details.

HRC
Hitachi Remote Control protocol. Uses JP1/IT Desktop Management's Agent to remotely access the target computers.

I

Ignored Nodes
Within the Settings module, the JP1/IT Desktop Management Admin can manually designate nodes that the JP1/IT Desktop Management should not manage. These nodes are moved to the Ignored Nodes panel of the Settings module.

IP address range
The IP address range is all the IP addresses between the two IP address, "From" and "To" you specify in the IP address range dialog box.

L

Last Discovery Log
The Last Discovery Log tab contains details of discovered nodes, status of the discovery process and the option to start discovery. If the number of discovered nodes exceeds or get close to maximum number associated with the purchased license, a warning message displays.

License Key File
A license key file is provided when you purchase a JP1/IT Desktop Management license. Use this file for registering licenses.

M

Managed Computer
Computers managed in JP1/IT Desktop Management.

Managed Device
Device managed by JP1/IT Desktop Management. Can be a computer, printer or USB device.

Managed Nodes
This refers to discovered nodes that are selected for management.

Management Server
Server on which JP1/IT Desktop Management is installed, is called a “Management Server”.

Monitoring Interval
Based on the monitoring interval you specify in Agent Configuration dialog box, JP1/IT Desktop Management Agents collect device information and report the details to manager at the specified intervals. In Agentless management, the device details are collected at the time specified in Auto-Monitoring interval.

N

Navigation area
Refers to the left-pane view of the JP1/IT Desktop Management dashboard. The contents of this area adjusts based on the selected module (Home, Security, Assets, Inventory, Events, Reports, Settings).

Network access control
The ability to detect unauthorized network access in the JP1/IT Desktop Management’s management environment and to deny or permit user access to the network. With network access control you can also configure security policies for temporary network access or denial.

Network Access Controller
JP1/IT Desktop Management’s feature that enables you to detect and allow or deny access to unauthorized computers that attempt to access your network.

Node
Refers to a monitored computer, switch, or a storage.

P

Product Update
You can automatically setup to receive or download product updates to your software and windows update from the Support Service site.

R

Remote Control
The ability to remotely access agent computers, and troubleshoot errors. With this feature you can transfer files between computers, record remote access sessions, transfer clipboard data, and chat with the agent- computer users.

Remote Controller
Allows you to perform the remote operations on the agent computer from the controller. When you connect to multiple agents from a controller, multiple remote controllers appear on the controller screen.

RFB
Remote framebuffer protocol, uses the simple protocol to remotely access managed nodes when the target computer is in agentless management.

S

Site Server
A computer on which a site server program is installed. You can deploy site servers and use them as storage locations for operation logs or relay points for the distribution facility to reduce the load on the management server and network.

Site Server Group
A group of more than one site server. When you deploy site servers, set a site server group and specify each site server as a storage location for operation logs for each network segment or a relay point for the distribution facility. When multiple site servers are registered in the site server group, if a site server cannot be connected to, another site server in a group is automatically connected to. This increases functional availability of site servers.

Site Server Program
A program installed on a computer used for load balancing on the management server. The site server program communicates with JP1/IT Desktop Management - Manager and agents to support functions related to operation logs and distribution-related functions. The program is called *JP1/IT Desktop Management - Remote Site Server*.

Smart Device
A portable small terminal, such as a smartphone, tablet PC, or PDA.

Start Discovery Wizard
This wizard launches for capturing information about your environment.

System Administrator Permission
Permission for performing all operations except registering, editing and deleting user accounts.

U

User Account
"User Account" is the unique user access credentials for each user with an ID, password and associated e-mail for logging into JP1/IT Desktop Management.

User ID
Each user will have an User Account with unique User ID to log into the management system.

User Management
This involves the following operations like 1. Adding, editing, or removing (deleting) an user account that have logged into the "Management Server". 2. User information management. 3.Control of login authentication and user permissions.

User Management Permission
Permission for only registering, editing and deleting user accounts.

W

Windows Update Management
The ability to receive alerts about the latest Windows updates from Microsoft, manage downloads, and setup automatic distribution of updates to target computers.

Index

I

J

K

L

M

N

O

P

R

S

T

U

V

W