



Remote Communication Gate S

Installation Guide

-
- 1 Pre-installation Checks
 - 2 Installation
 - 3 After Installation
 - 4 Uninstallation
 - 5 Appendix

How to Read This Manual

Symbols

The following set of symbols is used in this manual.

 **Important**

Indicates a situation that may result in property damage or malfunction if instructions are not followed. Be sure to read the instructions.

 **Preparation**

Indicates information or preparations required prior to operating.

 **Limitation**

Indicates a function's limitations.

 **Note**

Indicates supplementary relevant information.

 **Reference**

Indicates where you can find further relevant information.

[]

Indicates the names of keys that appear on the computer screen.

Terminology

The following is an explanation of the terminology used in this manual:

Term	Explanation
Authentication	Authentication refers to the process of verifying a user's identity, and allowing him or her access to the system. Remote Communication Gate S includes a built-in authentication system, and supports several external authentication systems such as LDAP and ActiveDirectory.
Device	A "device" is a printer or multifunction machine connected to the network or a printer connected to a computer via USB. Though the term generally includes routers, hubs, and other network devices, "device" in this manual is limited to printers and multifunction machines.

Term	Explanation
Discovery	Discovery refers to the process of automatically detecting devices connected to the network and devices connected to computers via USB, and then registering them to Remote Communication Gate S.
Package (Installation Package)	A package is an ".exe" file that contains all of the necessary files and settings to install a device driver. Packages are used to distribute device drivers to users. All content registered with a package is installed by running the ".exe" file. You can create packages using the Packager application, which you can download from the Remote Communication Gate S server and install it on a computer.
Packager	The Packager is an application for creating installation packages.
Settings	You can perform the various settings in Remote Communication Gate S server. Setting Menu related to the network, views, group management, notification, as well as individual customization and log settings can be performed for Remote Communication Gate S server.

Screens

The explanations in this manual use screen images from Windows Server 2008 Standard Edition, Windows Vista, and Internet Explorer 7.0. If you use another version of Windows, screen images may differ. However, you can perform the same steps.

Guides for This Solution

The following guides are available for Remote Communication Gate S:

Remote Communication Gate S Installation Guide (this manual, HTML/PDF)

This guide is intended for the administrator and explains the installation, uninstallation, and initial setup procedures for Remote Communication Gate S.

Remote Communication Gate S User's Guide (HTML/PDF)

This guide is intended for the end user. It explains how to display devices, search for devices, and install packages by logging in Remote Communication Gate S.

Remote Communication Gate S Administrator Operations Guide (HTML/PDF)

This guide is intended for the administrator. It explains how to utilize Remote Communication Gate S to configure and manage settings and operations: for example, registration and monitoring of devices, the creation of installation packages, or retrieval of device logs.

Note

- Acrobat Reader or Adobe Reader is required to view the PDF documentation.
- You can view the HTML documentation using a Web browser. We recommend Microsoft Internet Explorer 4.01 SP2 or a later version.
- A simplified version of the HTML documentation is available for earlier or non-recommended browsers.
- If JavaScript is disabled or unavailable in your browser, you will not be able to search or use certain buttons in the HTML documentation.
- If you are using an earlier or non-recommended browser and the simplified version of the documentation does not appear automatically, replace `\int\index_book.htm` with `\unv\index_book.htm` in your browser's address bar.

Important

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW:
 - THE SUPPLIER SHALL NOT BE LIABLE FOR THE RESULT OF OPERATION OF THIS SOFTWARE OR THE USE OF THIS DOCUMENT.
 - THE SUPPLIER SHALL NOT BE LIABLE TO YOU FOR DAMAGES OR LOSS OF ANY DOCUMENT OR DATA PRODUCED BY USING THIS SOFTWARE.
 - THE SUPPLIER SHALL NOT BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF BUSINESS INFORMATION, AND THE LIKE) CAUSED BY FAILURE OF THIS SOFTWARE OR LOSS OF DOCUMENTS OR DATA, NOR FOR ANY OTHER DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, IF THE SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- Some illustrations or explanations in this guide may differ from your product due to improvement or change in the product.
- The contents of this document are subject to change without notice.
- No part of this document may be duplicated, replicated, reproduced in any form, modified or quoted without prior consent of the supplier.
- It is possible that any document or data stored in the computer will be damaged or lost by user error during operation or software error. Be sure to back up all important data beforehand. Important documents and data should always be copied or backed up. Documents and data can be lost because of malfunction or human error. Furthermore, the customer is responsible for protection measures against computer viruses, worms, and other harmful software.
- Do not remove or insert any disk while operating this software.

Trademarks

Adobe[®], Acrobat[®], Acrobat Reader[®], and Flash[®] are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft[®], Windows[®], Windows Server[®], Windows Vista[®], Internet Explorer[®], and SQL Server[®] are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Pentium[®] is a registered trademark of Intel Corporation.

Lotus[®] and Domino[®] are registered trademarks of IBM Corporation and Lotus Development Corporation.

Novell[®], NetWare[®], NDS[®], and eDirectory[™] are registered trademarks or trademarks of Novell, Inc. in the United States.

Notes[®] is a registered trademark of IBM Corporation and Lotus Development Corporation.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

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

The proper names of the Windows operating systems are as follows:

- The product names of Windows 2000 are as follows:

Microsoft[®] Windows[®] 2000 Professional

Microsoft[®] Windows[®] 2000 Server

Microsoft[®] Windows[®] 2000 Advanced Server

- The product names of Windows XP are as follows:

Microsoft[®] Windows[®] XP Home Edition

Microsoft[®] Windows[®] XP Professional

- The product names of Windows Vista are as follows:

Microsoft[®] Windows Vista[®] Ultimate

Microsoft[®] Windows Vista[®] Enterprise

Microsoft[®] Windows Vista[®] Business

Microsoft[®] Windows Vista[®] Home Premium

Microsoft[®] Windows Vista[®] Home Basic

- The product names of Windows 7 are as follows:

Microsoft[®] Windows[®] 7 Home Premium

Microsoft[®] Windows[®] 7 Professional

Microsoft[®] Windows[®] 7 Ultimate

- The product names of Windows Server 2003 are as follows:

Microsoft® Windows Server® 2003 Standard Edition

Microsoft® Windows Server® 2003 Enterprise Edition

- The product names of Windows Server 2003 R2 are as follows:

Microsoft® Windows Server® 2003 R2 Standard Edition

Microsoft® Windows Server® 2003 R2 Enterprise Edition

- The product names of Windows Server 2008 are as follows:

Microsoft® Windows Server® 2008 Standard

Microsoft® Windows Server® 2008 Enterprise

- The product names of Windows Server 2008 R2 are as follows:

Microsoft® Windows Server® 2008 R2 Standard

Microsoft® Windows Server® 2008 R2 Enterprise

TABLE OF CONTENTS

How to Read This Manual.....	1
Symbols.....	1
Terminology.....	1
Screens.....	2
Guides for This Solution.....	3
Important.....	4
Trademarks.....	5

1. Pre-installation Checks

What You Can Do with Remote Communication Gate S.....	9
Remote Communication Gate S Editions.....	9
Components.....	13
System Requirements.....	15
Server Requirements.....	15
Client Computer Requirements.....	17
@Remote Requirements.....	19
Supported Device.....	20
Network Requirements.....	20
Communication Ports.....	21
Available Methods and Required Environments for Authentication.....	22
Setup Flow.....	24
Installation Type.....	25
Required Settings.....	26
Web Server Settings.....	26
Settings Windows Firewall-excepted Ports.....	26
Settings When Using Windows Server 2003 or Later.....	26
Activating Browser JavaScript.....	27

2. Installation

New Installation.....	29
Required Information for Installation.....	29
Installation Procedure.....	30
Overwrite Installation.....	42
Reinstalling Remote Communication Gate S.....	42
Upgrading from an Earlier Version of Remote Communication Gate S.....	43

Upgrading from Web SmartDeviceMonitor Professional IS/Standard.....	45
3. After Installation	
Access Remote Communication Gate S.....	47
Access from Server Computer's Start Menu.....	47
Access from Web Browser.....	47
Login to Remote Communication Gate S.....	49
Setup Wizard.....	51
Initial Settings.....	51
4. Uninstallation	
Uninstallation.....	67
Files Remaining after Uninstallation.....	68
5. Appendix	
Troubleshooting.....	69
INDEX	71

1. Pre-installation Checks

This chapter explains what you can do with Remote Communication Gate S and details the server and installation/operation requirements for running it.

What You Can Do with Remote Communication Gate S

Remote Communication Gate S enables you to manage multiple devices in your office easily and reduce their running costs through improved efficiency.

- **Printer Management**

You can retrieve the latest information about devices. The devices are automatically discovered according to the specified conditions, and you can list the devices on the maps and manage to register them into groups.

@Remote service

If you use @Remote service, you can:

- reduce the downtime caused by the device errors and firmware updates.
- retrieve reports of operating conditions for TCO management.
- collect counter information and order supplies such as toner automatically.

- **Log Management**

By collecting various types of logs, you can manage device usage more effectively.

- **Firmware Management**

You can access the global server to download the latest firmware updates for your devices. You can display a list of downloaded firmware, as well as view the details about the firmware, and delete unnecessary firmware.

- **Installation Support**

Multiple users can install printers easily and quickly using installation packages created using the Packager tool.

For details about Packager tool, see the Administrator Operations Guide.

Remote Communication Gate S Editions

There are two editions of Remote Communication Gate S, allowing you to implement a device management solution that fits your organization's system integration and budgetary requirements.

- **Remote Communication Gate S Pro for @Remote Enterprise**

See p.11 "Overview of Remote Communication Gate S Pro for @Remote Enterprise".

- Remote Communication Gate S Pro with Remote Communication Gate S Pro @Remote Connector^{*1}
See p.12 "Overview of Remote Communication Gate S Pro with Remote Communication Gate S Pro @Remote Connector".

*1 Remote Communication Gate S Pro @Remote Connector can be used only on a computer on which Remote Communication Gate S Pro for @Remote Enterprise is already installed.

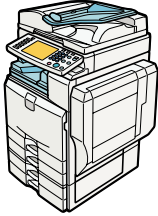
Product edition naming conventions

In this manual, the following names are used to describe the different editions of Remote Communication Gate S:

- "Remote Communication Gate S" is used as a general term for all editions of Remote Communication Gate S.
- "Remote Communication Gate S Pro" is used when an explanation applies to Remote Communication Gate S Pro for @Remote Enterprise.
- "Remote Communication Gate S Pro @Remote Connector" is abbreviated as "@Remote Connector".

Overview of Remote Communication Gate S Pro for @Remote Enterprise

Multifunction machine



Printer



Other brand multifunction machine



Other brand printer

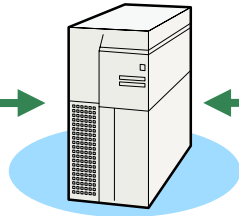


USB



Printer

- Printer management
- Log management
- Firmware management
- Installation support



Administrator's computer

- Device management through Web browser interface
- Package creation

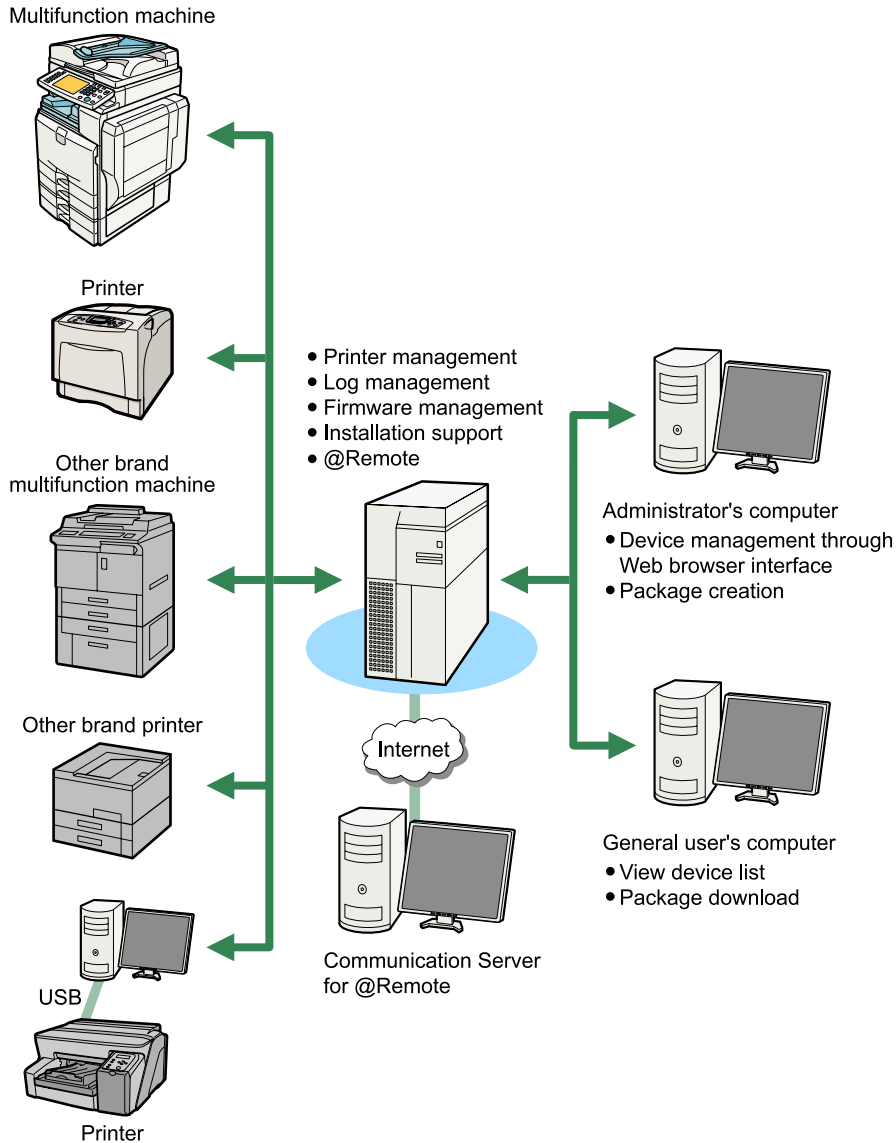


General user's computer

- View device list
- Package download

BRW001S

Overview of Remote Communication Gate S Pro with Remote Communication Gate S Pro @Remote Connector



BRW005S

To use the @Remote service, Remote Communication Gate S Pro @Remote Connector is required. For details, contact your service representative.

Components

Following components are provided:

Database component

Remote Communication Gate S uses Microsoft's SQL Server 2005 database application to manage the logs it collects.

↓ Note

- To install Remote Communication Gate S, you must first install SQL Server 2005, and then configure the necessary settings. For details, see p.31 "Step 1: Install SQL Server 2005 Express Edition Service Pack 3".

Remote Communication Gate S components

The following tools are all installed at the same time when the product is installed on a server that runs Remote Communication Gate S.

Component	Explanation
ManagementTool	A tool for managing Remote Communication Gate S server.
SSL Setting Tool	A tool for issuing and importing CA server certificates for encrypting communication channels using the SSL protocol. For details about SSL Setting Tool, see "Encrypting Communication Channels", Administrator Operations Guide.
Authentication Manager	A tool for unifying user authentication settings. This is a Windows application. The instructions and explanations in this guide assume that you are configuring the Authentication Manager Settings on the administrator's computer.
StartBrowser	A shortcut for displaying the login screen of Remote Communication Gate S.
Activation Tool	A tool for activating: <ul style="list-style-type: none"> Remote Communication Gate S Pro You must activate Remote Communication Gate S if you wish to continue using it after 45 days from the date of installation. @Remote service To use @Remote service, an additional contract and activation are required. Contact your service representative for details.

Component	Explanation
Import LDAP Server Certificate	A tool for importing the LDAP server SSL certificate to the Authentication service of Remote Communication Gate S.

System Requirements

Check that the server and administrator's computers satisfy the specifications detailed below.

1

Server Requirements

To install Remote Communication Gate S, the server computer must meet the following requirements:

Item	Requirements
Hardware	<ul style="list-style-type: none"> • CPU: Pentium 4 compatible 2.8 GHz or higher (with Hyper Threading Technology or equivalent) • Memory: 1 GB or higher (For @Remote service, we recommend at least 2 GB) • Minimum available hard disk space: 800 MB. Separate additional hard disk space is required for storage of logs, packages, and firmware. <p>★ Important</p> <ul style="list-style-type: none"> • Computer names can contain the following characters only: upper and lower case letters (A-Z, a-z), numbers (0-9), and hyphens (-).
Operating System	<ul style="list-style-type: none"> • Windows Server 2003 Standard Edition/Enterprise Edition: Service Pack 2 or later • Windows Server 2003 R2 Standard Edition/Enterprise Edition: Service Pack 2 or later • Windows Server 2008 Standard/Enterprise <p>↓ Note</p> <ul style="list-style-type: none"> • Operating systems must be 32 bit versions.
Database Application	<ul style="list-style-type: none"> • SQL Server 2005 Express Edition Service Pack 2 or later <p>↓ Note</p> <ul style="list-style-type: none"> • .NET Framework 2.0 must be installed. • SQL Server 2005 Express Edition Service Pack 3 is included in the Remote Communication Gate S installer. • For details about the required environment for installing SQL Server 2005, see Microsoft's online help Web site.
Web Server	<ul style="list-style-type: none"> • Apache 2.0 • Internet Information Services 6.0 or later

Item	Requirements
Supported Language	<p>Dutch, English, French, German, Italian, Spanish</p> <p>Note</p> <ul style="list-style-type: none"> Remote Communication Gate S supports only these six languages. If the display language is not one of these languages, Remote Communication Gate S is displayed in English. The priority of the display language can be changed in the Language preference settings in Internet Explorer.
Web Browser	<ul style="list-style-type: none"> Internet Explorer 6.0 Service Pack 1 or later Internet Explorer 7.0 Internet Explorer 8.0 <p>Important</p> <ul style="list-style-type: none"> JavaScript must be activated. For details about how to activate JavaScript, see p.27 "Activating Browser JavaScript". Adobe Flash Player 9.0 or later must be installed.
Network	<ul style="list-style-type: none"> TCP/IP and UDP must be installed and configured correctly. Only compatible with IPv4. To use the @Remote service, the server must be connected to the Internet. <p>Note</p> <ul style="list-style-type: none"> Implement management using fixed IP addresses.
Screen Resolution	1024 x 768 or higher
Virtual Machine Software	Remote Communication Gate S can run in VMware Infrastructure 3 Standard Edition.
Compatibility	<p>Remote Communication Gate S can be installed on the same computer with the following programs:</p> <ul style="list-style-type: none"> GlobalScan NX Card Authentication Package <p>Note</p> <ul style="list-style-type: none"> Remote Communication Gate S can be installed on the same computer as the listed programs, but it is recommended that you install them on separate servers.

Client Computer Requirements

To operate Remote Communication Gate S, the administrator system must meet the following requirements:

Administrator's computer requirements

Administrators perform device management by accessing Remote Communication Gate S through their computer's Web browser. Administrators also install the Packager tool to create installation packages, and the Authentication Manager to manage users and authentication methods.

Item	Requirements
Hardware	<ul style="list-style-type: none"> • CPU: Pentium compatible 500 MHz or higher • Memory: 200 MB • Minimum available hard disk space: same as recommended minimum for operating system
Operating System	<ul style="list-style-type: none"> • Windows XP Home Edition/Professional: Service Pack 1 or later • Windows Vista Ultimate/Enterprise/Business/Home Premium/Home Basic • Windows 7 Home Premium/Professional/Ultimate • Windows Server 2003 Standard Edition/Enterprise Edition: Service Pack 1 or later • Windows Server 2003 R2 Standard Edition/Enterprise Edition: Service Pack 1 or later • Windows Server 2008 Standard /Enterprise • Windows Server 2008 R2 Standard/Enterprise <p>Note</p> <ul style="list-style-type: none"> • Packager is usable under Windows Server 2008 R2, but not under any other 64-bit operating systems. All other operating systems must be 32-bit versions. • Packager is usable under Windows Server 2008 R2 only if ran under WoW64 (Windows-on-Windows 64) emulation mode. • If Packager is not required, the operating system can be either 32-bit or 64-bit.

Item	Requirements
Supported Language	Dutch, English, French, German, Italian, Spanish Note <ul style="list-style-type: none"> Remote Communication Gate S supports only these six languages. If the display language is not one of these languages, Remote Communication Gate S is displayed in English. The priority of the display language can be changed in the Language preference settings in Internet Explorer.
Web Browser	<ul style="list-style-type: none"> Internet Explorer 6.0 Service Pack 1 or later Internet Explorer 7.0 Internet Explorer 8.0 Important <ul style="list-style-type: none"> JavaScript must be activated. For details about how to activate JavaScript, see p.27 "Activating Browser JavaScript". Adobe Flash Player 9.0 or later must be installed.
Network	TCP/IP must be installed and configured correctly.
Screen Resolution	1024 x 768 or higher

General user's computer requirements

General users access Remote Communication Gate S through their computer's Web browser and download installation packages when they want to install a printer.

Item	Requirements
Hardware	<ul style="list-style-type: none"> CPU: Pentium compatible 500 MHz or higher Memory: 128 MB or higher Minimum available hard disk space: same as recommended minimum for operating system

Item	Requirements
Operating System	<ul style="list-style-type: none"> • Windows 2000 Professional/Server/Advanced Server (i386): Service Pack 4 or later • Windows XP Home Edition/Professional: Service Pack 2 or later • Windows Vista Ultimate/Enterprise/Business/Home Premium/Home Basic • Windows 7 Home Premium/Professional/Ultimate • Windows Server 2003 Standard Edition/Enterprise Edition: Service Pack 2 or later • Windows Server 2003 R2 Standard Edition/Enterprise Edition: Service Pack 2 or later • Windows Server 2008 Standard/Enterprise • Windows Server 2008 R2 Standard/Enterprise
Supported Language	<p>Dutch, English, French, German, Italian, Spanish</p> <p>Note</p> <ul style="list-style-type: none"> • Remote Communication Gate S supports only these six languages. If the display language is not one of these languages, Remote Communication Gate S is displayed in English. The priority of the display language can be changed in the Language preference settings in Internet Explorer.
Web Browser	<ul style="list-style-type: none"> • Internet Explorer 6.0 Service Pack 1 or later • Internet Explorer 7.0 • Internet Explorer 8.0 <p>Important</p> <ul style="list-style-type: none"> • JavaScript must be activated. For details about how to activate JavaScript, see p.27 "Activating Browser JavaScript". • Adobe Flash Player 9.0 or later must be installed.
Network	TCP/IP must be installed and properly configured.
Screen Resolution	1024 x 768 or higher

@Remote Requirements

The @Remote service is optional. An additional contract and activation are required to use this service. Activation of the @Remote service can only be performed by a Customer Engineer. Contact your service representative for details.

★ Important

- The @Remote service is only available when the server is connected to the Internet.

📖 Reference

- For details about the settings to be implemented by administrators, see "@Remote Settings", Administrator Operations Guide.

Supported Device

The product requirements for the devices that you can monitor using Remote Communication Gate S are as follows:

Network Devices

Item	Requirements
Network Protocol	TCP/IP <div data-bbox="610 848 783 883" style="border: 1px solid #0070C0; border-radius: 10px; padding: 2px; display: inline-block;"> ⬇ Note </div> <ul style="list-style-type: none"> • Not compatible with IPv6 and only compatible with IPv4.
Supported MIB	Printer MIB v2 (RFC 3805) / Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790)

Local Devices

Item	Requirements
Local printers	Connected to a Windows computer via USB. (Printers from a variety of manufacturers are supported.)

Network Requirements

The followings are the required protocols to use the Remote Communication Gate S functions.

Item	Protocol
Device Information Acquisition	SNMP, SNMPv3, or HTTP
Device Setting	SNMP, SNMPv3, or HTTP
Display on Browser	HTTP or HTTPS

Communication Ports

Remote Communication Gate S uses the following ports. Refer to this list when configuring Remote Communication Gate S.

★ Important

- When Remote Communication Gate S is installed on a firewall-protected Windows environment, opening the required ports is necessary.
- Set the ports so that they do not conflict with other connections and services running on the computer.

1. Click [Start] > [Control Panel] > [Windows Firewall].
2. Select [General], and then set it to [On].
3. Select the [Exceptions] tab, and then select [File and Printer Sharing].
4. Add the required ports:

Port Number	Protocol	Description
8080 (default) * ¹	TCP	Web server for Apache
80 (default) * ¹	TCP	Web server for IIS
8443 (default) * ¹	TCP	Web server for Apache
443 (default) * ¹	TCP	Web server for IIS (@Remote service) * ²
162	SNMP	Used for the Remote Communication Gate S system
8011	TCP	
41021	TCP	
50109	TCP	
55512	TCP	
55513	TCP	
135 (RPC)	TCP	Authentication Manger (communication between server and administrator's computer)
50304 (RSI)	UDP	
6001 * ³ (DCOM)	TCP	

*¹ Enter the port numbers that were specified when Remote Communication Gate S was installed. The port number must be a number between 1 and 65535. Do not use letters or double-byte characters.

*² Set this port only if you are using @Remote service. Do not use for other purposes.

*3 This is a sample number. Add all the DCOM ports that were added in the setup of DCOM. Specify a range of unused port numbers that can be secured contiguously (for example: 6000-6010).

1

Available Methods and Required Environments for Authentication

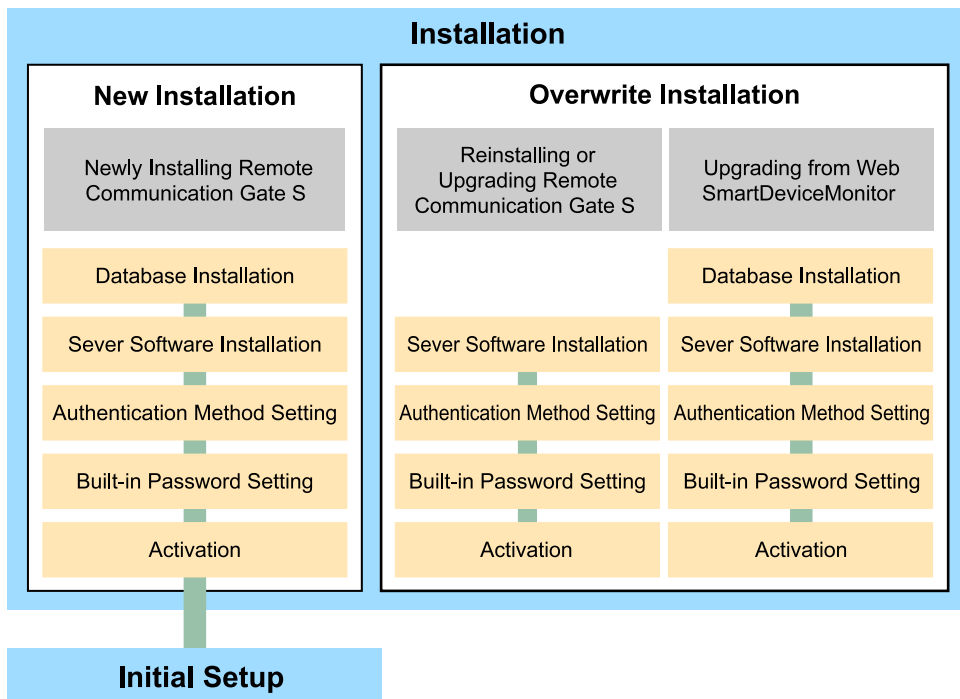
The available methods and required environments for Remote Communication Gate S authentication are as follows:

Authentication Method	Required Environment
Basic Authentication	Requires no particular environment.
Windows Authentication (NT compatible)	<p>Requires one of the following environments:</p> <p>The computer on which you want to install Remote Communication Gate S must be a domain member.</p> <ul style="list-style-type: none"> • Windows NT domain • Windows 2000 Active Directory domain (mixed mode, NT compatible access allowed mode) • Windows Server 2003 Active Directory domain (mixed mode, intermediate) • Windows Server 2008 Active Directory domain
Windows Authentication (native)	<p>Requires one of the following environments.</p> <p>The computer on which you want to install Remote Communication Gate S must be a domain member.</p> <ul style="list-style-type: none"> • Windows 2000 Active Directory domain (native mode, Windows 2000 only access allowed mode) • Windows Server 2003 Active Directory domain (native mode, intermediate) • Windows Server 2008 Active Directory domain

Authentication Method	Required Environment
Notes Authentication	<p>Requires a Lotus Domino R5/R6/R6.5/R7 environment.</p> <p>★ Important</p> <ul style="list-style-type: none"> • Set the "LDAP Service" to "enabled" in the Lotus Domino server default settings. • Notes accounts used for authentication require an Internet password to be set. • If Lotus Domino server default settings are already made, enable the LDAP Service by editing the "Notes.ini" file according to the following procedure: <ol style="list-style-type: none"> 1. Open the "Notes.ini" file. 2. Add LDAP Service to the "ServerTasks" settings. <p>Example:</p> <p>ServerTasks=Router,Replica,Update,Amgr,AdminP,Cal-Conn,Event,Sched,Stats,LDAP,maps</p> <p>! Limitation</p> <ul style="list-style-type: none"> • Do not use double-byte characters in Notes account user names. If you do, authentication, document list display, and searches might not function correctly. • Be sure to use a password-protected account.
NDS Authentication	<p>Requires a NetWare server environment.</p> <p>★ Important</p> <ul style="list-style-type: none"> • The version corresponding to Novell eDirectory for NetWare is Ver.8.7.3 or later.
LDAP Authentication	<p>Requires an LDAP server environment.</p> <p>★ Important</p> <ul style="list-style-type: none"> • The version corresponding to LDAP protocol is Ver.3 or later.

Setup Flow

The following diagram represents the flow of Remote Communication Gate S setup.



BRW002S

Reference

- For details about new installation, see p.29 "New Installation".
- For details about reinstalling Remote Communication Gate S, see p.42 "Reinstalling Remote Communication Gate S".
- For details about Upgrading from an earlier version of Remote Communication Gate S, see p.43 "Upgrading from an Earlier Version of Remote Communication Gate S".
- For details about upgrading from Web SmartDeviceMonitor, see p.45 "Upgrading from Web SmartDeviceMonitor Professional IS/Standard".
- For details about initial settings, see p.51 "Setup Wizard".

Installation Type

You can install Remote Communication Gate S using one of the following two procedures:

New installation

Select this installation type if:

- You are installing Remote Communication Gate S on a server that does not have the same or earlier version of this product installed on it.
- The server does have the same or earlier version of this product installed on it but you do not want to retain the existing data.

For details about new installation, see p.29 "New Installation".

Note

- Be sure to completely uninstall earlier versions before proceeding with a new installation. Otherwise, Remote Communication Gate S will inherit authentication information from previous installations, such as Web SmartDeviceMonitor Professional IS/Standard. For details about uninstalling an earlier version, see p.67 "Uninstallation".

Overwrite installation

Select this installation type if:

- You are reinstalling Remote Communication Gate S on a server computer that already has the same or earlier version of Remote Communication Gate S installed on it and you want to retain the existing data.
- You are installing Remote Communication Gate S on a server computer to upgrade from Web SmartDeviceMonitor Professional IS/Standard and you want to retain the earlier version's data.

Important

- **Discovery settings cannot be retained, and device polling settings return to their default values. Login to Remote Communication Gate S, and configure these settings again if required.**
- **If devices are registered but Remote Communication Gate S has been unable to establish a connection, click [Refresh Selected Device] to update the database information, and then click [Refresh] to display the updated list information.**
For details, see "Device Management Settings", Administrator Operations Guides.

For details about overwriting an earlier installation, see p.42 "Overwrite Installation".

Required Settings

Before using Remote Communication Gate S, perform the following settings.

1

Web Server Settings

If you want to use IIS as a Web server, perform the following settings beforehand. When you use Apache, the followings are not required.

1. Install the corresponding IIS using the CD-ROM of the server operating system.

Operating System	IIS version
<ul style="list-style-type: none"> • Windows Server 2003 Standard Edition/Enterprise Edition: Service Pack 2 or later • Windows Server 2003 R2 Standard Edition/Enterprise Edition: Service Pack 2 or later 	IIS 6.0
<ul style="list-style-type: none"> • Windows Server 2008 Standard/Enterprise 	IIS 7.0

2. Launch the Web service before starting the installation of Remote Communication Gate S.

Note

- This product will run under an anonymous user account for IIS (IUSR_<Computer name>). For this reason, do not disable the IUSR account. For details about changing the IUSR account password, see Microsoft's online help Web site.

Settings Windows Firewall-excepted Ports

If you are installing Remote Communication Gate S in a firewall-protected Windows environment, you must open the required ports.

Log on to Windows as an administrators group member, and then open the required ports. For details about the required ports settings, see p.21 "Communication Ports".

Settings When Using Windows Server 2003 or Later

If the computer used to log on to Remote Communication Gate S is Windows Server 2003 or later, perform the security settings in Internet Options in the sequence given below.

1. Start Internet Explorer.
2. On the [Tools] menu, select [Internet Options...].

3. Click the [Security] tab.
 4. Select [Local intranet] and click [Sites...].
 5. Enter the URL below in [Add this Web site to the zone].
http://{Remote Communication Gate S host name or IP address}
 6. Click [Add].
 7. Click [Close] to close the [Local intranet] dialog box.
 8. Click [OK] to close the [Internet Options] dialog box.
- This completes the settings.

Activating Browser JavaScript

To access and view Remote Communication Gate S, it is necessary to activate JavaScript on the Web browser.

1. On the Internet Explorer [Tools] menu, select [Internet Options...].
2. Click the [Security] tab.
3. Click [Custom Level...].
4. Under [Scripting] select [Enable] in [Active scripting].
5. Click [OK] to close the [Security Settings] dialog box.
6. Click [OK] to close the [Internet Options] dialog box.

2. Installation

This chapter explains the procedure for installing Remote Communication Gate S on a server computer.

New Installation

Select this installation type if you are installing Remote Communication Gate S on a server that does not have an earlier version of this product installed on it, or has the same or earlier version of this product installed on it but you do not want to retain the existing data, such as network addresses or port numbers.

2

General outline for installing and setting up Remote Communication Gate S:

- Step1: Install SQL Server 2005 Express Edition Service Pack 3
- Step2: Install Remote Communication Gate S
- Step3: Set authentication method
- Step4: Set built-in password
- Step5: Activate Remote Communication Gate S
- Step6: Activate @Remote service

For details about each step, see p.30 "Installation Procedure".

Required Information for Installation

The following user information is required for installation:

Required Information	Description	When to use
Administrators group user account	This refers to information about users who have administrator privileges on the computer. Be sure to use the same account when you install the Remote Communication Gate S and log on to Windows. Leaving the Password box blank is not allowed.	<ul style="list-style-type: none">• The initial logon to Windows• The logon to Windows after the restart during the installation procedure
SA password for the database	This refers to the administrator password, which is required when installing SQL Server 2005.	<ul style="list-style-type: none">• Step1: Install SQL Server 2005 Express Edition Service Pack 3• Step2: Install Remote Communication Gate S

Required Information	Description	When to use
Access information to use the domain or server for user authentication	<p>The following domains and servers can be used for user authentication. When you use the following, access information is required</p> <ul style="list-style-type: none"> • Windows NT domain • Windows Active directory domain • LDAP server • Novell server <p>If there are no above environments, use "Basic Authentication" to set the user authentication. In this case, creating users is required. For details, see "Managing Basic Authentication Users", Administrator Operations Guide.</p>	<ul style="list-style-type: none"> • Step3: Set authentication method
Built-in password	<p>This refers to information about users who have total authority to manage Remote Communication Gate S. The built-in user name is "Admin".</p>	<ul style="list-style-type: none"> • Step4: Set built-in password
License code	<p>This refers to information required for activation.</p> <p>You can use Remote Communication Gate S without activation for up to 45 days after installation. To continue using Remote Communication Gate S after 45 days of installation, a license code is required for activation.</p> <p>When you use @Remote service, an additional activation is required. Contact your service representative for details.</p>	<ul style="list-style-type: none"> • Step5: Activate Remote Communication Gate S • Step6: Activate @Remote service

Installation Procedure

★ Important

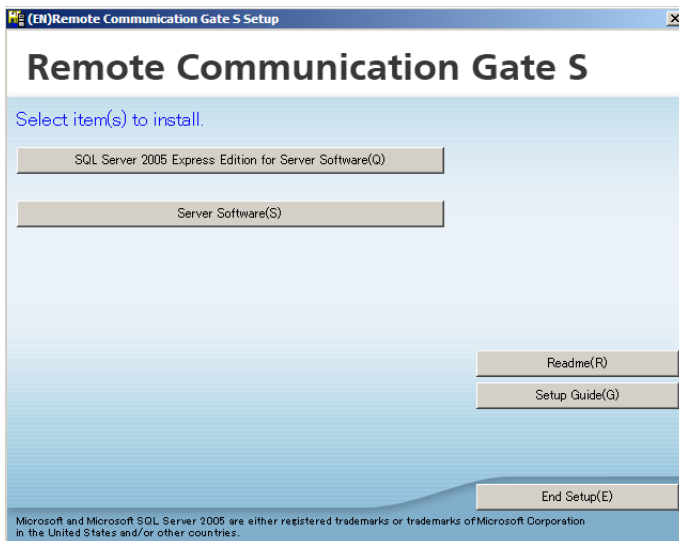
- Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.

- During installation, you are asked to log on to Windows again. Log on as the same user who installed Remote Communication Gate S.

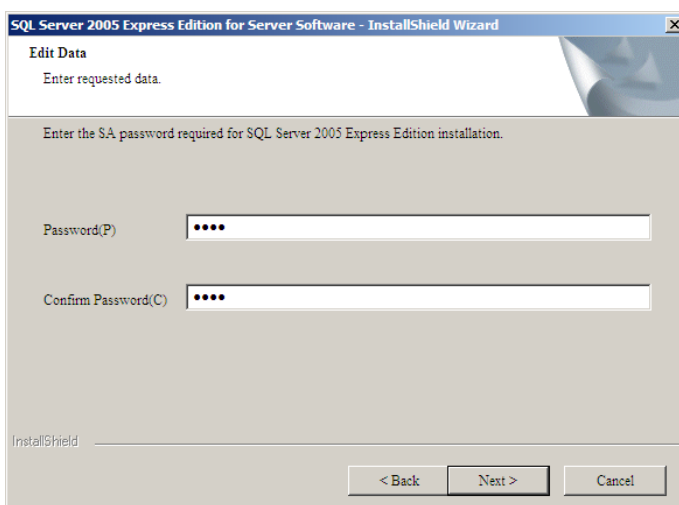
Step 1: Install SQL Server 2005 Express Edition Service Pack 3

1. Double-click RDLaunch.exe.
2. On the initial screen, select "SQL Server 2005 Express Edition for Server Software".

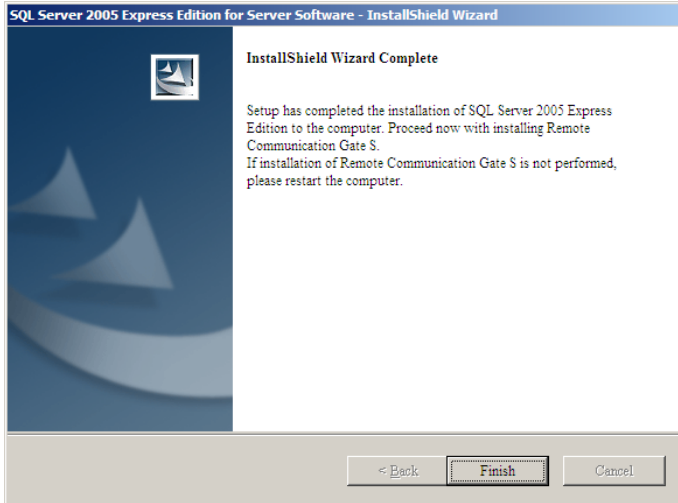
2



3. Read the warning, and then click [OK].
4. Click [Next>].
5. Enter the SA password in the [Password] and [Confirm Password] boxes, and then click [Next>].



6. Click [Install] to start the installation of SQL Server 2005.
7. Click [Finish] to close the [InstallShield Wizard Complete] screen.

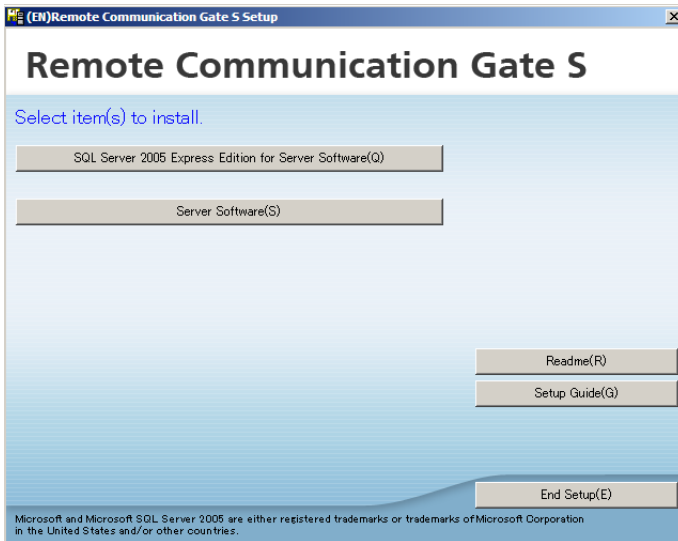


DB instance (RDHWEBSERVICE) is now added.

You can confirm it on the [SQL Server 2005 Network Configuration] screen.

Step2: Install Remote Communication Gate S

1. On the initial screen, select "Server Software".



2. Read the warning, and then click [OK].
3. Click [Next>].

4. Read the terms of the license agreement, and if you agree, click [Yes].

5. Enter [User Name] and [Company Name], and then click [Next>].

↓ Note

- For [User Name] and [Company Name], enter the user name and company name registered in the product.

6. Check the folder for the installation is the correct folder, and then click [Next>]. To change the folder, click [Browse...]. Select a different folder, and then click [Next>].

! Limitation

- Double-byte characters cannot be used in the destination folder name.

7. Check the folder where software data is to be saved is the correct folder, and then click [Next>]. To change the folder, click [Browse...]. Select a different folder, and then click [Next>].

↓ Note

- Software data refers to the installation package prepared by the Packager and the device firmware. The installation package and firmware are managed, respectively, by Package Management and Firmware Management. For details about Package Management and Firmware Management, see the Administrator Operations Guide.

8. Check the folder where log data is to be saved is the correct folder, and then click [Next>]. To change the folder, click [Browse...]. Select a different folder, and then click [Next>].

↓ Note

- Log data refers to Job Logs and Access Logs collected by the Log Management function from the device. For details about Log Management, see the Administrator Operations Guide.

9. When the authentication screen appears, select whether or not to allow inheriting of authentication details, and then click [Next>].

↓ Note

- Select [Yes] to inherit the authentication information to Remote Communication Gate S.

10. Check the network address is correct, and then click [Next>].

11. Select either [Apache] or [Internet Information Services (IIS)] as the Web server type in use and click [Next>].

↓ Note

- You can only choose Apache when IIS is not installed. To use IIS, install IIS first, and then launch the Web service.
- If Apache is selected as the Web server type, regular maintenance of the server's access logs is required.

Reference

- For details about performing regular maintenance of Apache Web server access logs, see "Managing Web Server Log Files", Administrator Operations Guide.
- For details about the IIS installation, see p.26 "Web Server Settings".
- It may be possible to select IIS depending on the OS in use. See Microsoft's online help Web site for the IIS installation method.

12. Enter each port number for [HTTP] and [HTTPS] that the Web server will use, and then click [Next>].

★ Important

- Port numbers cannot be changed after the installation. To change the port numbers, you must first uninstall and then reinstall Remote Communication Gate S.
- When moving Remote Communication Gate S to another server, the Authentication Manager backup must be restored on the new server. To do this, you must specify the same port number as was used to save the backup data on the original server. The Authentication Manager backup can be restored only if the same port number is specified.
- Set the HTTP or HTTPS ports so that they do not conflict with other connections and services running on the computer.

13. Enter the SA password set when SQL Server 2005 was installed, and then click [Next>].

14. Check your setup, and then click [Next>] to start the installation of Remote Communication Gate S.

★ Important

- When the [Windows Security Alert] dialog box appears, click [Unblock] and continue installation.

15. Make sure you select [Yes, I want to restart my computer now.], and then click [Finish] to restart Windows.

16. On the logon window, log on to Windows with the logon user that performed the Remote Communication Gate S installation.

★ Important

- Installation will not continue if the logon user is different.

17. On the [Authorization for Server Access] dialog box, enter the Windows logon password in the [Password:] and [Confirm password:] text boxes and click [OK].

Settings differ according to the conditions of the server computer in which Remote Communication Gate S is installed.

Step3: Set authentication method

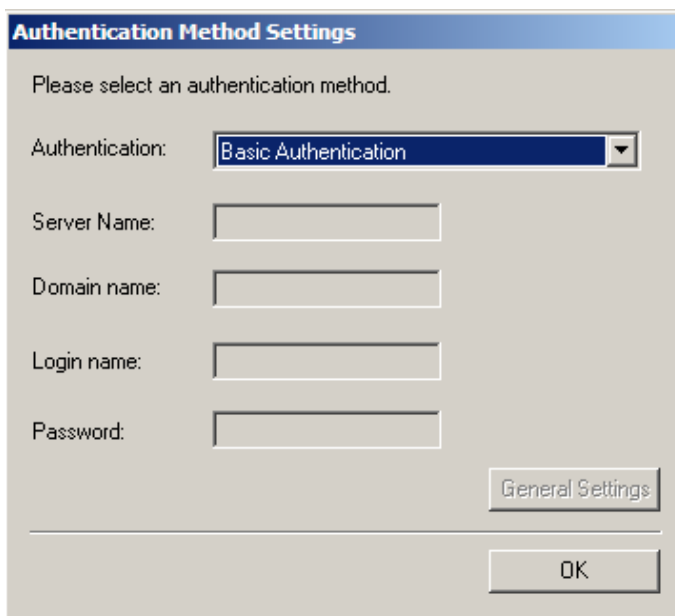
Preparation

- Decide the authentication method in advance. For details about the authentication method, see p.22 "Available Methods and Required Environments for Authentication".

Note

- When authenticating using Windows authentication (NT Compatible or Native), Notes authentication, NDS authentication, or LDAP authentication, it is necessary for the user to be registered as a member of the domain in advance.
- Authentication Manager is also installed on the server.
- The displayed screen differs according to the conditions of the server computer on which Remote Communication Gate S is installed.

1. On the [Authentication Method Settings] dialog box, select the authentication method.



Authentication Method Settings

Please select an authentication method.

Authentication: Basic Authentication

Server Name:

Domain name:

Login name:

Password:

General Settings

OK

2. Specify the required settings.

Information to be entered differs depending on the selected authentication method as follows:

Authentication Method	Explanation
Basic Authentication	<p>This is an authentication method for registering and managing unique authentication users. It is possible to develop a user authentication environment even if other authentication environments than basic authentication environment does not exist.</p> <p>No information is required for any of the items in the [Authentication Method Settings] dialog box.</p>
Windows Authentication (NT compatible)	<p>User accounts for the following domains constructed in the network are used.</p> <ul style="list-style-type: none"> • Windows NT domain • Windows 2000 Active Directory domain (mixed mode, NT compatible access allowed mode) • Windows Server 2003 Active Directory domain (mixed mode, Windows Server 2003 intermediate) • Windows Server 2008 Active Directory domain (mixed mode, Windows Server 2008 intermediate) <p>No information is required for any of the items in the [Authentication Method Settings] dialog box.</p>
Windows Authentication (native)	<p>User accounts of domains constructed in the network are used.</p> <ul style="list-style-type: none"> • Windows 2000 Active Directory domain (native mode, Windows 2000 only access allowed mode) • Windows Server 2003 Active Directory domain (native mode, Windows Server 2003 intermediate) • Windows Server 2008 Active Directory domain (native mode, Windows Server 2008 intermediate) <p>Enter logon information used to access the domain in [Login name:] and [Password:] of the [Authentication Method Settings] dialog box.</p>

Authentication Method	Explanation
Notes Authentication	<p>User accounts of Notes domains constructed in the network are used.</p> <p>Enter the following data in the items of the [Authentication Method Settings] dialog box.</p> <ul style="list-style-type: none"> • [Server name:] Enter Notes server name. • [Domain name:] Enter the name of the domain with which the Notes server is affiliated. • [Login name:] Enter the user name registered in the Notes server. • [Password:] Enter the password for the user name.
NDS Authentication	<p>Uses network user names and passwords.</p> <p>Enter the following in the fields of the [Authentication Method Settings] dialog box:</p> <ul style="list-style-type: none"> • [Login name:] The user name registered in the Novell server. • [Password:] The password set for the user name. <p>You can change the authentication server settings by clicking [General Settings].</p>
LDAP Authentication	<p>Uses network user names and passwords.</p> <p>Enter the following data in the fields of the [Authentication Method Settings] dialog box:</p> <ul style="list-style-type: none"> • [Login name:] The user name registered in the LDAP server. • [Password:] The password set for the user name. <p>You can change the authentication server settings by clicking [General Settings].</p>

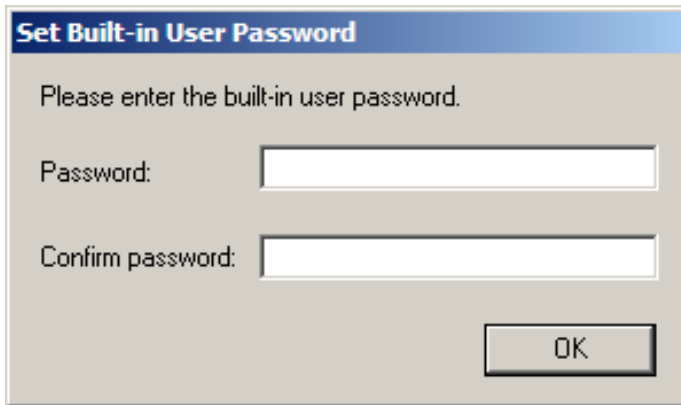
Note

- If Authentication Manager is already installed and a built-in user password has been set, the authentication method set by the previously installed Authentication Manager will be selected in the [Authentication Method Settings] dialog box. Enter the required information, and then click [OK] to proceed.

2**Step4: Set built-in password**

1. In the [Set Built-in User Password] dialog box, enter the password of the administrator with special authority to develop Remote Communication Gate S.

The administrator's user name is "Admin". The administrator has authority for all management operations including Authentication Manager.



2. Click [OK].

Important

- If you forget the built-in password, you will no longer be able to log on as "Admin". If that happens, you must reinstall Remote Communication Gate S since it is not possible to recover the password. Take care to avoid forgetting the built-in password.

This completes the installation of Remote Communication Gate S.

It is necessary to perform the activation in order to use the installation support tool properly.

Step5: Activate Remote Communication Gate S**Important**

- If you do not activate Remote Communication Gate S within 45 days after installation, it will become unavailable.

1. Click [Start] > [All Programs] > [Remote Communication Gate S] > [Activation Tool].

★ Important

- If User Access Control (UAC) is enabled on your system, you must run Activation Tool as an administrator. To do this, right-click Activation Tool and select [Run as Administrator]. If UAC is enabled and you do not run Activation Tool as an administrator, the activation function will not run correctly, and you will not be able to Remote Communication Gate S.

2. On the Activation List screen, click [Next>].

↓ Note

- In this list box, the product name that has been already activated is displayed. If this is the first time activation after you purchased it, nothing appears in the list box.

3. Follow the operations displayed on the screen to make settings for obtaining the Remote Communication Gate S license.

If you already have a License code, select [Enter License Code] and click [Next>]. Enter the License code, and then click [Next>]. This completes activation.

If you do not have a License code, proceed to step 4.

4. Under [Activation Method], select [Internet].

The product registration wizard opens in a Web browser.

↓ Note

- If the computer cannot connect to the Internet, access the following URL using a different computer, and then acquire the License Code. Then set the Activation Method to Enter license code, and register the License Code you receive.
- <https://www.onlineactivation.net>

5. Read the privacy statement thoroughly. Select the [I Agree] checkbox, and then click [Next].
6. From the drop-down list on the [Privacy Statement] screen, select the language you want to use for the activation.
7. Click [Help] to download the activation guide.
8. Follow the procedures in the activation guide to register user information and receive a License Code.
9. Copy and paste the License code into the text box on the Activation Tool, and then click [Next>].

This completes activation.

After completing the activation procedure for Remote Communication Gate S, you must configure the initial settings. For details, see p.51 "Setup Wizard".

If you want to use @Remote service, an additional contract and activation are required. For activation method, proceed to "Step6: Activate @Remote service". For details, contact your service representative.

Step6: Activate @Remote service

Activation of the @Remote service can only be performed by a Customer Engineer. For details, contact your service representative.

1. Click [Start] > [All Programs] > [Remote Communication Gate S] > [Activation Tool].

★ Important

- If User Access Control (UAC) is enabled on your system, you must run Activation Tool as an administrator. To do this, right-click Activation Tool and select [Run as Administrator]. If UAC is enabled and you do not run Activation Tool as an administrator, the activation function will not run correctly, and you will not be able to Remote Communication Gate S.

2. On the Activation List screen, click [Next>].

↓ Note

- In this list box, the product name that has been already activated is displayed. If this is the first time activation after you purchased it, nothing appears in the list box.

3. Follow the operations displayed on the screen to make settings for obtaining the Remote Communication Gate S license.

If you already have a License code, select [Enter License Code] and click [Next>]. Enter the License code, and then click [Next>]. This completes activation.

If you do not have a License code, proceed to step 4.

↓ Note

- Contents of the Activation screen are subject to change without prior notice.

4. Under [Activation Method], select [Internet].

The product registration wizard opens in a Web browser.

↓ Note

- If the computer cannot connect to the Internet, access the following URL using a different computer, and then acquire the License Code. Then set the Activation Method to Enter license code, and register the License Code you receive.
- <https://www.onlineactivation.net>

5. Read the privacy statement thoroughly. Select the [I Agree] checkbox, and then click [Next].
6. From the drop-down list on the [Privacy Statement] screen, select the language you want to use for the activation.
7. Click [Help] to download the activation guide.
8. Follow the procedures in the activation guide to register user information and receive a License Code.

9. Copy and paste the License code into the text box on the Activation Tool, and then click [Next>].

This completes activation.

Overwrite Installation

Select this installation type if you are reinstalling Remote Communication Gate S on a server computer that already has the same or an earlier version installed or if you are upgrading from Web SmartDeviceMonitor Professional IS/Standard, and want to retain the earlier version's data, such as network addresses or port numbers.

Reinstalling Remote Communication Gate S

Use the following procedure to reinstall Remote Communication Gate S on a computer on which the same version of Remote Communication Gate S is already installed. Performing a reinstall allows you to retain the previous installation's data, such as network addresses and port number settings.

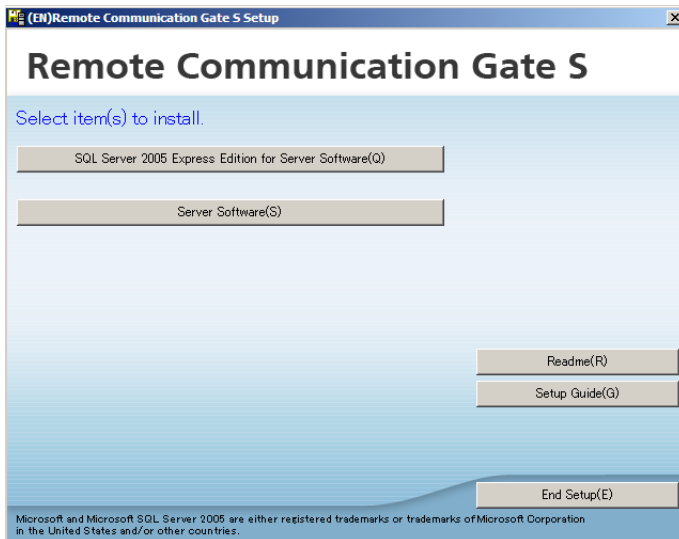
★ Important

- Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.

↓ Note

- After you upgrade to Remote Communication Gate S Pro, you should download and reinstall Packager. For details, see "Download and install Packager", Administrator Operations Guide.

1. Double-click RDLaunch.exe.
2. On the initial screen, select "Server Software".



3. Read the warning, and then click [OK].
4. Click [Next>].

5. Check your setup, and then click [Next>].

★ Important

- If the [Windows Security Alert] dialog box appears, click [Unblock] and continue installation.

6. Make sure you select [Yes, I want to restart my computer now.], and then click [Finish] to restart Windows.

7. On the logon window, log on to Windows with the logon user that performed the Remote Communication Gate S installation.

★ Important

- Installation will not continue if the logon user is different.

8. On the [Authentication for Server Access] dialog box, enter the Windows logon password in the [Password:] and [Confirm password:] text boxes and click [OK].

9. Set the authentication method.

For details, see p.35 "Step3: Set authentication method".

10. Set the built-in password.

For details, see p.38 "Step4: Set built-in password".

11. Perform the activation procedure if necessary.

For details, see p.38 "Step5: Activate Remote Communication Gate S".

Upgrading from an Earlier Version of Remote Communication Gate S

Use the following procedure to install Remote Communication Gate S on a computer on which an earlier version of Remote Communication Gate S is already installed. Performing an upgrade allows you to retain the previous installation's data, such as network addresses and port number settings.

★ Important

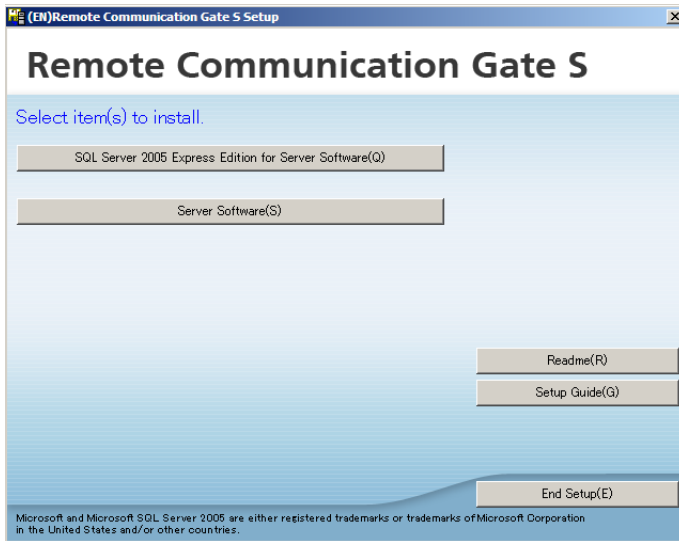
- Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.

↓ Note

- After you upgrade to Remote Communication Gate S Pro, you should download and reinstall Packager. For details, see "Download and install Packager", Administrator Operations Guide.
- It is not possible to upgrade from Remote Communication Gate S to Remote Communication Gate S Pro by performing an overwrite installation: You must first uninstall Remote Communication Gate S and then install Remote Communication Gate S Pro. For details, see p.29 "New Installation".

1. Double-click RDLaunch.exe.

2. On the initial screen, select "Server Software".



3. Read the warning, and then click [OK].
4. Click [Yes].
5. Click [Next>].
6. Enter the SA password, and then click [Next>].
7. Check your setup, and then click [Next>].

★ Important

- If the [Windows Security Alert] dialog box appears, click [Unblock] and continue installation.

8. Make sure you select [Yes, I want to restart my computer now.], and then click [Finish] to restart Windows.
9. On the logon window, log on to Windows with the logon user that performed the Remote Communication Gate S installation.

★ Important

- Installation will not continue if the logon user is different.

10. On the [Authentication for Server Access] dialog box, enter the Windows logon password in the [Password:] and [Confirm password:] text boxes and click [OK].
11. Set the authentication method.
For details, see p.35 "Step3: Set authentication method".
12. Set the built-in password.
For details, see p.38 "Step4: Set built-in password".
13. Perform the activation procedure if necessary.
For details, see p.38 "Step5: Activate Remote Communication Gate S".

Upgrading from Web SmartDeviceMonitor Professional IS/Standard

Use the following procedure to install Remote Communication Gate S on a computer on which Web SmartDeviceMonitor Professional IS/Standard is already installed. Performing an upgrade allows you to retain the previous installation's data, such as network addresses and port number settings.

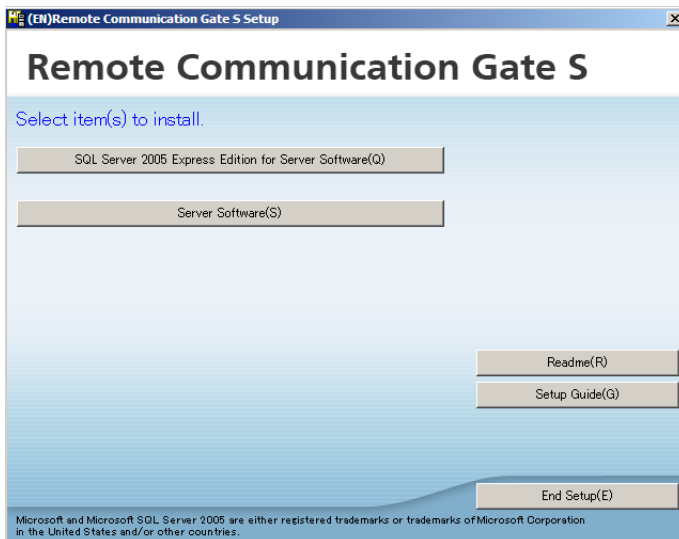
★ Important

- Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.
- If MSDE was used for Web SmartDeviceMonitor, it is necessary to install the SQL Server 2005. For details, see p.31 "Step 1: Install SQL Server 2005 Express Edition Service Pack 3". However, note that the SA password is not required.

↓ Note

- After you upgrade to Remote Communication Gate S, you should download and reinstall Packager. For details, see "Download and install Packager", Administrator Operations Guide.

1. Double-click RDLlaunch.exe.
2. On the initial screen, select "Server Software".



3. Read the warning, and then click [Yes].
4. Click [Yes].
5. Click [Next>].
6. Read the terms of the license agreement. If you agree, click [Yes].
7. Enter the SA password, and then click [Next>].

8. Check your setup, and then click [Next>] to start the installation of Remote Communication Gate S.

★ Important

- If the [Windows Security Alert] dialog box appears, click [Unblock] and continue installation.

9. Make sure you select [Yes, I want to restart my computer now.], and then click [Finish] to restart Windows.

10. On the logon window, log on to Windows with the logon user that performed the Remote Communication Gate S installation.

★ Important

- Installation will not continue if the logon user is different.

11. On the [Authorization for Server Access] dialog box, enter the Windows logon password in the [Password:] and [Confirm password:] text boxes and click [OK].

12. Set the authentication method.

For details, see p.35 "Step3: Set authentication method".

13. Set the built-in password.

For details, see p.38 "Step4: Set built-in password".

14. Perform the activation procedure.

For details, see p.38 "Step5: Activate Remote Communication Gate S".

★ Important

- Discovery settings cannot be retained, and device polling settings return to their default values. Login to Remote Communication Gate S, and configure these settings again if required.
- If devices are registered but Remote Communication Gate S has been unable to establish a connection, click [Refresh Selected Device] to update the database information, and then click [Refresh] to display the updated list information.
For details, see "Device Management Settings", Administrator Operations Guides.

3. After Installation

This chapter explains the initial setup procedure for Remote Communication Gate S after installation.

Access Remote Communication Gate S

To access Remote Communication Gate S, use one of the following procedures.

Access from Server Computer's Start Menu

3

On the computer where you installed Remote Communication Gate S, you can access the Remote Communication Gate S web interface from the [Start] menu.

On the [Start] menu, point to [All Programs] > [Remote Communication Gate S], and then select [StartBrowser].

Access from Web Browser

You can access the Remote Communication Gate S Web interface from any computer on the local network.

Condition	URL
Without SSL encryption	http://{host name}:{port number}/mgmt or http://{IP address}:{port number}/mgmt
With SSL encryption	https://{host name}:{port number}/mgmt or https://{IP address}:{port number}/mgmt

- {host name}: name of the Remote Communication Gate S server
- {IP address}: IP address of the Remote Communication Gate S server
- {port number}: port number specified when Remote Communication Gate S was installed

For example:

- http://192.168.17.21:8080/mgmt
- https://intra.example.org:8443/mgmt

Note

- If 80 is used as the port number, you can omit it from the URL. For example,

`http://intra.example.org/mgmt`

- The page located at `/mgmt` is for redirection purposes only. When you access Remote Communication Gate S at `http://xxx:xx/mgmt`, you are redirected to the actual login page.
- The default port numbers differ depending on the type of Web server you are using: For details, see p.21 "Communication Ports".

Reference

- For details about secure connections, see "Encrypting Communication Channels", Administrator Operations Guide.

Login to Remote Communication Gate S

The login screen is displayed when you access Remote Communication Gate S via its URL.

1. Enter the built-in user information.

- [User name:] Admin
- [Password:] built-in password
- [Domain name:] blank

Note

- [Domain name:] is not displayed if Basic authentication, NDS authentication, or LDAP authentication is selected as the authentication method.

2. Click [Login].

When no devices are registered, the [Settings] screen appears when you log in.

Important

- When using Remote Communication Gate S, do not use your browser's [Back] button or other browser functions. Use only the navigation controls on the content pages.
- If you want to switch users, click the [Logout] button, and then log in again as a different user. Do not use your browser's [Back] button to redisplay the login screen.

 **Note**

- If you are using Remote Communication Gate S for the first time, take a moment to read the information that appears when you click the [Readme] icon. This information explains the limitations of Remote Communication Gate S and provides instructions for its use. To close this screen, click [Close].
- For details about operating procedures, see "Contents Help" for the various functions. Contents Help is displayed by clicking the [Help Contents] button in the header area of each operation screen. The content displayed differs depending on the login user (administrator, general user).

Setup Wizard

After the installation, configure the initial settings to use Remote Communication Gate S.

Initial Settings

Initial Settings Wizard consists of six screens:

On the [Settings] screen, click [Initial Settings Wizard] to start the wizard.

1. Group Settings

Create new categories and groups for the management of printers.

2. HTTP Proxy Settings

Select whether to use a proxy server when connecting to the global server, and then configure the proxy server settings if necessary.

3. Email Settings

Configure the SMTP server settings so that Remote Communication Gate S can send notification e-mails.

4. Device Polling Settings

Set the polling time and timeout to collect the device status.

5. Discovery Settings

Configure the settings for automatic printer discovery.

6. Settings completion screen

↓ Note

- Even after you complete the Initial Settings Wizard, you can still access the wizard from the [Settings] screen. For the details of each setting, see Administrator Operations Guide.

Group Settings

Create new categories and groups for the management of printers.

Categories and groups

You can register devices in groups and manage them. Devices can be easily managed by registering them in groups by office, location, use, etc. Once you are able to use the following categories and groups effectively, you will be able to search for devices to be managed in the department category or identify devices with problems in the floor category.

- Category

You must create categories to perform group management. You can consolidate groups into preferred categories such as by department, by floor, etc. You can reflect office management structures by creating multiple categories and registering groups and devices to match the categorization.

- Group

Groups are added to categories. You can also create groups in other groups to create a nested structure.

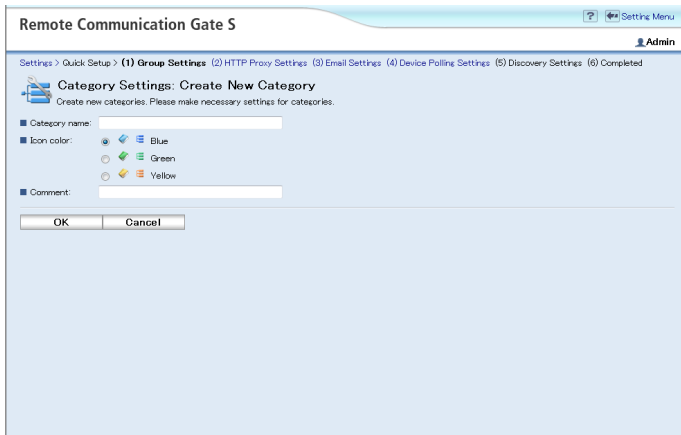
You can manage devices by group by registering them in groups. For a group, you can specify a recipient to be notified when a device error occurs.

! Limitation

- You cannot register devices directly in categories.
- A device cannot be registered to multiple groups within the same category, but it can be registered to a group in another category.
- You can create a maximum of three categories.
- You can create up to five group tiers within categories.

Creating categories

1. Click [Create] > [New Category].
2. Set each item on the [Category Settings: Create New Category] screen.



Setting	Description
Category name:	Enter the name of newly created category.

Setting	Description
Icon color:	Select an icon color for a newly created group database. <ul style="list-style-type: none"> • [Blue] • [Green] • [Yellow] <div style="border: 1px solid blue; border-radius: 10px; padding: 2px; display: inline-block; margin-top: 5px;"> ↓ Note </div> <ul style="list-style-type: none"> • Default: [Blue]
Comment:	Enter any relevant comments to append to the newly created category.

3

3. Click [OK].

Creating groups

1. Select the Category in which you want to create a group, and then click [Create] > [New Group].
2. On the [Group Settings: Create New Group] screen, set each item.

Setting	Description
Group location:	Displays the location of the group.
Group name:	Enter the name of the group you want to create.
Comment:	Enter any necessary comments to append to newly created group.
Email address list for error notification:	Leave this item blank for the initial settings.

3. Click [OK].

For details about other settings, batch grouping, or creating a map, see Administrator Operations Guide.

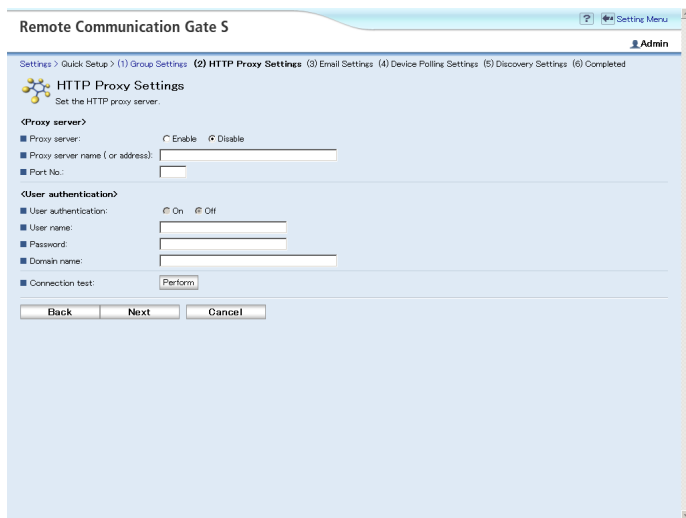
4. Click [Next].

HTTP Proxy Settings

Select whether to use a proxy server when connecting to the global server, and then configure the proxy server settings if necessary.

3

1. On the [HTTP Proxy Settings] screen, set each item.



<Proxy server>

Setting	Description
Proxy server:	<p>Select whether your network uses a proxy server to connect to the Internet.</p> <ul style="list-style-type: none"> [Enable] Connection is through a proxy server. [Disable] Connection is direct (not through a proxy server). <p>Note</p> <ul style="list-style-type: none"> Default: [Disable]
Proxy server name (or address):	Enter the IP address or host name of the proxy server.

Setting	Description
Port No.:	Enter the port number to use for communicating with the proxy server.

<User authentication>

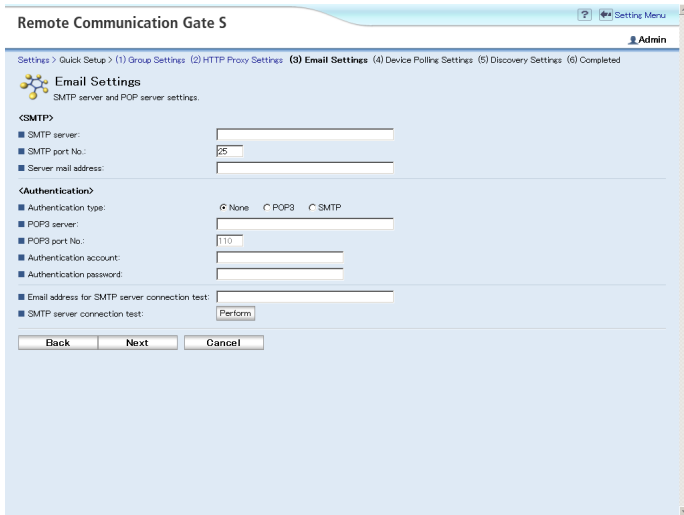
Setting	Description
User authentication:	<p>Specify whether to perform authentication when connecting to the proxy server.</p> <ul style="list-style-type: none"> • [On] • [Off] <p>Note</p> <ul style="list-style-type: none"> • Default: [Off]
User name:	Enter the user name for authentication.
Password:	Enter the password for authentication.
Domain name:	Enter the domain name for authentication.
Connection test:	Click [Perform] to test the connection to the proxy server.

2. Click [Next].

Email Settings

Configure the SMTP server settings so that Remote Communication Gate S can send notification e-mails.

1. On the [Email Settings] screen, set each item.



3

<SMTP>

Setting	Description
SMTP server:	Enter the SMTP server host name or IP address.
SMTP port No.:	Enter the port number used for SMTP. <div style="border: 1px solid blue; border-radius: 10px; padding: 2px; display: inline-block;"> ↓ Note </div> <ul style="list-style-type: none"> Default: 25
Server mail address:	Enter the mail address of the SMTP server.

<Authentication>

Setting	Description
Authentication type:	Either POP3 or SMTP is designated for authentication. <ul style="list-style-type: none"> [None] [POP3] [SMTP] <div style="border: 1px solid blue; border-radius: 10px; padding: 2px; display: inline-block;"> ↓ Note </div> <ul style="list-style-type: none"> Default: [None]
POP3 server:	Enter the IP address or host name of the POP3 server that will provide authentication.
POP3 port No.:	Enter the port number to use when communicating with the POP3 server.

Setting	Description
Authentication account:	Enter the user name for authentication with the POP3 server.
Authentication password:	Enter the password for authentication with the POP3 server.

Setting	Description
Email address for SMTP server connection test:	Enter an e-mail address. A test e-mail will be sent to the address to confirm that the SMTP server settings are correct.
SMTP server connection test:	Click [Perform]. A test e-mail will be sent to the e-mail address specified in [Email address for SMTP server connection test:].

3

2. Click [Next].

Device Polling Settings

Set the polling time and timeout to collect the device status.

1. On the [Device Polling Settings] screen, specify each setting.

Remote Communication Gate 5

Settings > Quick Setup > (1) Group Settings > (2) HTTP Proxy Settings > (3) Email Settings > (4) Device Polling Settings > (5) Discovery Settings > (6) Completed

Status Polling
Enter device status confirmation interval time.

- Interval between polling for status information: 1 hour(s)
- Polling interval time for tray, toner/ink information: 3 hour(s)
- Polling interval time for other information: 6 hour(s)
- Interval between collection of charge and administrator counters: 1 day(s)
- Polling timeout: 3 sec.

<Excluded IP Address>

Select All | Clear All | Remove

- Starting address: 0.0.0.0
- Ending address: 0.0.0.0
- Subnet mask: 255.255.255.0

Buttons: Back, Next, Cancel

Setting	Description
Interval between polling for status information	<p>Specify the frequency at which Remote Communication Gate S polls devices for their status. Enter a number and select [min.], [hour(s)], or [day(s)] from the menu.</p> <p>The time you specify here is the time that will elapse between polling.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: 1 hour
Polling interval time for tray, toner/ink information	<p>Specify the frequency at which Remote Communication Gate S polls devices for their paper tray levels, and toner/ink status. Enter a number and select [min.], [hour(s)], or [day(s)] from the menu.</p> <p>The time you specify here is the time that will elapse between polling.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: 3 hours
Polling interval time for other information	<p>Specify the frequency at which Remote Communication Gate S polls devices for other status information. Enter a number and select [min.], [hour(s)], or [day(s)] from the menu.</p> <p>The time you specify here is the time that will elapse between polling.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: 6 hours
Interval between collection of internal and administrator counters	<p>Specify the frequency at which Remote Communication Gate S polls devices for the collection of administrator and internal counters. Enter a number and select [min.], [hour(s)], or [day(s)] from the menu.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: 1 day
Polling timeout:	<p>Enter the number of seconds to wait for a response from a device.</p> <p>If the machine receives no response when polling a device, it continues attempting polling for a specified period. Polling is cancelled after this period.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: 3 seconds

<Excluded IP Address>

Setting	Description
Starting address:	Enter the starting IP address of the IP address range that you want to exclude.
Ending address:	Enter the ending IP address of the IP address range that you want to exclude.
Subnet mask:	Enter the subnet mask of the IP address range that you want to exclude.
Add	Adds an IP address range to the list of IP address ranges that you want to exclude. Enter values in [Starting address:], [Ending address:], and [Subnet mask:], and then click [Add] to include an IP address range in the exclusion list.
Select All	Selects all entered IP address ranges.
Clear All	Deselects all entered IP address ranges.
Remove	Remove all selected IP address ranges from the exclusion list.

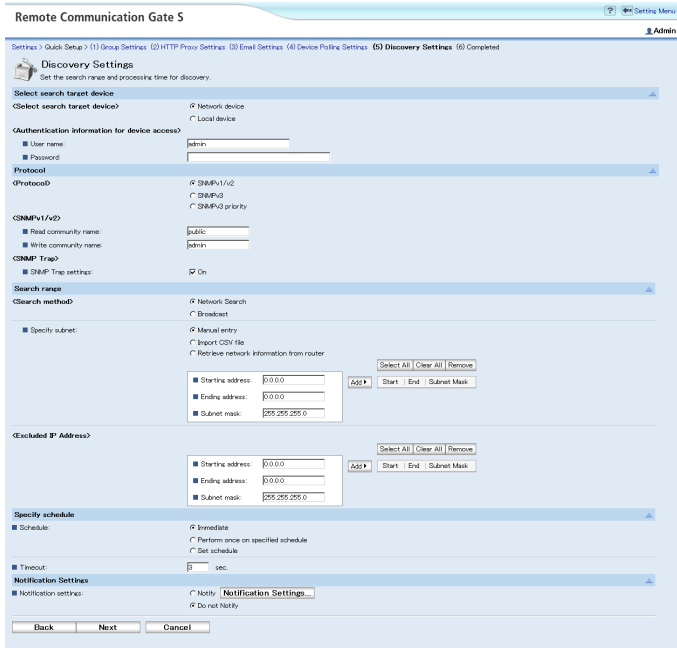
2. Click [Next].**Discovery Settings**

Configure the settings for automatic printer discovery.

↓ Note

- You cannot change discovery function settings while discovery is running.
- Click [Cancel] to cancel editing of the discovery settings.

1. On the [Discovery Settings] screen, set each item.



Select search target device

Setting	Description	
Select search target device	Select the discovery target. <ul style="list-style-type: none"> [Network device] [Local device] <p>Note</p> <ul style="list-style-type: none"> Default: [Network device] 	
Authentication information for device access	User name:	Enter the user name of the account. <p>Note</p> <ul style="list-style-type: none"> Default: admin
	Password:	Enter the password of the account.

Search account for local device

Setting	Description
User name:	Enter the user name of the account. Enter the account name of the domain administrator.



Setting	Description
Password:	Enter the password of the account.
Domain name:	Enter the name of the domain that you want to search.

Protocol

Setting	Description
Protocol	<p>Select the protocol to use for discovery.</p> <ul style="list-style-type: none"> • [SNMPv1/v2] • [SNMPv3] • [SNMPv3 priority] <p>Note</p> <ul style="list-style-type: none"> • Default: [SNMPv1/v2]
SNMPv1/v2	<p>Read community name:</p> <p>Enter the community name for read access to the printers.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: public
	<p>Write community name:</p> <p>Enter the write community name for write access to the printers.</p> <p>Note</p> <ul style="list-style-type: none"> • Default: admin

Setting	Description	
SNMPv3	User name:	Enter the user name of a device administrator set in the device. Note <ul style="list-style-type: none"> • Default: admin
	Password:	Enter the password for the user name set in the device.
	Confirm password:	Enter the password again. This must be the same as the password entered above.
	Authentication algorithm:	Select the encryption algorithm for SNMPv3. <ul style="list-style-type: none"> • [MD5] Select when specifying a device using the MD5 authentication algorithm. • [SHA1] Select when specifying a device using the SHA1 authentication algorithm. Note <ul style="list-style-type: none"> • Default: [MD5]
	Encryption password:	Enter the encryption password set in the device.
	Confirm encryption password:	Re-enter the password to use for encryption. This must be the same as the password entered previously.
	Context name:	Enter the context name set in the device.
SNMP Trap	SNMP Trap settings:	Check this check box to automatically set the device Trap. Note <ul style="list-style-type: none"> • Default: [On]

Search range

Setting	Description	
Search method	Select which method to use for search. <ul style="list-style-type: none"> [Network Search] [Broadcast] <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 2px; display: inline-block;">  Note </div> <ul style="list-style-type: none"> Default: [Network Search] 	
Specify subnet	Specify the subnet mask. <ul style="list-style-type: none"> [Manual entry] Manually input the IP address ranges or subnets to search within. [Import CSV file] Specify a CSV file that contains the IP address ranges or subnets to search within. [Retrieve network information from router] Specify a subnet, and obtain the subnet information from routers on the subnet. <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 2px; display: inline-block;">  Note </div> <ul style="list-style-type: none"> Default: [Manual entry] 	
Excluded IP Address	Starting address:	Enter the first IP address in the IP address range.
	Ending address:	Enter the last IP address in the IP address range.
	Subnet mask:	Enter the subnet mask for the IP addresses.
	Add	Adds an IP address range to the list of IP address ranges that you want to exclude. Enter values in [Starting address:], [Ending address:], and [Subnet mask:], and then click [Add] to include an IP address range in the exclusion list.
	Select All	Selects all entered IP address ranges.
	Clear All	Deselects all entered IP address ranges.
	Remove	Remove all selected IP address ranges from the exclusion list.

Specify schedule

Setting	Description
Schedule:	<p>Specify the discovery schedule.</p> <ul style="list-style-type: none"> [Immediate] Perform discovery immediately after you have finished configuring the discovery settings. [Perform once on specified schedule] Perform discovery once on the specified day and time. [Set schedule] Perform discovery periodically. <p>Note</p> <ul style="list-style-type: none"> Default: Immediate
Timeout:	<p>Enter the number of seconds to wait for a response from printers.</p> <p>Note</p> <ul style="list-style-type: none"> Default: 3 seconds

Notification settings

Setting	Description
Notification settings:	<p>Select whether to receive notification when the discovery has completed.</p> <ul style="list-style-type: none"> [Notify] Click [Notification Settings...] and edit the settings. [Do not Notify] Do not send notification e-mail. <p>Note</p> <ul style="list-style-type: none"> Default: [Do not Notify]

2. Click [Next].

3. On the [Discovery Task List] screen, confirm the discovery tasks.

Note

- You can configure discovery to be automatically performed on a periodic basis. For details, see "Discovery Settings", Administrator Operations Guide.

4. Click [Next].

Device discovery will be performed according to your settings. Depending on your network environment, discovery may take some time to complete. When discovery has finished, the Remote Communication Gate S initial setup is complete.

After initial setup is complete, you can perform other tasks such as adding users and configuring log settings. For details, see "What You Can Do with Remote Communication Gate S", Administrator Operations Guide.

4. Uninstallation

This chapter explains the procedures for uninstalling Remote Communication Gate S.

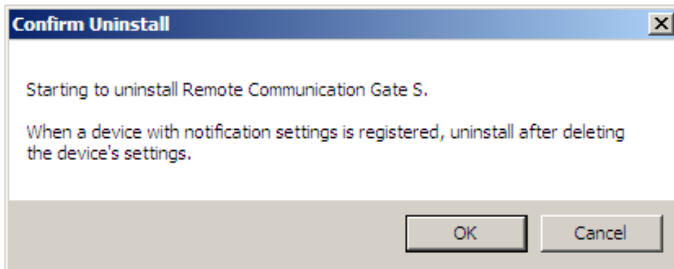
Uninstallation

For details about making a backup using ManagementTool and Authentication Manager, see "Backing Up Server Data" and "Maintenance of Remote Communication Gate S Server", Administrator Operations Guide.

★ Important

- If any devices are set to log transfers, disable log transfer for those devices before uninstalling Remote Communication Gate S. For details, see "Device Log Transfer Settings", Administrator Operations Guide.
- To uninstall Remote Communication Gate S, log on to Windows as the same administrator who performed the installation.
- SQL Server 2005 is not uninstalled with the uninstallation of Remote Communication Gate S. Perform the same uninstallation procedures from [Programs and Features] to uninstall SQL Server 2005.
- If you are using the @Remote service, a confirmation dialog box appears. To uninstall Remote Communication Gate S correctly, you must cancel the contract for @Remote service before you begin the uninstallation procedure. For details, contact your service representative.

1. From the Windows [Start] menu, click [Control Panel].
2. Click [Programs and Features].
3. Select this software, and then click [Uninstall].
4. On the [Confirm Uninstall] dialog box, click [OK].



5. Enter the SA password, and then click [OK].
6. Select whether to retain the authentication information, and then click [Next>] to start uninstallation.

When the uninstallation has completed, the [Uninstall Complete] dialog box appears.

7. Make sure you select [Yes, I want to restart my computer now.], and then click [Finish] to restart Windows.

Files Remaining after Uninstallation

The folders listed below and some of the files they contain remain stored in the computer after uninstallation (assuming Remote Communication Gate S is installed in drive C):

- Log files in:
 - C:\Program Files\Common Files\RDH Shared2
 - C:\Program Files\Common Files\RDH Shared2\reg
 - C:\Program Files\RMWSDMEX\bin
 - C:\Program Files\RMWSDMEX\atremote
 - C:\Program Files\Common Files\RDHWebService
- Files in:
 - C:\Program Files\Common Files\RDH Shared2\bin
 - C:\Program Files\Common Files\RDH Shared2\bin\log

5. Appendix

Troubleshooting

If problems occur during setup of Remote Communication Gate S, take the remedial actions indicated in the following table.

Problem	Cause and Solutions
Remote Communication Gate S has not been installed correctly.	To install Remote Communication Gate S, you must log on to Windows as an Administrators group member.
	Uninstall any earlier versions of Remote Communication Gate S before installing a new version.
	After installation when you restart the computer, you must log in to Windows as the same user who performed installation.
	The port numbers assigned to Remote Communication Gate S conflict with the port numbers of other services running on your computer, such as SMTP (port 25) or FTP (ports 20/21). Reinstall Remote Communication Gate S and set the ports again so that they do not conflict with other connections and services.
The login screen reappears after a certain amount of time has passed.	The Login screen reappears if no operation is performed for more than 30 minutes after logging in to the Remote Communication Gate S server. Log in on the login screen again and resume operations.
A message is displayed indicating that the designated port cannot be used during Remote Communication Gate S installation.	If Remote Communication Gate S is uninstalled and then reinstalled on a computer using IIS, it is not possible to use IIS because the previous port is reserved. Take either of the following two steps. <ul style="list-style-type: none">• Specify a port number different from that previously used.• Activate Internet Service Manager and delete sites that use the port. For details about Internet Service Manager, see Microsoft's online help Web site.
An error message "Failed to connect to the authentication management service." appears during Remote Communication Gate S installation.	If your Web server is using IIS, check that the appropriate IIS version is installed. If the appropriate IIS version is not installed, install it, and then reinstall Remote Communication Gate S.

Problem	Cause and Solutions
Remote Communication Gate S has not been uninstalled correctly.	<p>Stop the Remote Communication Gate S service before you uninstall.</p> <p>To uninstall Remote Communication Gate S, you must log on to Windows as an Administrators group member.</p>
The Remote Communication Gate S login screen does not appear.	<p>The port number entered in the client computer is not correct.</p> <p>Enter the correct port number for the Remote Communication Gate S server. The default port number is "8080" when using the Apache web server, and "80" when using the IIS web server.</p> <p>The Web server port is being blocked by a firewall. Refer to p.21 "Communication Ports" to set the Web server port as a firewall exception.</p> <p>The computer name of the Remote Communication Gate S server contains characters other than alphanumeric characters and hyphens.</p> <p>Change the server's computer name so that it only contains the characters A-Z, a-z, 0-9, and hyphens.</p>
The device list or other lists do not appear when connecting via SSL.	<p>You might have enabled the saving of encrypted pages. To turn off this function:</p> <ol style="list-style-type: none"> 1. On the Internet Explorer menu bar, click [Tools] > [Internet Options...], and then select the [Advanced] tab. 2. Clear the [Do not save encrypted pages to disk] check box. 3. Click [OK].
Immediately after updating or re-installing Remote Communication Gate S, device information migrated from the earlier version appears gray.	<p>Until Remote Communication Gate S detects the device, device information is grayed out. Wait until the device is detected.</p>
Only one account, "Admin", is provided after updating or re-installing Remote Communication Gate S.	<p>Account settings are not preserved, unlike device information. Add accounts as required.</p>

INDEX

@Remote requirements.....	19
@Remote service.....	9

A

About Remote Communication Gate S.....	9
Access Remote Communication Gate S.....	47
Activate	
@Remote service.....	40
Remote Communication Gate S.....	38
Activating browser JavaScript.....	27
Activation Tool.....	13
Administrator's computer requirements.....	17
After installation.....	47
Apache.....	33
Authentication	
Basic authentication.....	22, 36
LDAP authentication.....	23, 37
NDS authentication.....	23, 37
Notes authentication.....	23, 37
Windows authentication (native).....	22, 36
Windows authentication (NT compatible).....	22, 36
Authentication Manager.....	13
Authentication method.....	22, 35

B

Basic authentication.....	22, 36
Built-in password.....	30, 38

C

Category.....	51
Communication ports.....	21
Components.....	13

D

Device Polling Settings.....	57
Discovery Settings.....	59

E

Email Settings.....	55
---------------------	----

F

Files remaining after uninstallation.....	68
Firmware management.....	9

G

General user's computer requirements.....	18
Group.....	52
Group Settings.....	51

H

How to read this manual.....	1
HTTP Proxy Settings.....	54

I

Import LDAP Server Certificate.....	14
Initial Settings Wizard.....	51
Installation	
New installation.....	25, 29
Overwrite installation.....	25, 42
Required settings.....	26
Installation procedure.....	30
Installation support.....	9
Installation type.....	25
Internet Information Services (IIS).....	26, 33

J

JavaScript.....	27
-----------------	----

L

LDAP authentication.....	23, 37
License code.....	30
Log management.....	9
Login to Remote Communication Gate S.....	49

M

ManagementTool.....	13
---------------------	----

N

NDS authentication.....	23, 37
Network requirements.....	20
New installation.....	25, 29
Notes authentication.....	23, 37

O

Overwrite installation.....	25, 42
Reinstalling Remote Communication Gate S.....	42, 43
Remote Communication Gate S.....	43
Upgrading from Web SmartDeviceMonitor Professional IS/Standard.....	45

P

Package.....	2
Packager.....	2, 9
Pre-installation checks.....	9
Printer management.....	9

R

Required information for installation.....	29
Requirements	
@Remote service.....	19
Administrator's computer.....	17
General user's computer.....	18
Network.....	20
Server.....	15
System.....	15

S

SA password.....	29
Screens.....	2
Server requirements.....	15
Setup flow.....	24
Setup wizard.....	51
SQL Server 2005.....	13, 31
SSL Setting Tool.....	13
StartBrowser.....	13
Supported device.....	20
Symbols.....	1
System requirements.....	15

T

Terminology.....	1
Troubleshooting.....	69

U

Uninstallation.....	67
---------------------	----

W

Windows authentication (native).....	22, 36
Windows authentication (NT compatible).....	22, 36
Windows Firewall-excepted ports.....	26
Windows Server 2003 settings.....	26

Remote Communication Gate S

Installation Guide

