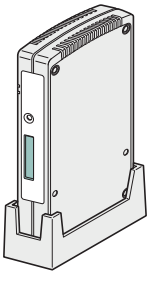
Remote Communication Gate A

Operating Instructions



Read this manual carefully before you use this machine and keep it handy for future reference. For safe and correct use, be sure to read "Safety Information" before using the machine.

How to Read This Manual

Symbols

The following set of symbols is used in this manual.

Important

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

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.

Notes

Contents of this manual are subject to change without prior notice.

Certain options might not be available in some countries. For details, contact your local dealer.

Some illustrations in this manual might be slightly different from the machine.

Depending on which country you are in, certain units may be optional. For details, please contact your local dealer.

About the Abbreviation

In these sheets, we use the term RC Gate as an abbreviation of Remote Communication Gate A. Generally, "administrator" refers to the "RC Gate administrator," unless otherwise specified in this Manual.

Screens

The explanations in this manual use screen images from Windows XP and Internet Explorer 6.0. If you use different OS, screen images may differ. However, you can perform the same steps.

Manuals for This Equipment

The following manuals describe procedures to operate and maintain this equipment. For safe and efficient operation of this equipment, all users should read and follow the instructions carefully.

Operating Instructions (this manual)

Provides all of the information on how to use this equipment. Perform the procedures in this manual after you have completed the procedures in "Setup Guide".

Safety Information/Setup Guide

Provides the information on safe usage of this equipment and how to install/set up it.

Note

- You need not perform the registration procedures explained in this manual if a customer engineer has already registered your equipment. However, in order to operate and maintain the equipment, you must read this manual carefully.
- Adobe Acrobat or Adobe Reader is necessary to view this manual in PDF format.

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®, and Microsoft Internet Explorer® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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 product names of Windows XP are as follows:

  Microsoft® Windows® XP Professional

  Microsoft® Windows® XP Home Edition

TABLE OF CONTENTS

4. Registering Devices with the Communication Server

5. Configuring the Details of the Registered Information

6. Appendix

1. About the RC Gate

This chapter will describe the outline of the RC Gate.

What Can be Done with the RC Gate

The following operations are available using the RC Gate:

- Send an automatic service call notifying the Communication Server that a device has malfunctioned.
- Update device firmware.
- Obtain device counter information and send it to the Communication Server.
- Automatically order new supplies, such as toner, when a device indicates that its supplies are low.
- Quickly check the usage status of multiple devices.

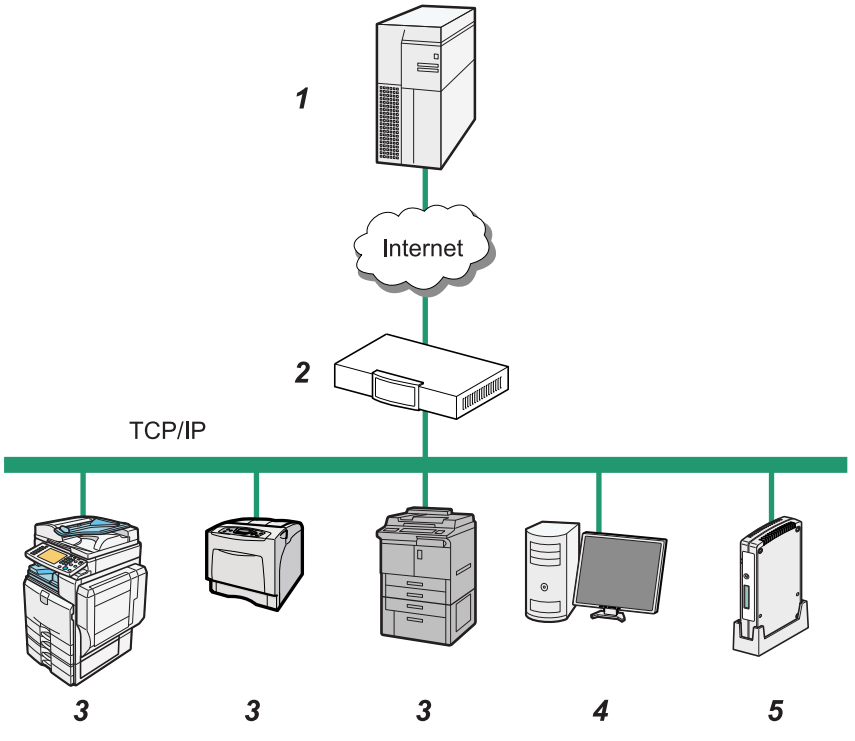
Outline of the System

The RC Gate communicates with the Communication Server over the Internet using HTTPS. Mutual authentication by HTTPS ensures the security of communication between the RC Gate and the Communication Server.

The Communication Server serves as the HTTPS server, and the RC Gate works as the HTTPS client.

Communication is possible when the following conditions are satisfied:

- Your environment is arranged to be able to access Web sites outside of your network.
- If the proxy server requires authentication, the account and password for the proxy server are available.



1. **Communication Server**

   Information sent for various services will be aggregated to this server.

2. **Proxy Server and/or Firewalls**

   You are able to use your proxy server and firewalls with this equipment. When using proxy server, Basic authentication, Digest authentication, and Windows authentication (only NTLMv2authentication available) can be used with this equipment.

3. **Device**

   A printer and multifunction machine can be managed by this equipment. This equipment can manage a maximum of 100 devices.

There are two types of devices managed by the RC Gate. One is compatible with HTTPS, and the other is compatible with SNMP. The user can identify the type by using the Device Registration Wizard or referring to "Connection Type" on the Registered Device List.

Mutual authentication in the HTTPS connection ensures the security of communication between the RC Gate and an HTTPS-compatible device. As a requirement for HTTPS-compatible devices, [Do not Prohibit] must be specified in "@Remote Service" under the Administrator Tools menu. For details about the relevant settings, see the manual for each device.

SNMPv1/v2 or SNMPv3 can be used for communication between the RC Gate and SNMP-compatible devices.

If you have installed optional memory and storage to expand the capacity, up to 1,000 devices can be registered. Contact your service representative for details.

For option information, see page 15 "About Options".

4. **Computer for Administration**

   You can manage this equipment by accessing the RC Gate Monitor via Web browser. For details, see page 16 "About the RC Gate Monitor".

5. **This Equipment (RC Gate)**

   Intermediates the managed devices and the Communication Server. Sends the device information to the Communication Server, and receives software to update the devices from the Communication Server.

   If you have installed optional memory, the RC Gate can acquire the device counter information specified by the Communication Server on a per user basis (by user code) and communicate it to Communication Server. Contact your service representative for details about services that use a per-user counter.

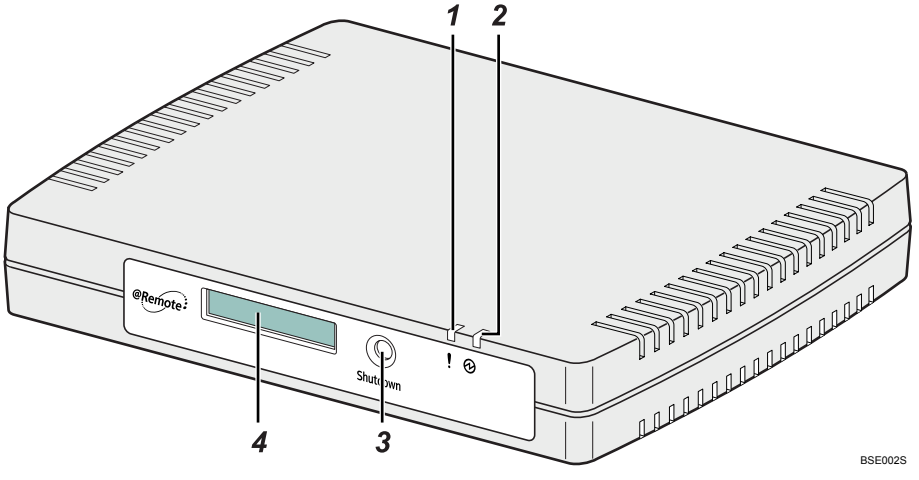
   For option information, see page 15 "About Options".

Guide to Equipment

This section explains names and functions of each part.

Front

This section explains names and functions of the parts on the front side of the RC Gate.



1. **! Error Status (Red)**

   Indicates different patterns depending on the status of the RC Gate:

   - The LED is on if the certificate has not been issued.
   - The LED blinks slowly in the following cases:
     - The entire service is suspended by user settings.
     - A communication error has occurred in the RC Gate.
   - The LED blinks fast in the following cases:
     - The communication with the communication server has been suspended.
     - A system error has occurred in the RC Gate.
     - The RC Gate has been suspended due to abnormal conditions.
   - The LED is off when communication between the RC Gate and Communication Server has been successfully established.

2. **Power (Green)**

   Lights green when the power of the RC Gate is on.

3. **Shutdown button**

   Shuts down the RC Gate when this button is pressed and held for five or more seconds.

If the power plug is disconnected before shutting down the RC Gate, the memory/storage will be damaged. In such a case, the latest logs, a maximum of an hour, will be lost. Be sure to shut down the RC Gate before disconnecting the power plug.

4. **Display**

   Displays the status of the RC Gate on the first line and the IP address of the RC Gate on the second line.

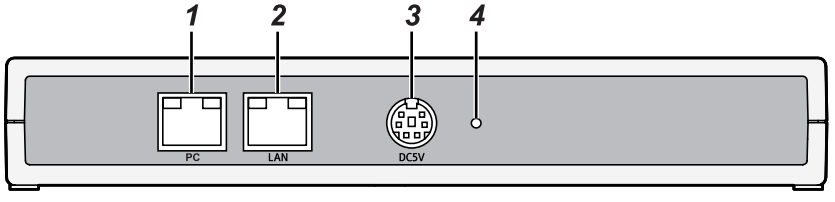
   If an error has occurred in the RC Gate, the second line displays an error message. For details about error messages, see page 141 "LCD Messages".

Note

- If the Error Status LED blinks or an error code is shown on the display, see page 143 "Troubleshooting".
- To restart the RC Gate, see page 123 "Restart RC Gate".

Back

This section explains names and functions of the parts on the back side of the RC Gate.



BSE003S

1. **PC Port (Maintenance port)**

   This port is used when a customer engineer performs maintenance, or when the designated administrator connects a PC to perform initial settings and registration of the RC Gate.

2. **LAN Port**

   The network (Ethernet) interface port to connect the RC Gate to the network. The default IP address is 192.168.0.2, but it can be changed.

3. **Power Socket**

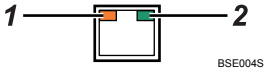
   Connect to the power cord.

4. **Screw Hole**

   A hole for a screw to set the power cord anchor bracket

LAN Port Indicator

You can check the connection condition of the PC port (maintenance port) and LAN port.



1. **Orange**

   Indicates that the RC Gate is connected to the network.

2. **Green**

   Indicates that the RC Gate is transmitting data.

About Options

This section explains the names and functions of options for the RC Gate.

Expandable memory and storage are available as hardware options for the RC Gate. Contact your service representative for installation.

- Remote Communication Gate Memory 1000

  Expands the memory capacity from 128 MB to 512 MB.

- Remote Communication Gate Storage 1000

  Expands the storage capacity from 2 GB to 18 GB.

Note

- The RC Gate can manage a maximum of 100 devices. If you have installed optional memory and storage to expand the capacity, up to 1,000 devices can be registered. Contact your service representative for details.
- If you have installed optional memory, the RC Gate can acquire the device counter information specified by the Communication Server on a per user basis (by user code) and communicate it to Communication Server. Contact your service representative for details about services that use a per-user counter.

About the RC Gate Monitor

The RC Gate Monitor is the software used to register, monitor, and make settings of the RC Gate. The software is pre-installed in the RC Gate.

Access the RC Gate Monitor in this equipment from Web browser in the computer. The computer must be on the same network as this equipment.

Important

- **Some failure in operation or in displaying might occur in the following cases:**
  - **You use Web browsers lower than the recommended version.**
  - **JavaScript is not set to valid.**
  - **Cookie is not set to valid.**
  - **You set to show cache in the Web browser.**
- **Page layout may be out of shape depending on the font size settings. We recommend to set it to "Medium" or smaller.**
- **Some letter deterioration may occur if you use languages that do not correspond to Web browser.**

Applicable Operating System

Use operating systems which support the recommended Web browsers below.

Recommended Web Browser

- Microsoft Internet Explorer 6.0 or later (Internet Explorer 7.0 or later when accessing the URL with IPv6 address)

Important

- **Adobe Flash Player 10.0 or later must be installed.**

Note

- Contact the network administrator for the SSL certificate.

Users of the RC Gate Monitor

The following types of users can log in to the RC Gate:

Administrator

The administrator can set up the RC Gate, register devices, change the settings of this equipment, and confirm the device management information.

When you log in to the RC Gate as the administrator, select the screen to be displayed from "Initial Settings" screen or "RC Gate Configuration" screen.

If you select "Initial Settings" screen, the following menus will appear:

- Setup Wizard

Starts the wizard for referring and registering the RC Gate to the Communication Server.

Once the wizard has been completed, the menu will not be displayed.

- @Remote Service Registration Wizard

  The menu is displayed when the "Setup Wizard" has been completed.

- Shift Device Firmware Update Time

  Starts the wizard for setting the time at which device firmware update by network segment.

  The menu is displayed when the "@Remote Service Registration Wizard" has been completed.

- Access Prohibited IP Address

  Starts the wizard for specifying the IP address of the network device that you want to prohibit the RC Gate from accessing.

  The menu is displayed when the "@Remote Service Registration Wizard" has been completed.

- Ping Send Permission

  Starts the wizard for setting whether to allow ping transmission.

  The menu is displayed when the "@Remote Service Registration Wizard" has been completed.

- Auto Discovery Setting Wizard

  Starts the wizard for setting the usage and schedule of the Auto Discovery function.

  The menu is displayed when the "@Remote Service Registration Wizard" has been completed.

- Device Registration Wizard

  Starts the wizard for registering the devices on network with the Communication Server.

  The menu is displayed when the "@Remote Service Registration Wizard" has been completed.

- Service Call

  Displays the error codes and error information of the RC Gate.

General user

A general user can only view the information about the managed devices. General users are responsible for the managed devices, and cannot change settings of the RC Gate. Up to 10 general users can be registered.

General users can view the following screens:

- Registered Device List

  Displays the list of devices managed by the RC Gate.

- Details

  Displays the details of the devices managed by the RC Gate.

- Call Report Record(s)

  Displays the date of a call report, call type, and the device information on which a call has been reported.

- Registered Device Counter

  Displays the counter information of the devices managed by the RC Gate.

- Service Call

  Displays the error codes and error information of the RC Gate.

To view the device information as a general user, a user account must be created by the administrator. For details on account settings, see page 128 "User Account Settings".

Note

- Ask the administrator to remove any general user accounts that are not in use.

To Start the RC Gate Monitor

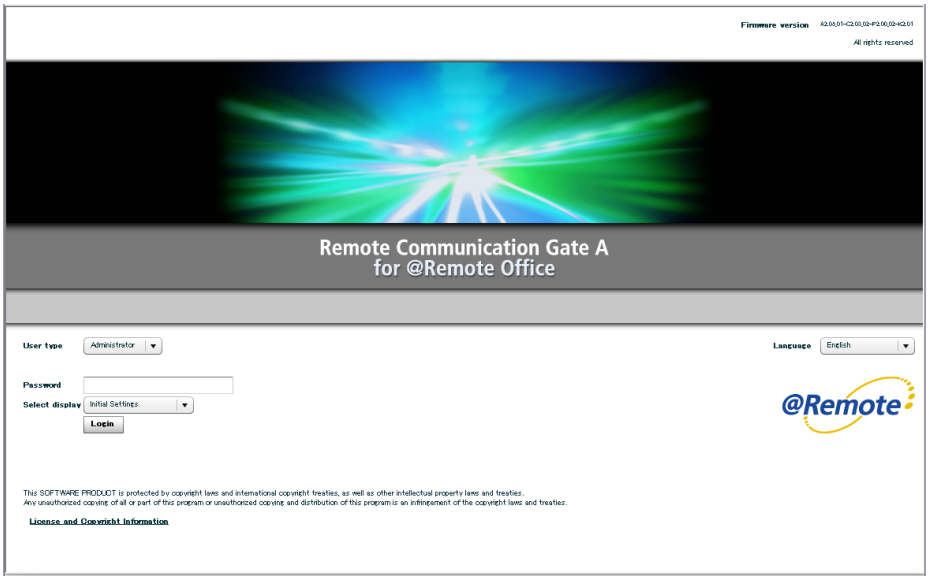
Important

- **Use a browser that can display disguised characters (such as asterisks) during password entry.**
- **Change the password. Be sure to change the password for actual operation of the RC Gate Monitor. See page 129 "Password" for details.**
- **For security, further login attempts are rejected if you fail to login three times within five minutes. Wait one minute before attempting to login again.**

1. **Start the Web browser of the computer, which is on the same network with the RC Gate.**
2. **Enter "https://{LAN port IP address}:9443/index.html" in "Address".**
3. **Click [Yes].**
4. **The firmware version appears in the top right of the top page on the RC Gate monitor. If using this product as CC certified, confirm it by checking the firmware version. You can check the CC certified firmware versions at the URL of the RC Gate manuals. Select your language from "Language", select [Administrator] or [General user] from "User type", and then enter the corresponding password.**

   When logging in as [General user]:

   - Enter the password given by the administrator.
   - Enter a user name in "User Name".



5. **Select the display screen.**
6. **Click [Login].**

Note

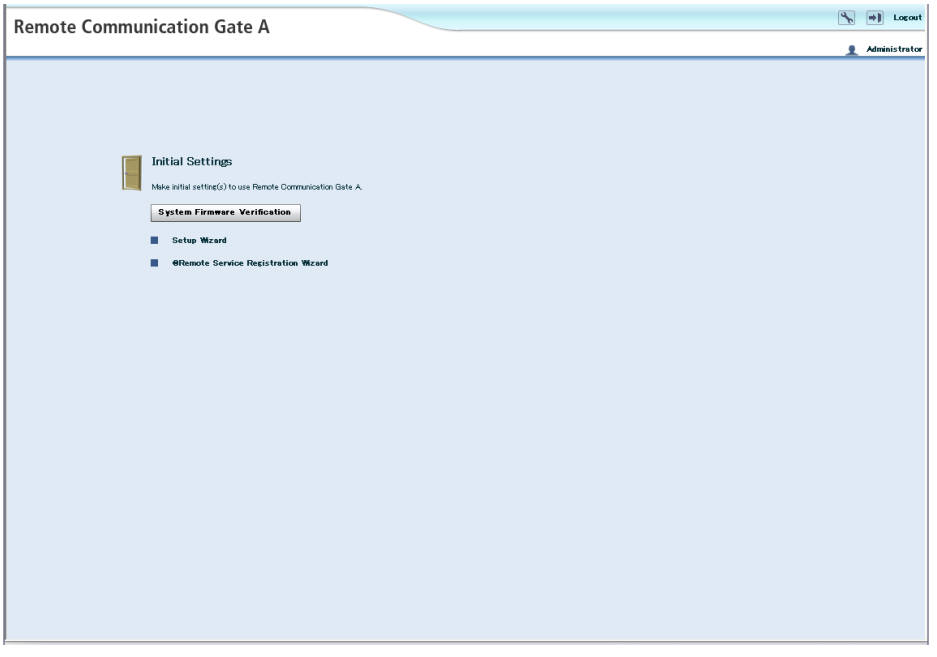
- If you cannot access the RC Gate Monitor, see page 20 "Proxy Settings (Internet Explorer 6.0)" and make the proxy settings.
- Security logs can be configured. See page 136 "Security Log" for details.

Checking the Validity of the Software

Before operating the RC Gate Monitor, check whether the software included in the RC Gate is valid.

1. **Start the RC Gate Monitor, select "Initial Settings" as the screen to display, and log in as [Administrator].**

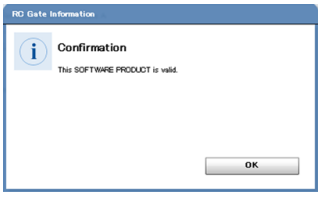
2. **Click [System Firmware Verification].**



A dialog box appears and displays the results of the check.

A message "This SOFTWARE PRODUCT is not valid. Please call service for instructions" appears if the software is not valid. Follow the message indicated on the screen and call service for instructions.

3. **Click [OK].**



The screen returns to the top page.

Proxy Settings (Internet Explorer 6.0)

1. **On your Web browser's [Tools] menu, select [Internet Options...].**
2. **Click [Connections] tab.**
3. **Click [LAN Settings...].**
4. **Under [Proxy Server], select [Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).], and click [Advanced...].**

5. Under [Exceptions], after [Do not use proxy server for addresses beginning with], enter the IP address of the RC Gate's LAN port.
6. Click [OK] three times.

To Close the RC Gate Monitor

Important

- An administrator or general user must always click [Logout] before closing the Web browser. If you close the Web browser without clicking [Logout], the user will remain logged in to RC Gate Monitor.
- When you are finished using RC Gate Monitor, remember to click [Logout]. If you leave the monitor idle for 5 minutes, you will be automatically logged out.

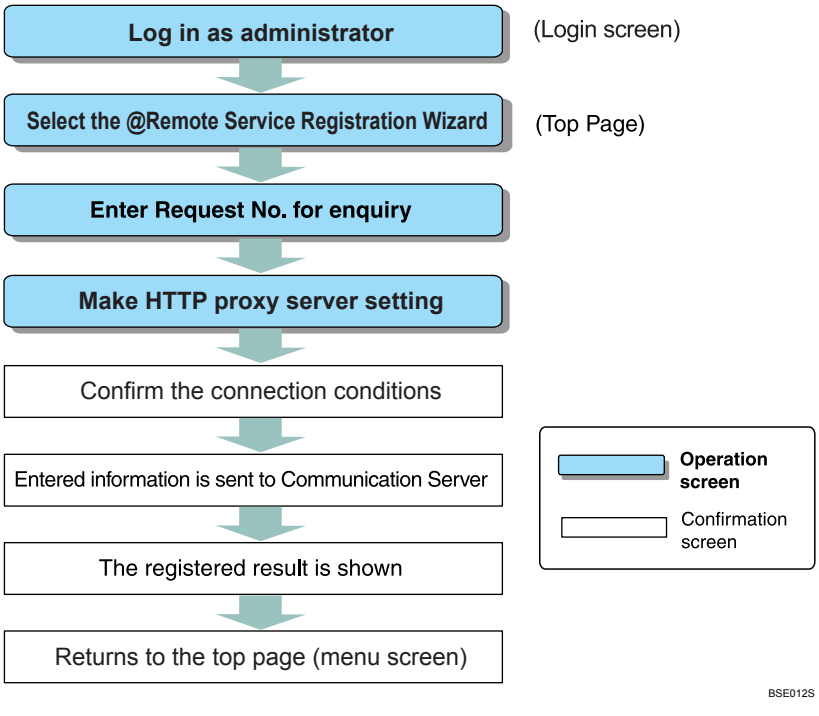
1. Click [Logout] in the header area.
2. Confirm that the logged in user has logged out the RC Gate Monitor, and then close the Web browser.

2. Registering the RC Gate

This chapter explains the procedure for registering the RC Gate with the Communication Server.

Outline of the @Remote Service Registration Wizard

This section explains how to register the RC Gate to the Communication Server.



Operating the @Remote Service Registration Wizard

The following procedures explain how to register the RC Gate with the Communication Server.

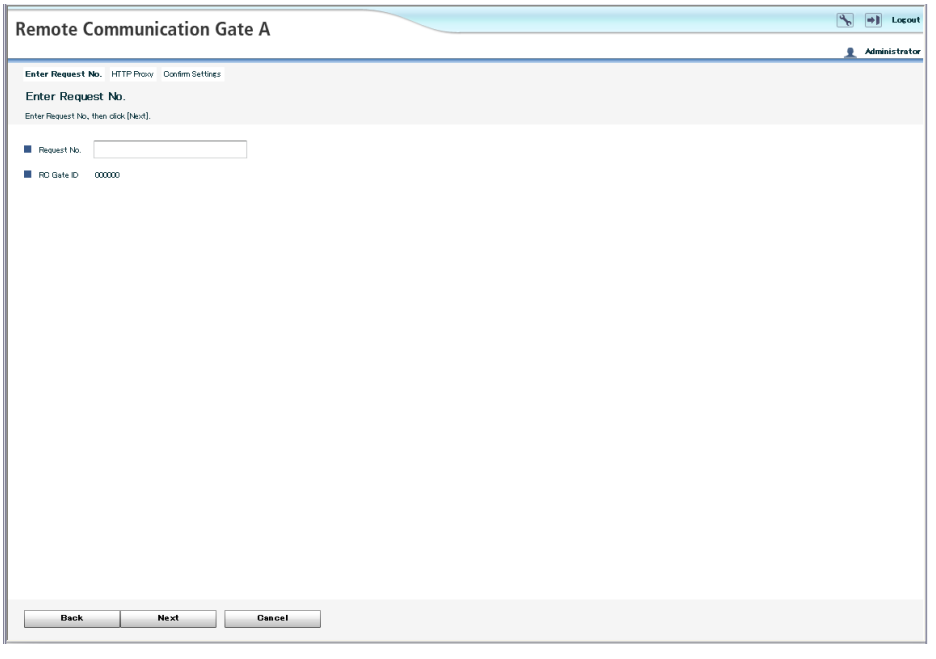
1. **Start the Web browser, access the RC Gate Monitor, and log in as [Administrator].**

   For Details about accessing the RC Gate Monitor, see page 16 "About the RC Gate Monitor".

2. **Click [@Remote Service Registration Wizard].**

   [@Remote Service Registration Wizard] will not appear if it has already been finished. Proceed to page 28 "Operating the Auto Discovery Setting Wizard".

3. **Enter "Request No.", and click [Next].**

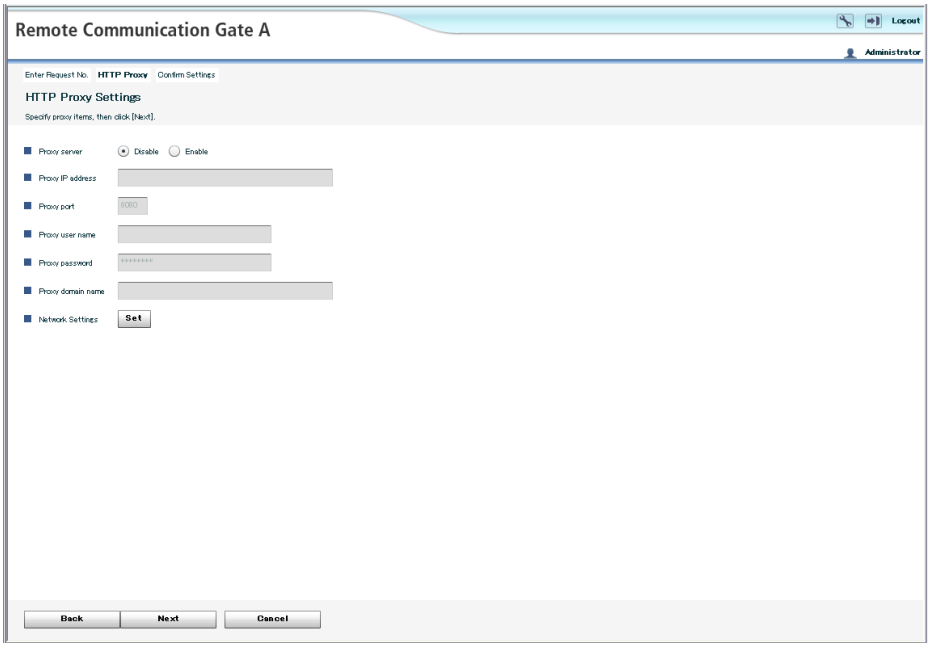


   "Request No." will identify your RC Gate with the Communication Server.

4. **To use an HTTP proxy server, select [Enable] for "Proxy server" to configure the proxy server settings, and then click [Next].**

   If you want to change the network settings, click [Set].

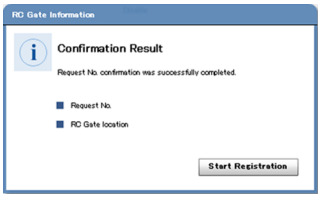
   If you do not use an HTTP proxy server, select [Disable], and then click [Next].



5. **Confirm the connection conditions, and click [Next].**

   It will take a few minutes for the RC Gate to complete confirming the entered settings to the Communication Server. Wait until the "Confirmation Result" screen appears.

6. **Confirm that confirmation is successful, and click [Start Registration].**



7. **Confirm that registration is successful, and click [OK].**

   "@Remote Service Registration Wizard" finishes, and the screen returns to the "Initial Settings" screen.

8. **If the network cable is connected to the PC port, remove the cable from the port, and then restore the network settings of the computer.**

Note

- [OK] will appear when the confirmation or registration fails. Click [OK] and start the wizard again from step 3.

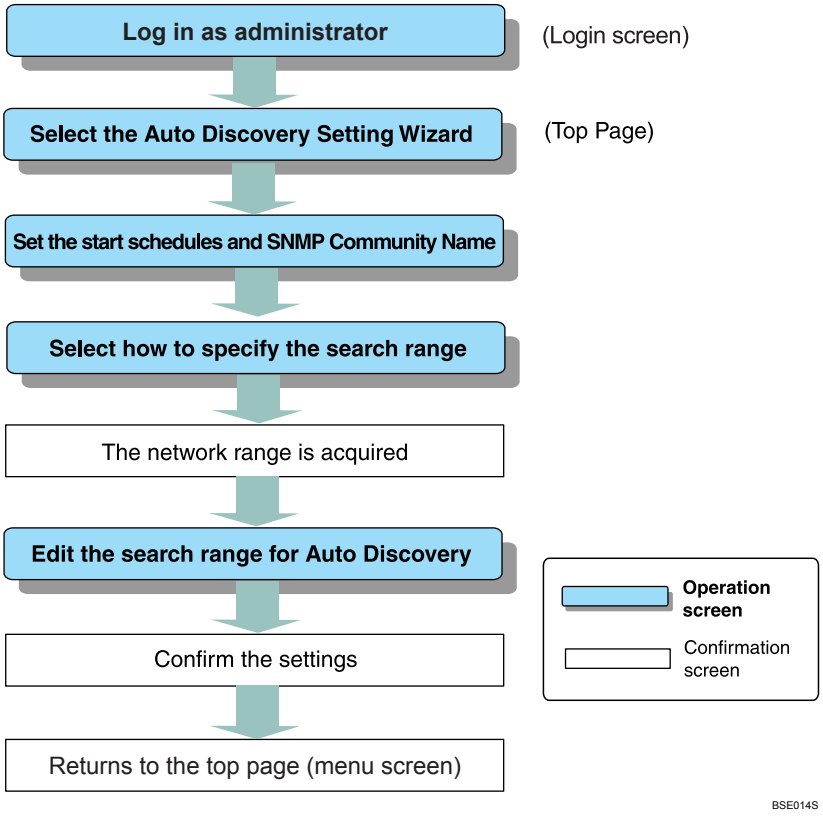
3. Setting the Auto Discovery

When Auto Discovery is enabled, the RC Gate collects information about the devices on the network using the specified schedule, and then reports it to the Communication Server.

You can configure the Auto Discovery function using the "Auto Discovery Setting Wizard". The wizard appears when you log in as [Administrator], and "@Remote Service Registration Wizard" has been completed.

Outline of the Auto Discovery Setting Wizard

This section explains the outline of enabling the Auto Discovery function.



Operating the Auto Discovery Setting Wizard

This section explains how to specify the method by which the RC Gate discovers devices using Auto Discovery.

There are five methods by which Auto Discovery can discover devices on a network:

- By searching through a specified range of IPv4 addresses.
- By searching through specified host names.
- By searching through specified network segments.
- By searching through specified IPv6 addresses.
- By searching through IPv6 multicast addresses.

Important

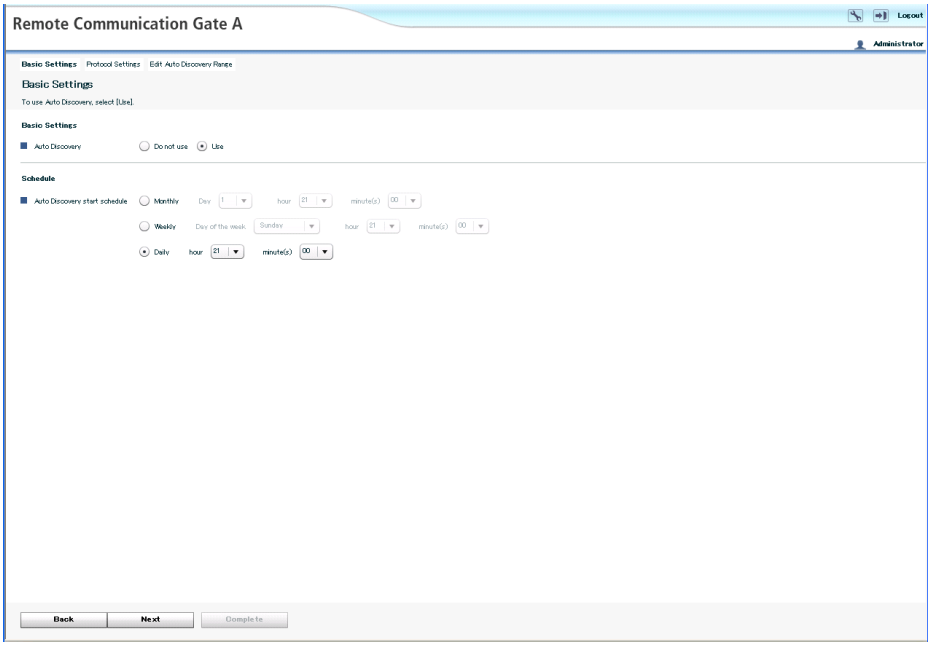
- **You can import search ranges from a CSV file stored on your computer. For details on creating a CSV file, see page 47 "To Create a CSV File".**

When Specifying Auto Discovery Range by IPv4 Address

This section explains how to specify the Auto Discovery search range by specifying IPv4 address of the device.

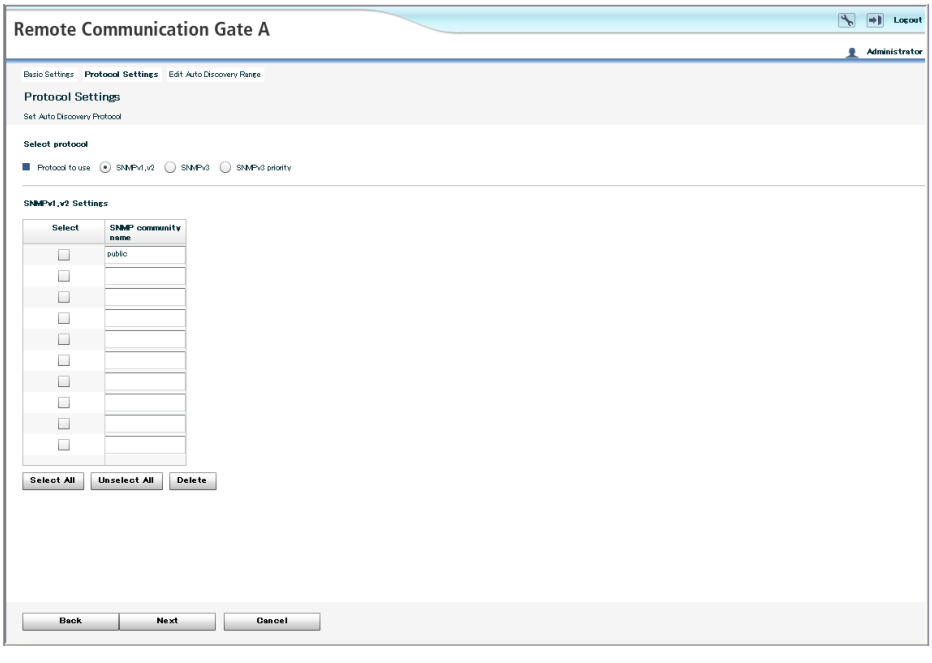
1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Auto Discovery Setting Wizard].**

3. Select [Use] for Auto Discovery.



4. Set each item in "Schedule", and then click [Next].

5. Select a protocol for searching, and then click [Next].



- If you select [SNMPv1,v2]:

The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

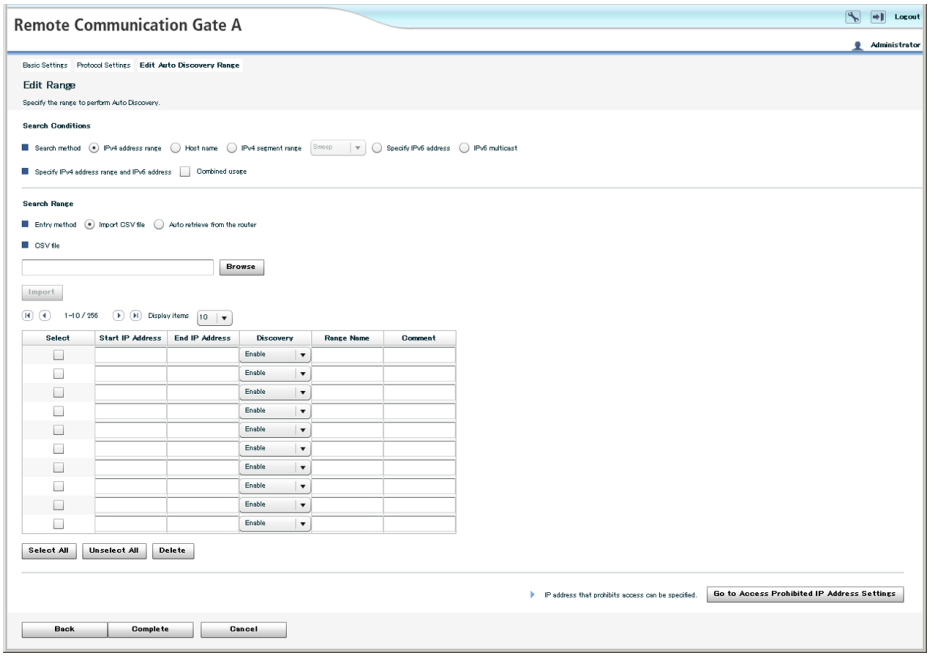
To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

6. **Select [IPv4 address range] for the search method.**

   If you specify both IPv4 address range and IPv6 address, select [Combined usage].

7. **Set the search ranges.**



- When entering the ranges directly:

Enter the starting IPv4 address and finishing IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 10 sets of addresses.

Enter a higher IPv4 address for the finishing IPv4 address than for the starting IPv4 address.

If you set "0.0.0.0" for the finishing address, the range of IPv4 address on that line will not be searched.

An error will occur if the value for the starting IPv4 address is "0.0.0.0" and the value for the finishing IP address is other than "0.0.0.0".

- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import].

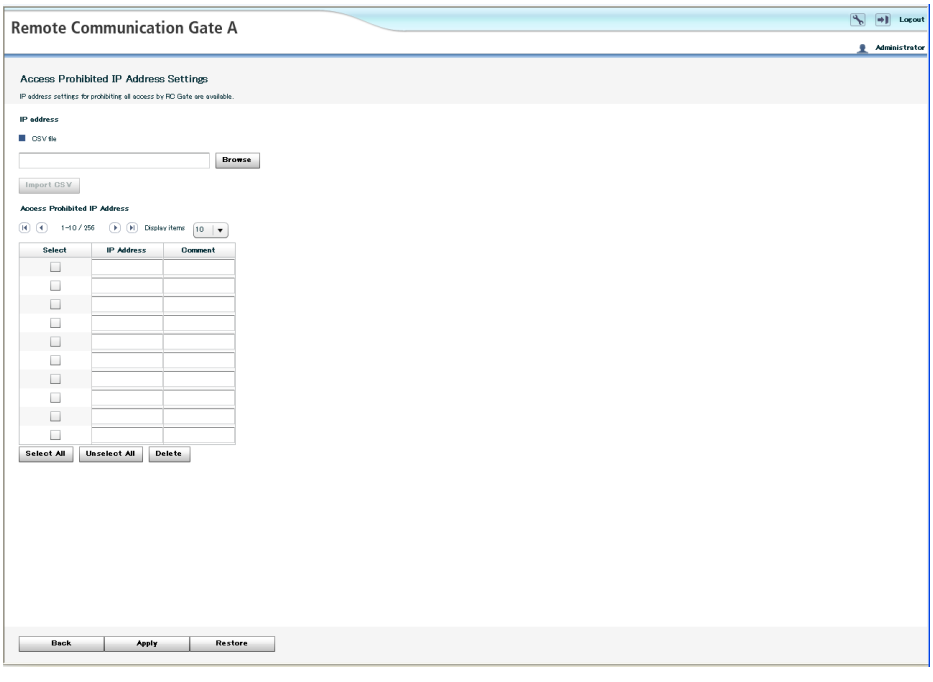
  Once the search ranges have been imported from the CSV file, all previously specified ranges will be deleted.

- When obtaining IP address information from the router:

  Select [Auto retrieve from the router]. Specify the number of search hops (0 to 10), and then click [Start Retrieval].

You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

8. Click [Go to Access Prohibited IP Address Settings], and then specify the IP address that you want to prohibit the RC Gate from accessing.



If you do not need to prohibit any IPv4 addresses, proceed to Step 10.

- When entering the IPv4 address directly:

Enter the IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 256 addresses.

- When importing from a CSV file:

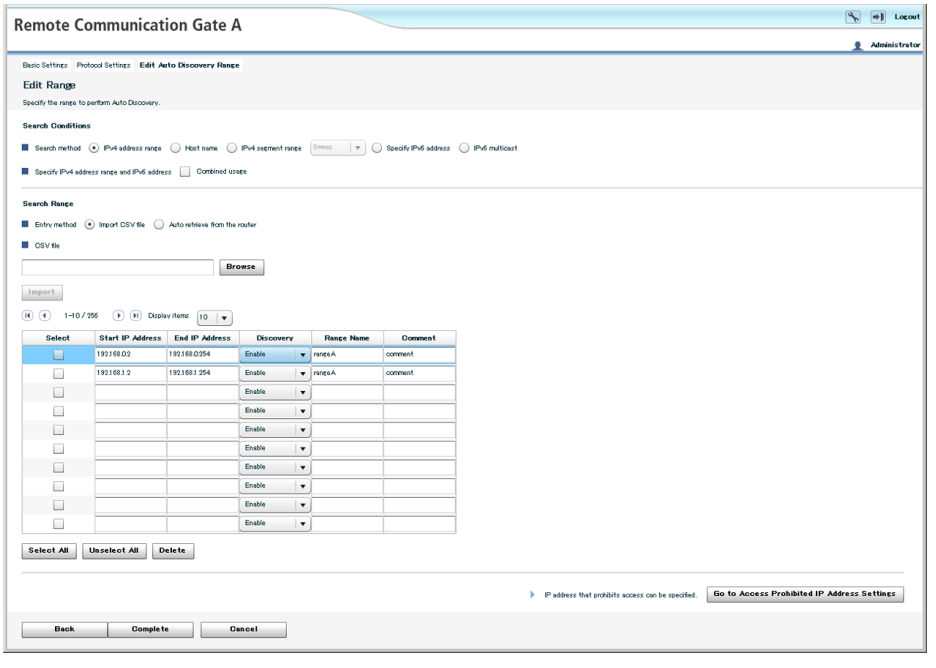
  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified IPv4 addresses will be deleted.

9. **Select the check boxes of the IPv4 address you want to prohibit, and then click [OK].**
10. **Edit the range.**

    To delete the range, select the check box of the range that you want to delete, and click [Delete].
11. **Specify [Enable] for "Discovery" if Auto Discovery is applied to the identified devices.**

    Enter a name for the search ranges in "Range Name" as necessary. The maximum length for a name is 61 ASCII characters.



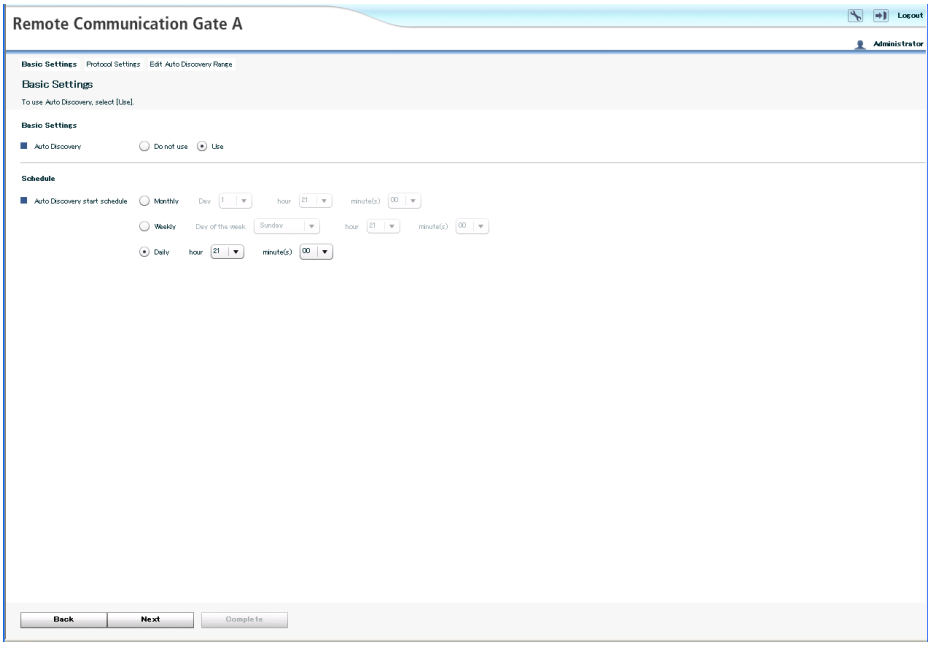
12. **Click [Complete].**

When Specifying Auto Discovery Range by Host Name

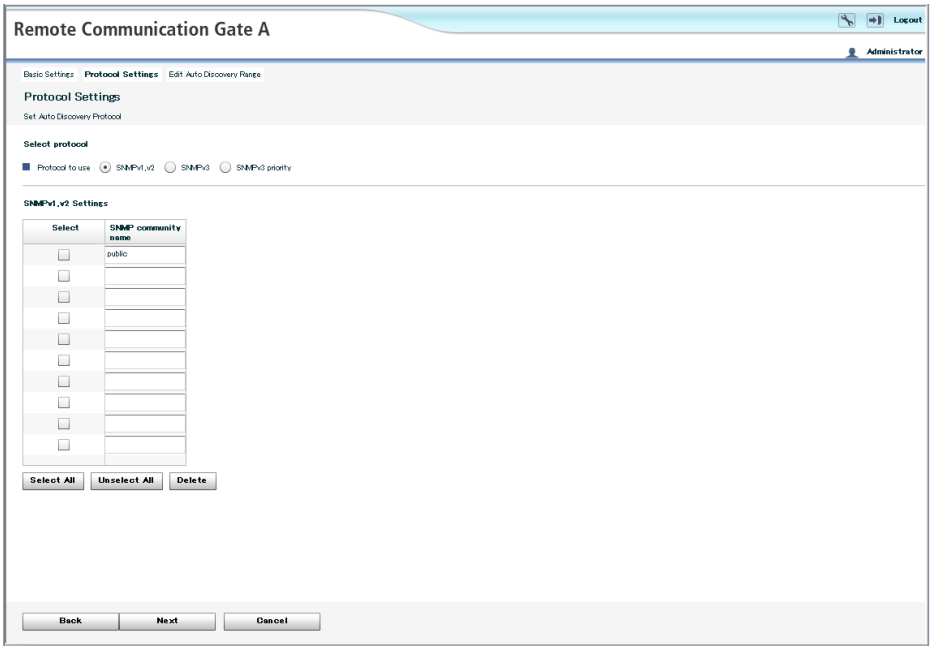
This section explains how to specify the Auto Discovery search range by specifying host names of the device.

1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Auto Discovery Setting Wizard].**

3. Select [Use] for Auto Discovery.



4. Set each item in "Schedule", and then click [Next].
5. Select a protocol for searching, and then click [Next].



- If you select [SNMPv1,v2]:

The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

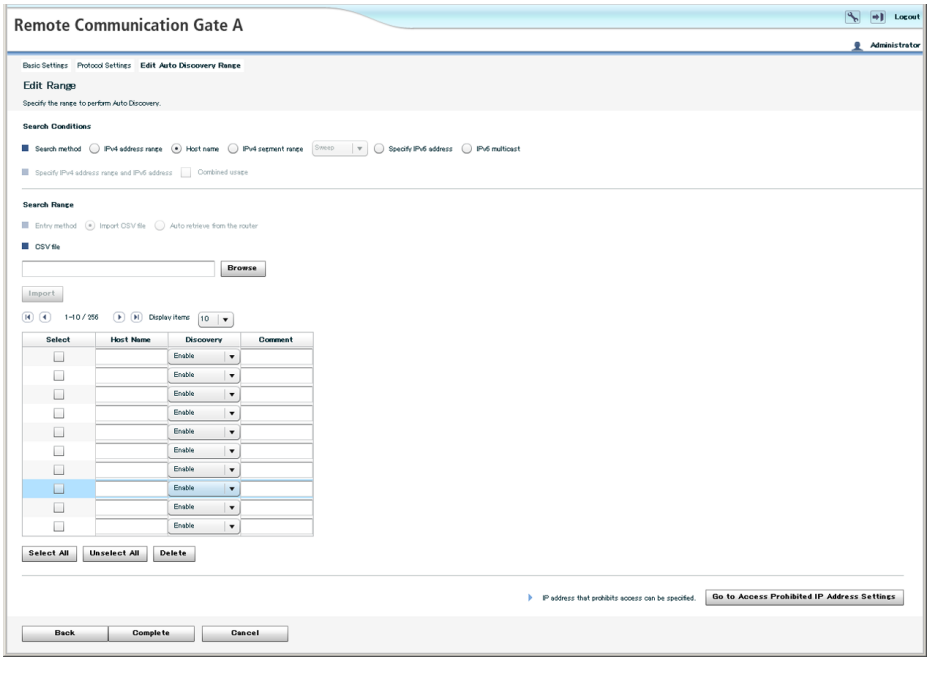
- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

6. **Select [Host name] for the search method.**
7. **Set the search ranges.**

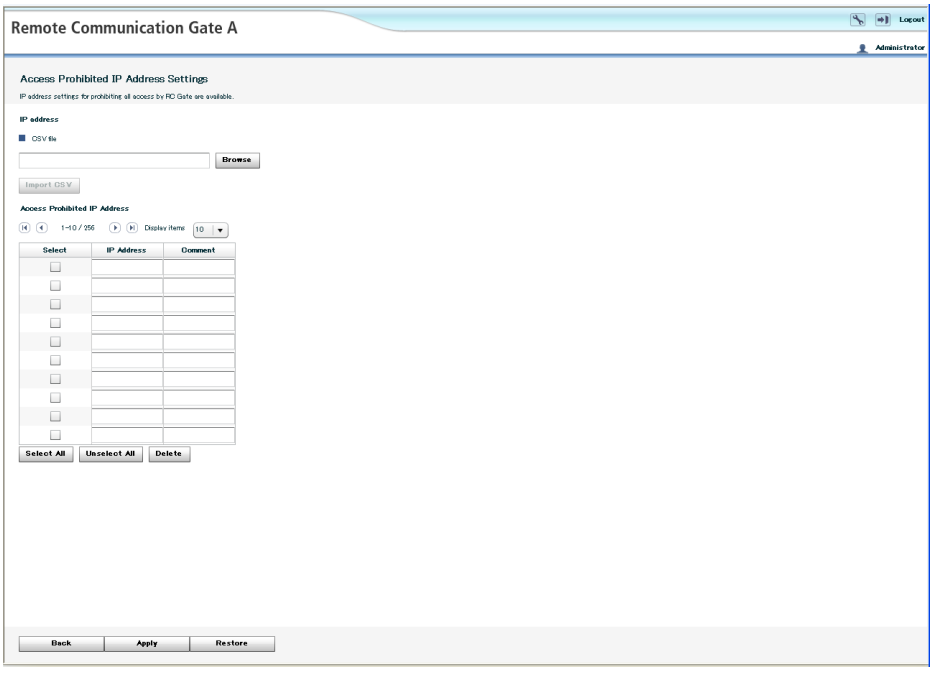


- When entering host names directly:

  Enter host names. You can enter up to 100 names (1,000 names if you have installed optional memory and storage).

You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

8. **Click [Go to Access Prohibited IP Address Settings], and then specify the IPv4 address that you want to prohibit the RC Gate from accessing.**



If you do not need to prohibit any IPv4 addresses, proceed to Step 10.

- When entering the IPv4 address directly:

  Enter the IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 256 addresses.

- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

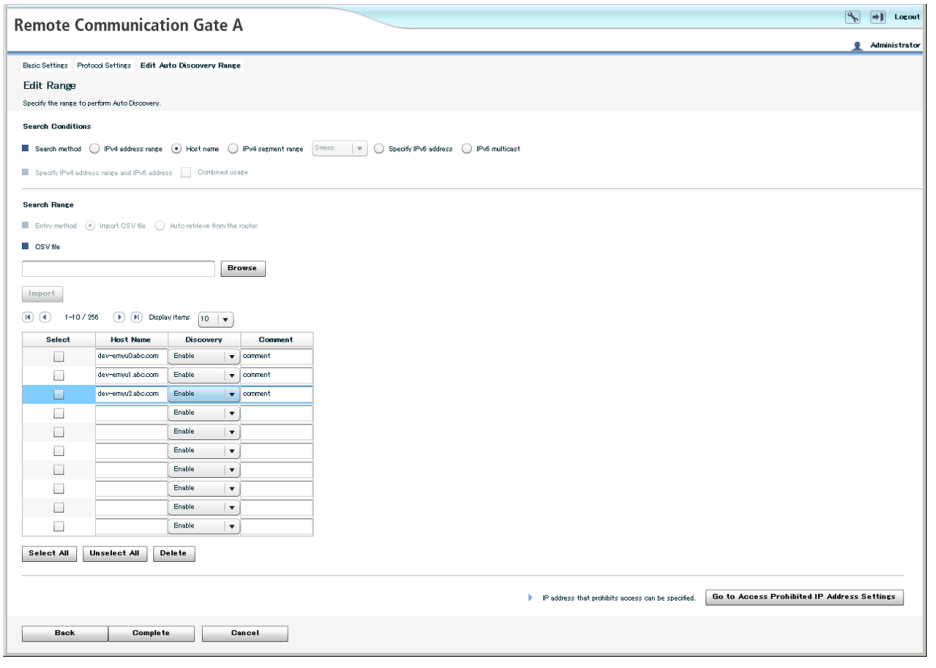
  Once the search ranges have been imported from the CSV file, all previously specified IPv4 addresses will be deleted.

9. **Select the check boxes of the IPv4 address you want to prohibit, and then click [OK].**
10. **Edit the range.**

    To delete the range, select the check box of the range that you want to delete, and click [Delete].

11. **Specify [Enable] for "Discovery" if Auto Discovery is applied to the identified devices.**

    Enter a name for the search ranges in "Range Name" as necessary. The maximum length for a name is 61 ASCII characters.



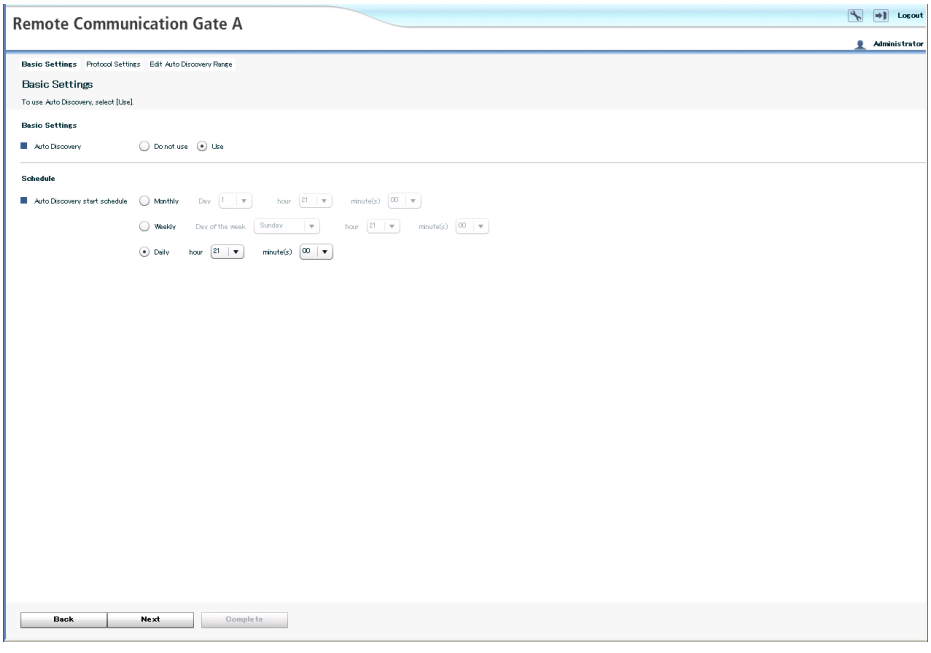
12. Click [Complete].

When Specifying Auto Discovery Range by Network Segment

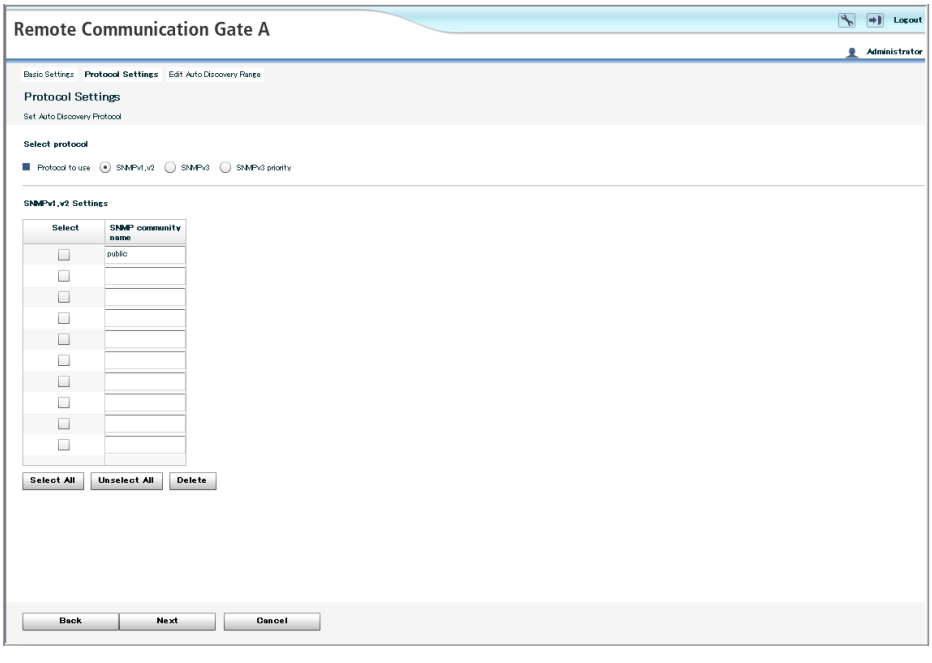
This section explains how to specify the Auto Discovery search range by specifying the network segments.

1. Start the RC Gate Monitor, and then log in as [Administrator].
2. Click [Auto Discovery Setting Wizard].

3. Select [Use] for Auto Discovery.



4. Set each item in "Schedule", and then click [Next].
5. Select a protocol for searching, and then click [Next].



- If you select [SNMPv1,v2]:

The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

6. **Select [IPv4 segment range] for the search method.**

   Select one of the following search methods:

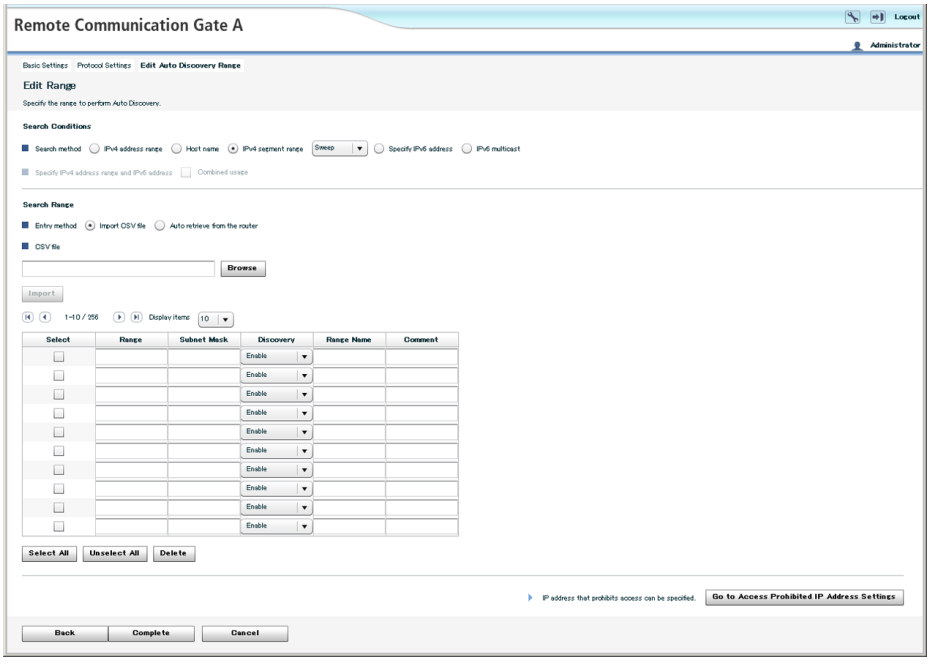
   - Segment search by Sweep

     The RC Gate sends a ping to each IPv4 address (host addresses 1 to 254) in a specified network segment.

   - Segment search by Broadcast

     The RC Gate issues an SNMP broadcast and searches any responding IPv4 addresses within the specified network segment.

7. Set the search ranges.



- When entering the ranges directly:

  Enter the subnet IPv4 address, subnet mask, and range name. You can enter up to 10 sets of information.

- When Importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import].

  Once the search ranges have been imported from the CSV file, all previously specified ranges will be deleted.

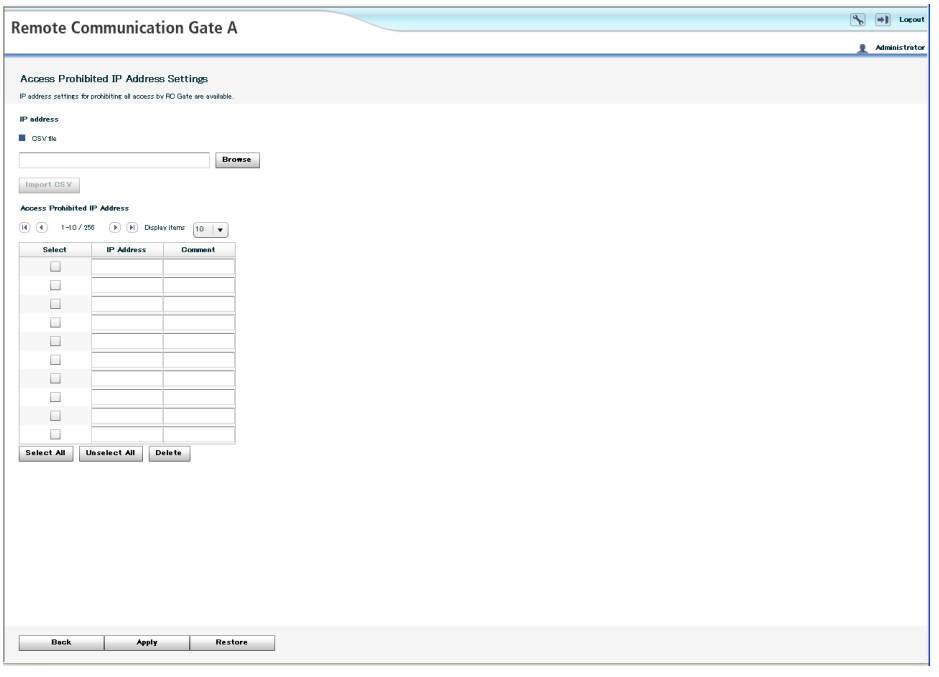
- When obtaining the segment information from the router:

  Select [Auto retrieve from the router]. Specify the number of search hops (0 to 10), and then click [Start Retrieval].

You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

8. Click [Go to Access Prohibited IP Address Settings], and then specify the IPv4 address that you want to prohibit the RC Gate from accessing.

If you do not need to prohibit any IPv4 addresses, proceed to Step 10.



- When entering the IPv4 address directly:

  Enter the IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 256 addresses.

- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

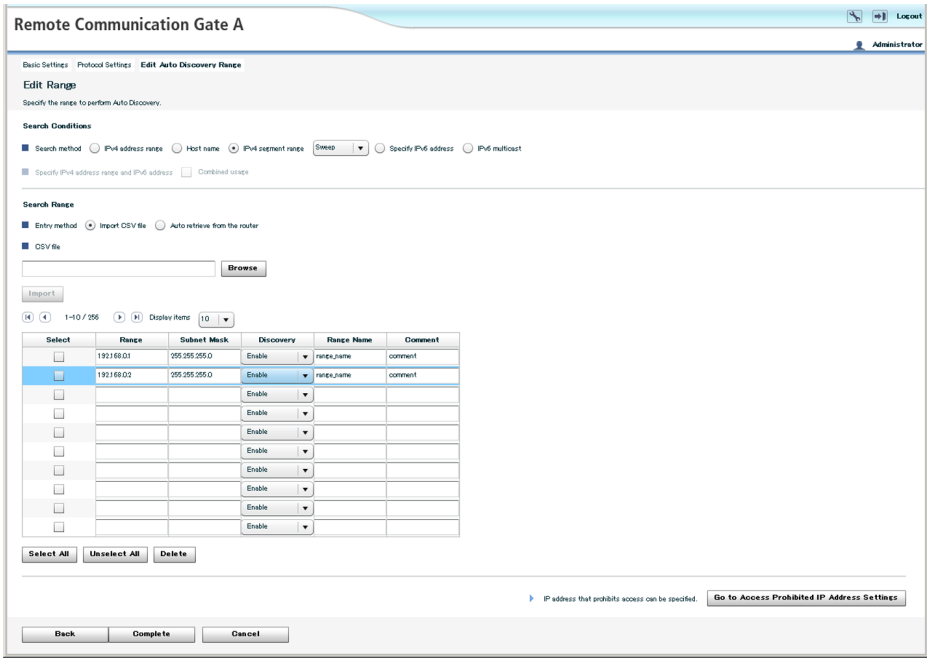
  Once the search ranges have been imported from the CSV file, all previously specified IPv4 addresses will be deleted.

9. **Select the check boxes of the IPv4 address you want to prohibit, and then click [OK].**
10. **Edit the range.**

    To delete the range, select the check box of the range that you want to delete, and click [Delete].

11. **Specify [Enable] for "Discovery" if Auto Discovery is applied to the identified devices.**

    Enter a name for the search ranges in "Range Name" as necessary. The maximum length for a name is 61 ASCII characters.



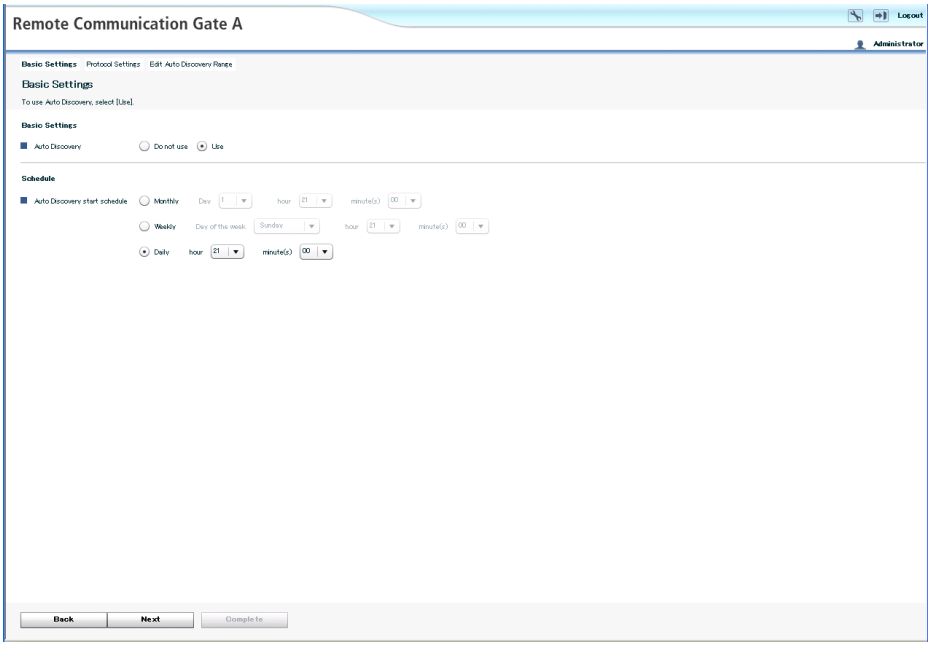
12. Click [Complete].

When Specifying Auto Discovery Range by IPv6 Address

This section explains how to specify the Auto Discovery search range by specifying IPv6 addresses.

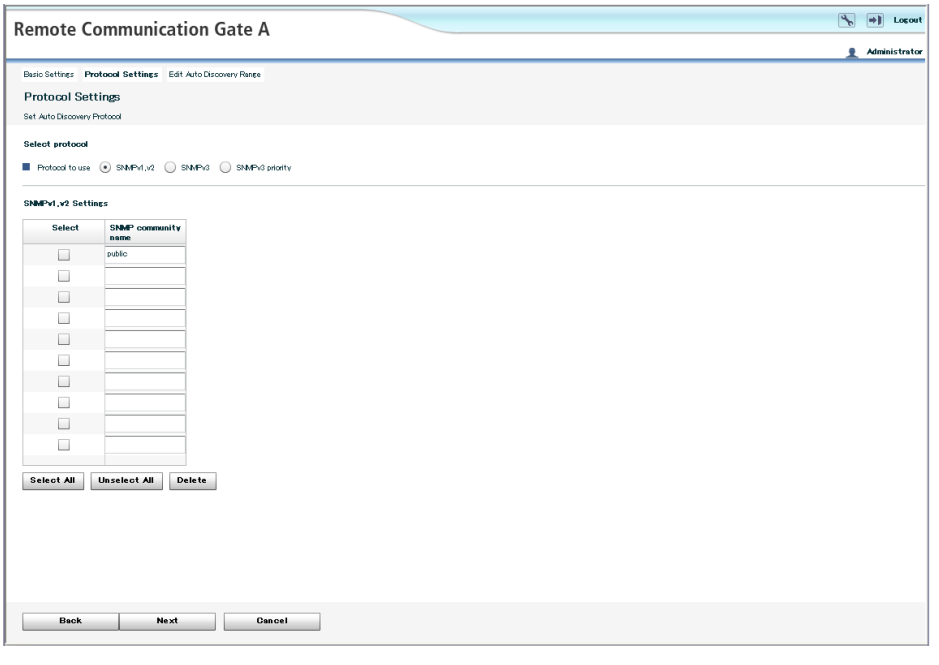
1. Start the RC Gate Monitor, and then log in as [Administrator].
2. Click [Auto Discovery Setting Wizard].

3. Select [Use] for Auto Discovery.



4. Set each item in "Schedule", and then click [Next].

5. Select a protocol for searching, and then click [Next].



- If you select [SNMPv1,v2]:

The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

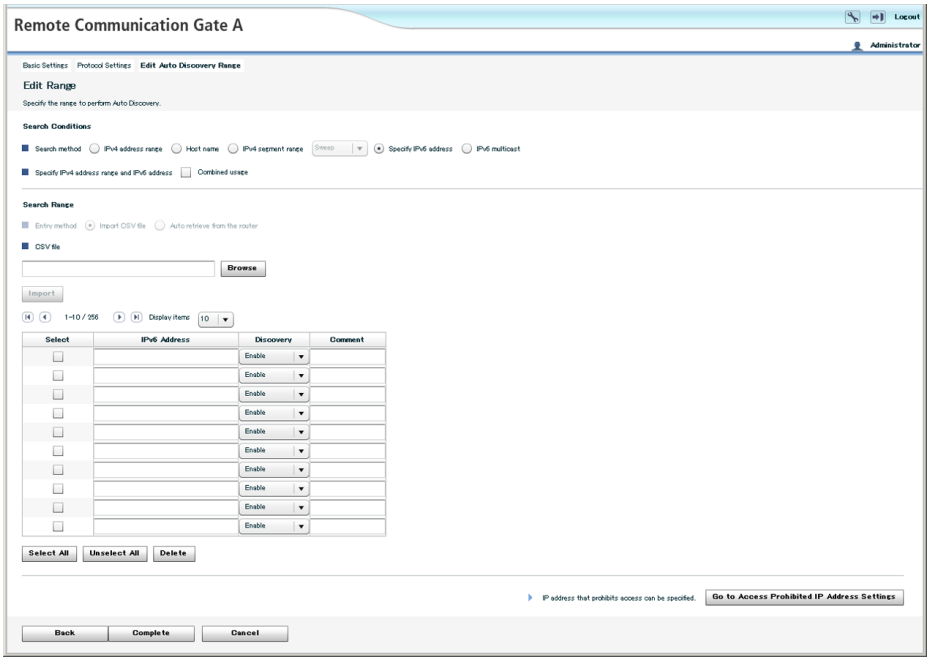
To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

6. **Select [IPv6 address] for the search method.**

   If you specify both IPv4 address range and IPv6 address, select [Combined usage].

7. **Set the search ranges.**



- When entering IPv6 addresses directly:

Enter IPv6 addresses in “xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx” format (”x” standing for hexadecimal number. Consecutive “0” can be omitted.). You can enter up to 100 sets of addresses (1,000 sets of addresses if you have installed optional memory and storage).

- When Importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import].

  Once the search ranges have been imported from the CSV file, all previously specified IPv6 addresses will be deleted.

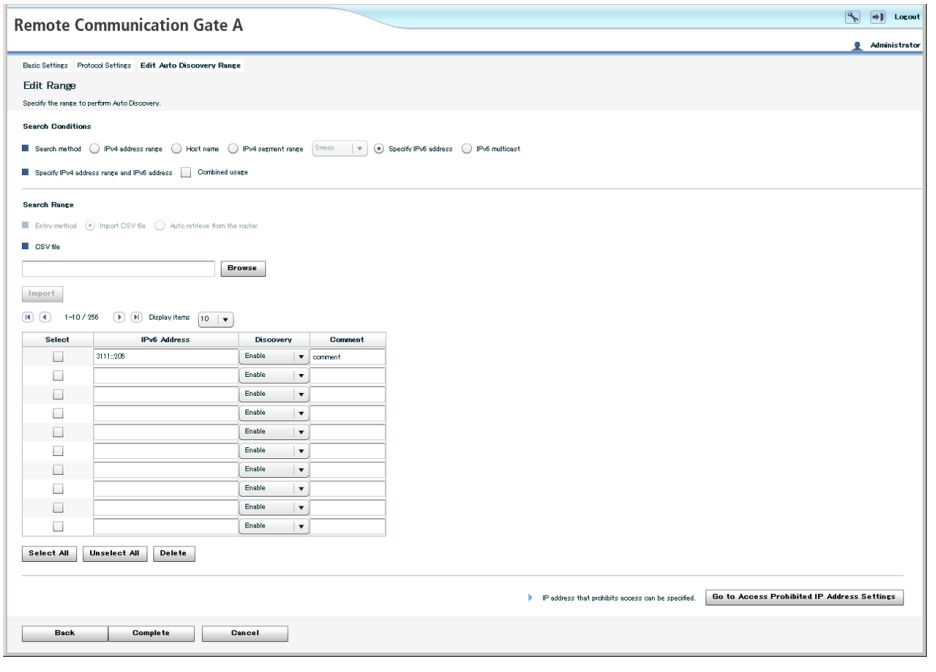
You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

8. **Edit the range.**

   To delete the range, select the check box of the range that you want to delete, and click [Delete].

9. **Specify [Enable] for "Discovery" if Auto Discovery is applied to the identified devices.**

   Enter a name for the search ranges in "Range Name" as necessary. The maximum length for a name is 61 ASCII characters.

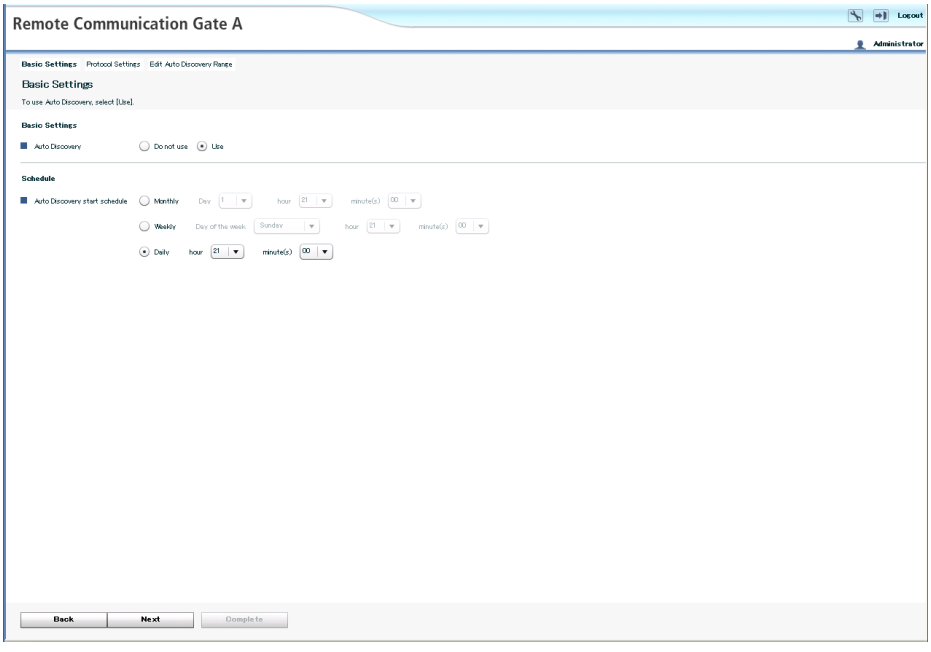


10. **Click [Complete].**

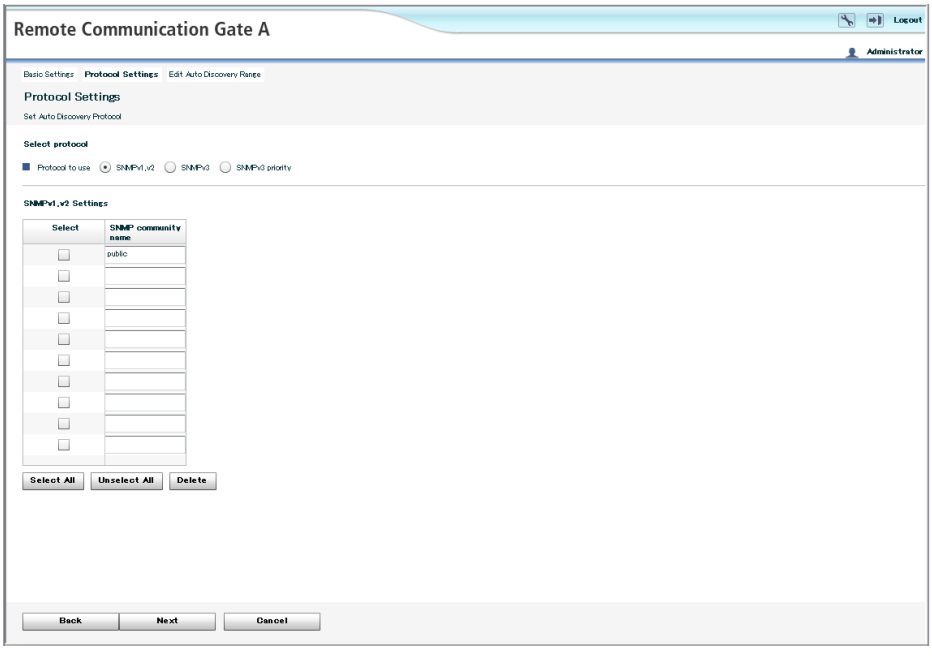
When Specifying Auto Discovery Range by IPv6 Multicast Address

This section explains how to specify the Auto Discovery search range by IPv6 multicast addresses “FF02::1”.

1. Start the RC Gate Monitor, and then log in as [Administrator].
2. Click [Auto Discovery Setting Wizard].
3. Select [Use] for Auto Discovery.



4. Set each item in "Schedule", and then click [Next].
5. Select a protocol for searching, and then click [Next].



- If you select [SNMPv1,v2]:

  The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

  Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

  Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

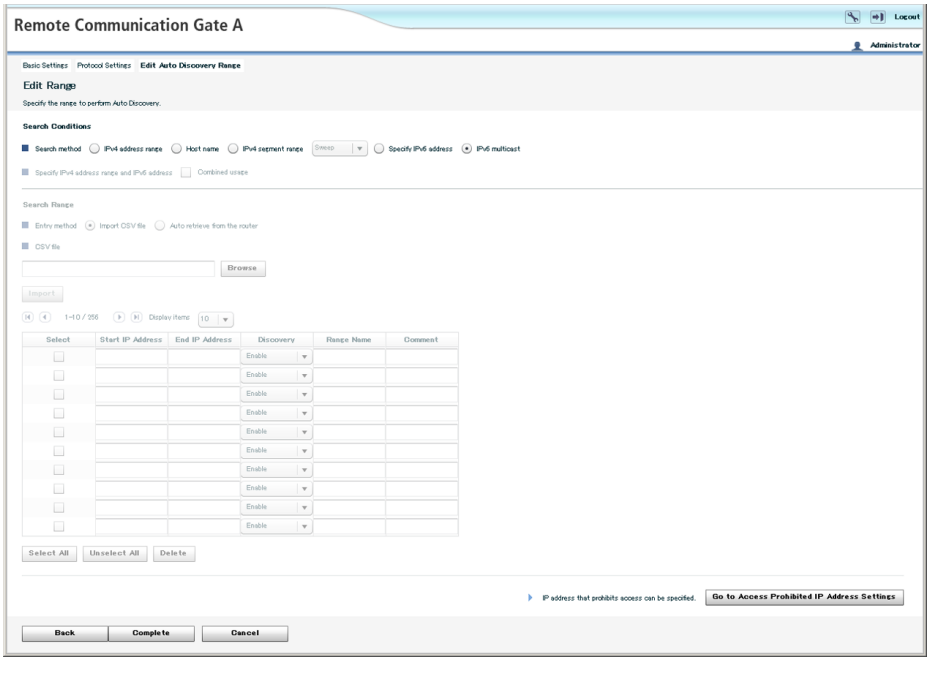
- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

6. **Select [IPv6 multicast] for the search method.**



7. **Click [Complete].**

To Create a CSV File

To import a CSV file, you must create a CSV file.

CSV file for specifying the search ranges by IPv4 address:

To create the CSV file, enter the information for each IPv4 address range by separating it with a comma. Each line should contain the following items: starting IPv4 address, finishing IPv4 address, discovery, range name, and comment. You can enter up to 256 sets of addresses.

Example:

```
192.168.0.1,192.168.0.2,Enable,abc,1-63
192.168.0.3,192.168.0.4,Disable,def,64-127
192.168.0.5,192.168.0.6,Enable,ghi,128-191
192.168.0.7,192.168.0.8,Enable,jkl,192-254
```

BSE015S

CSV file for specifying the search ranges by network segment:

To create the CSV file, enter the information for each network segment by separating it with a comma. Each line should contain the following items: subnet IP address, subnet mask, discovery, range name, and comment. You can enter up to 256 sets of information.

Example:

```
192.168.1.0,255.255.255.0,Enable,abc,1-63
192.168.2.0,255.255.255.0,Disable,def,64-127
192.168.3.0,255.255.255.0,Enable,ghi,128-191
192.168.4.0,255.255.255.0,Enable,jkl,192-254
```

BSE016S

CSV file for specifying the search ranges by host name:

To create the CSV file, enter the information for each host name by separating it with a comma. Each line should contain the host name, discovery and comment. You can enter up to 100 names.

Example

```
host0,Enable
host1,Disable
host2,Enable
host3,Enable
host4,Disable
```

BSE021S

CSV file for specifying IPv6 address:

To create the CSV file, enter the information for each IPv6 address by separating it with a comma. Each line should contain the IPv6 address, discovery and comment. You can enter up to 100 addresses.

Example

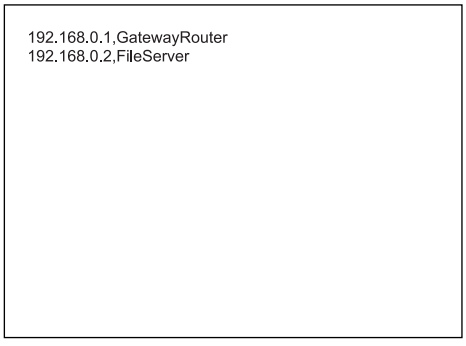
```
2001:DB8::1:0,Enable
2001:DB8::2:0,Disable
2001:DB8::3:0,Enable
2001:DB8::4:0,Enable
```

BSE022S

CSV file for specifying access prohibited IP addresses:

To create the CSV file, enter the information for each IP address by separating it with a comma. Each line should contain the IP address and comment. You can enter up to 256 sets of addresses.

Example:



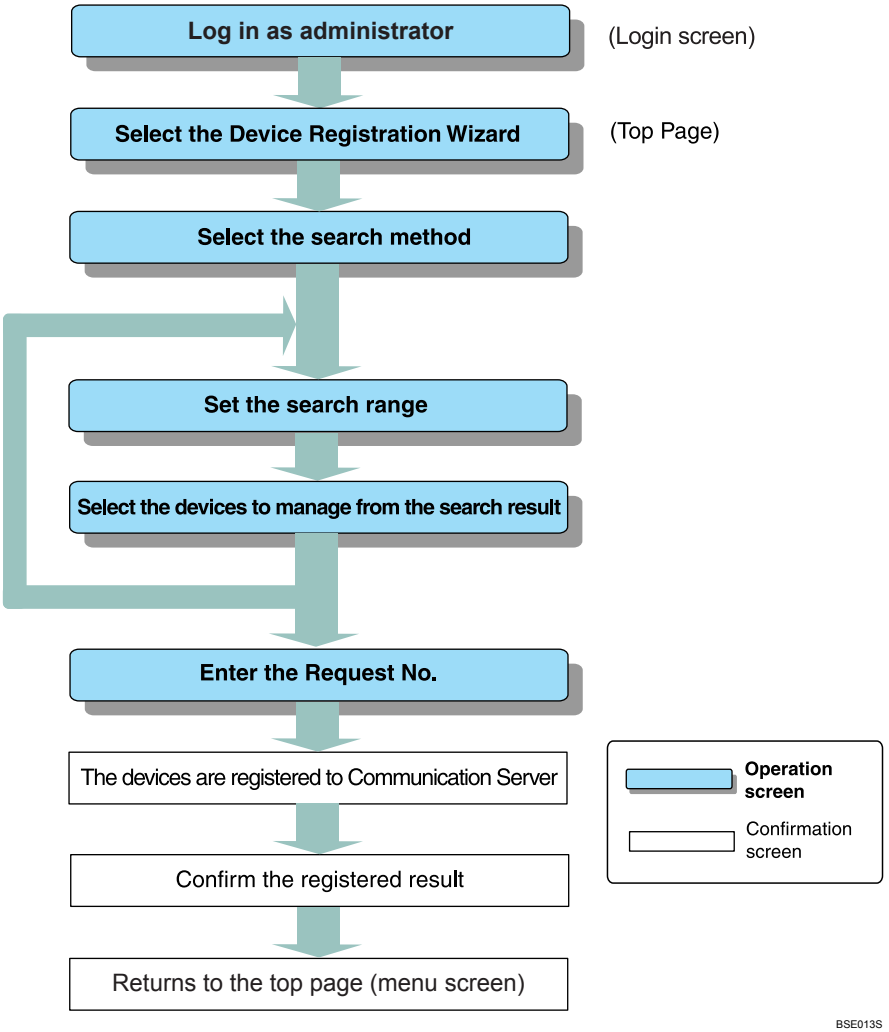
BSE018S

4. Registering Devices with the Communication Server

This chapter explains the procedure for registering the devices with the Communication Server.

Outline of the Device Registration Wizard

This section describes how to register the device to the Communication Server.



Operating the Device Registration Wizard

This section explains how to register devices on network with the Communication Server.

There are five methods by which the RC Gate can discover devices on a network:

- By searching through a specified range of IPv4 addresses.
- By searching through specified host names.
- By searching through specified network segments.
- By searching through specified IPv6 addresses.
- By searching through IPv6 multicast addresses.

Important

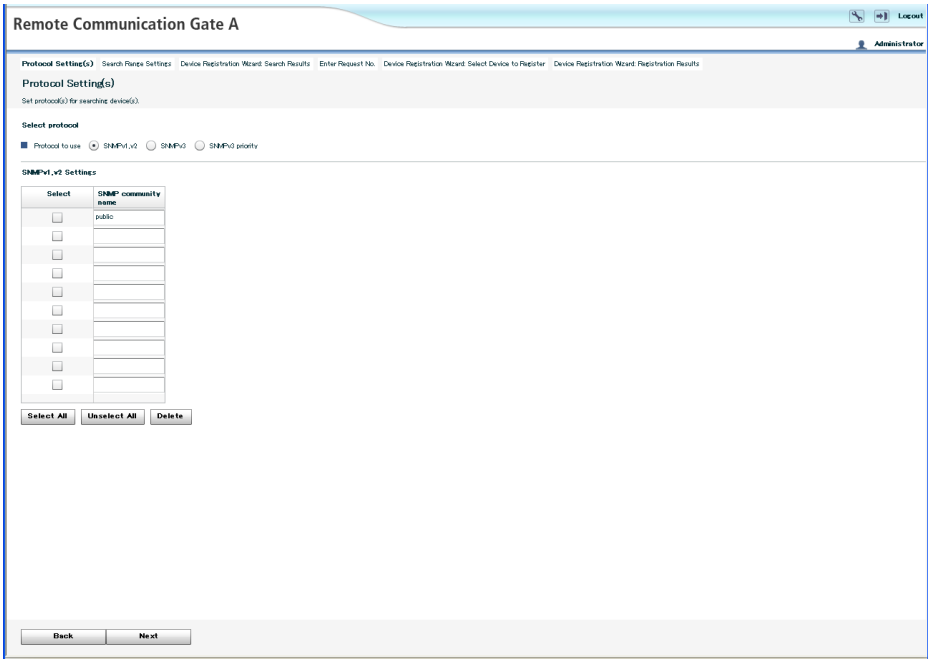
- **The search results can contain up to 100 devices. If you have installed optional memory and storage, the results can contain up to 1,000 devices. Contact your service representative for details.**
- **You can import search ranges from a CSV file stored on your computer. For details on creating a CSV file, see page 76 "To Create a CSV File".**

Searching for Devices by IPv4 Address

This section explains how to search for devices you want to register with the Communication Server by specifying IPv4 address ranges.

1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Device Registration Wizard].**

3. **Select a protocol for searching, and then click [Next].**



- If you select [SNMPv1,v2]:

  The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

  Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

  Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

- If you select [SNMPv3 priority]:

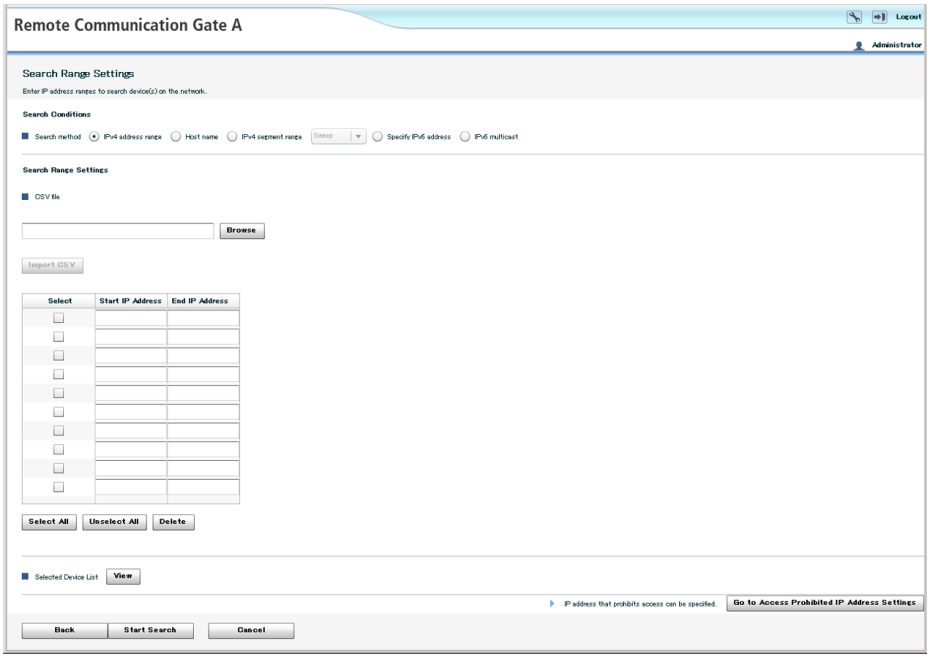
  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

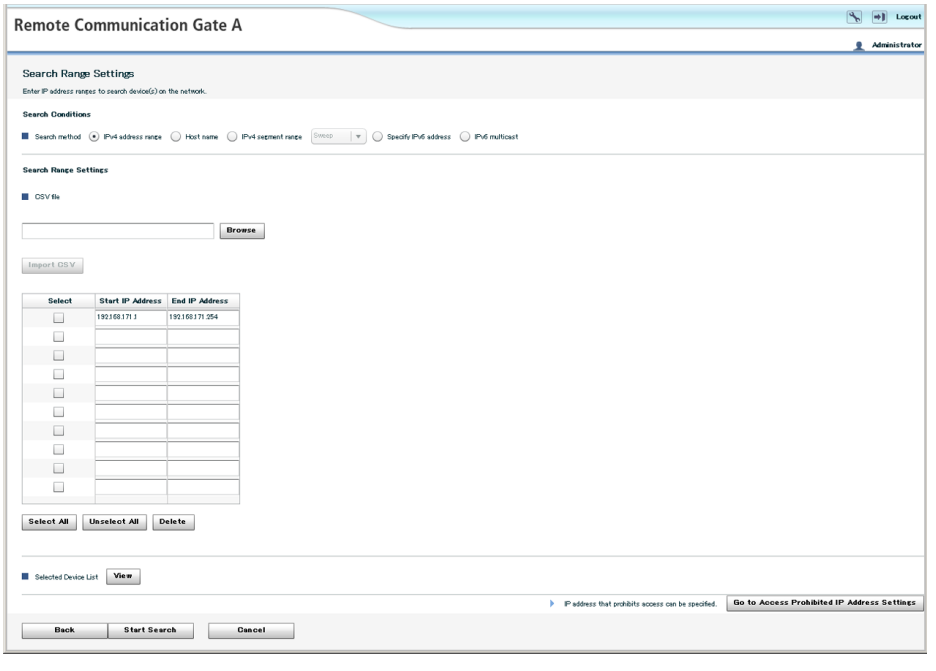
To cancel all selected items in the list, click [Unselect All].

4

4. Select [IPv4 address range] for the search method.



5. Set the search ranges.



- When entering the ranges directly:

Enter the starting IPv4 address and finishing IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 10 sets of addresses.

Enter a higher IPv4 address for the finishing IPv4 address than for the starting IPv4 address.

If you set "0.0.0.0" for the finishing address, the range of IPv4 address on the line will not be searched.

An error will occur if the value for the starting IPv4 address is "0.0.0.0" and the value for the finishing IPv4 address is other than "0.0.0.0".

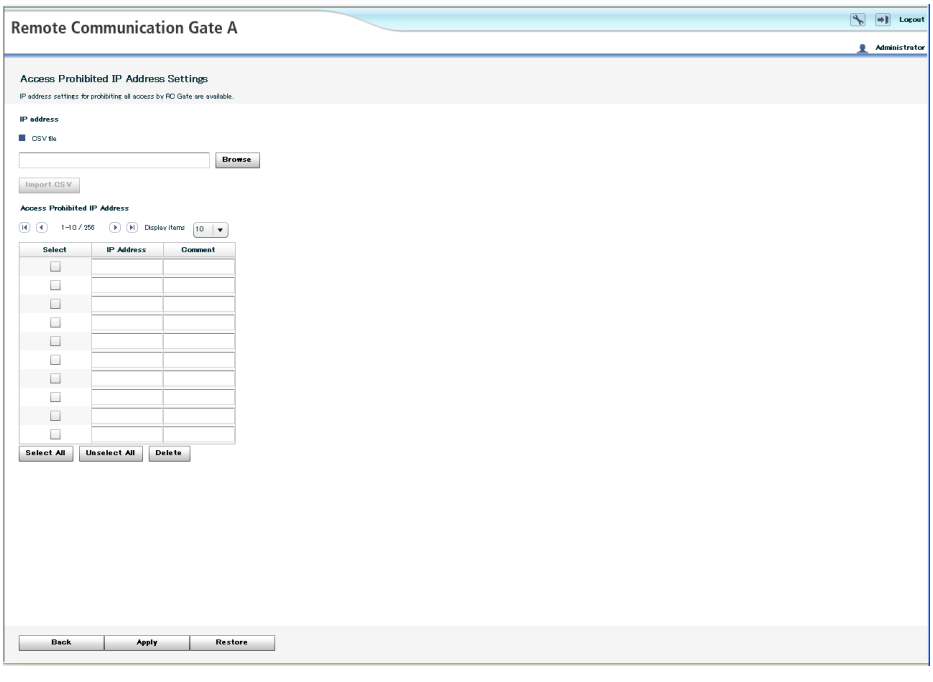
- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified ranges will be deleted.

6. **Click [Go to Access Prohibited IP Address Settings], and then specify the IPv4 address that you want to prohibit the RC Gate from accessing.**

   If you do not need to prohibit any IPv4 addresses, proceed to step 8.



- When entering the IPv4 address directly:

  Enter the IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 256 addresses.

- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

Once the search ranges have been imported from the CSV file, all previously specified ranges will be deleted.

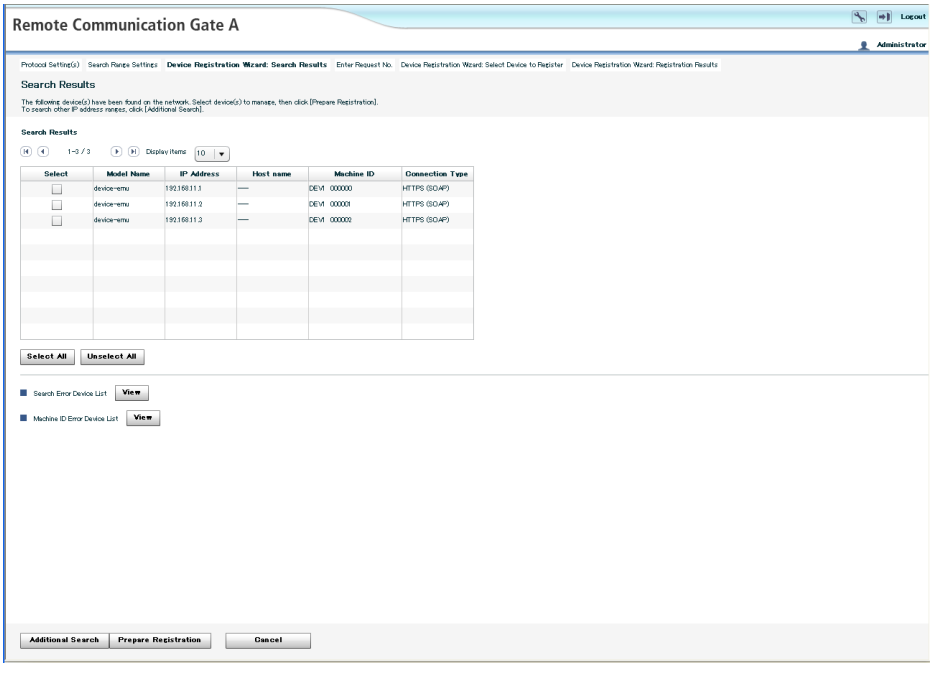
7. **Select the check boxes of the IPv4 address you want to prohibit, and then click [OK].**

   The screen returns to "Search Range Settings".

8. **Click [Start Search].**

   Device searching starts.

9. **Select the check boxes of the devices you want to register, and then click [Prepare Registration].**



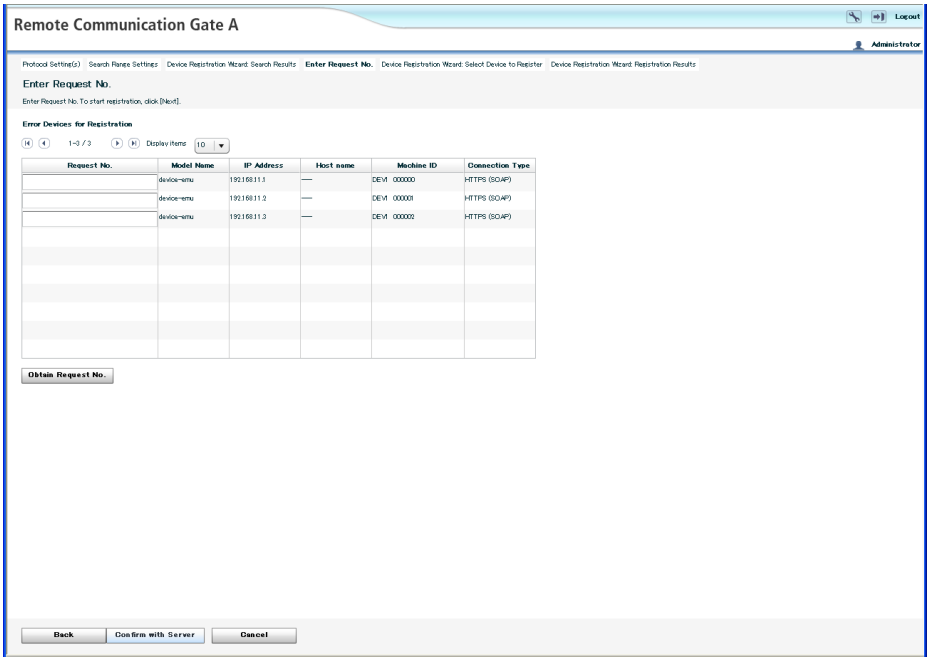
You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

The [Select] box masked in gray indicates that the device has been already registered to the Communication Server.

- [Select All]: Select all devices including the devices which are not on the current page.
- [Unselect All]: Cancel the selection of all devices including the devices which are not on the current page.
- [Additional Search]: Repeat searching and selecting of devices. Return to Step 5, and specify the searching ranges you want to add.
- [Machine ID Error Device List]: Display a list of the IP Address, MAC Address, Model Name of the devices for which the equipment could not identify the Machine ID.

10. **Enter request numbers for each device, and then click [Confirm with Server].**

    To have "Request No." automatically filled in, click [Obtain Request No.].



11. **Select the check boxes of the devices you want to register, and then click [Register].**

    To see the details of the confirmed devices, click [Machine ID]. Be sure to check the location of the devices when using multiple models of the same type.

    If "Failed" is displayed in "Confirmation Result", device registration has failed. Click [Machine ID] of a device whose result is "Failed".

12. **Confirm the registered items, and then click [Complete].**

    The screen returns to "Initial Settings".

Note

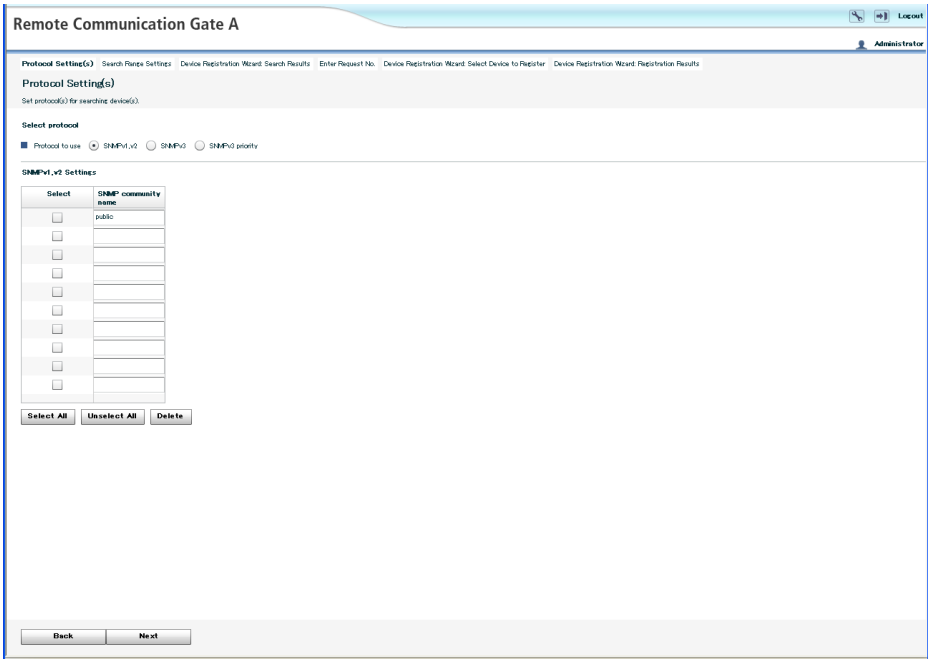
- You can specify the IPv4 addresses of the devices you want to prohibit the RC Gate from accessing after finishing "Device Registration Wizard". For details, see page 97 "Access Prohibited IP Address".

Searching for Devices by Host Name

This section explains how to search for devices you want to register with the Communication Server by specifying host names.

1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Device Registration Wizard].**

3. **Select a protocol for searching, and then click [Next].**



- If you select [SNMPv1,v2]:

  The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

  Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

  Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

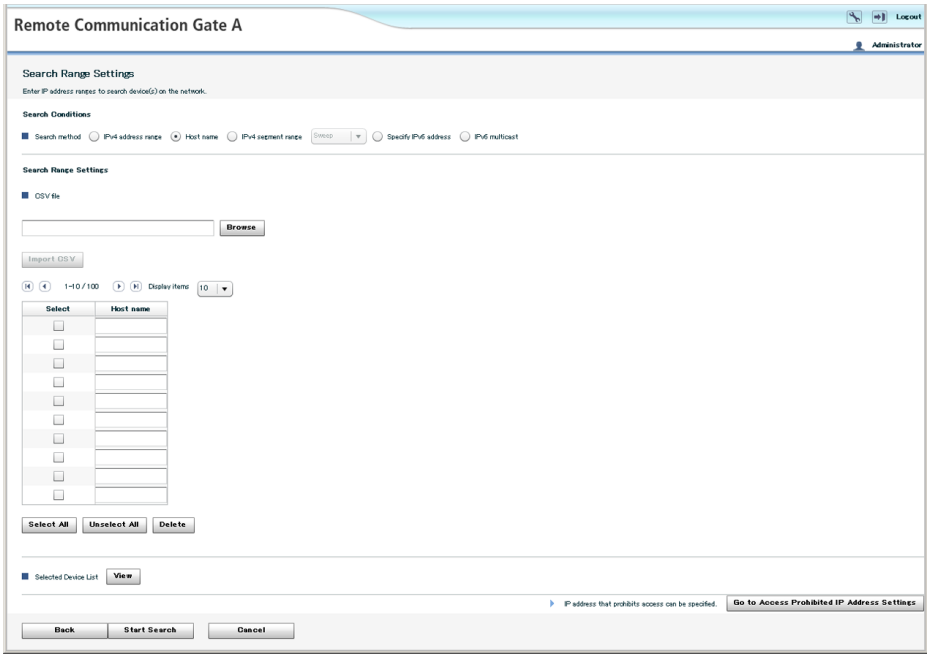
- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

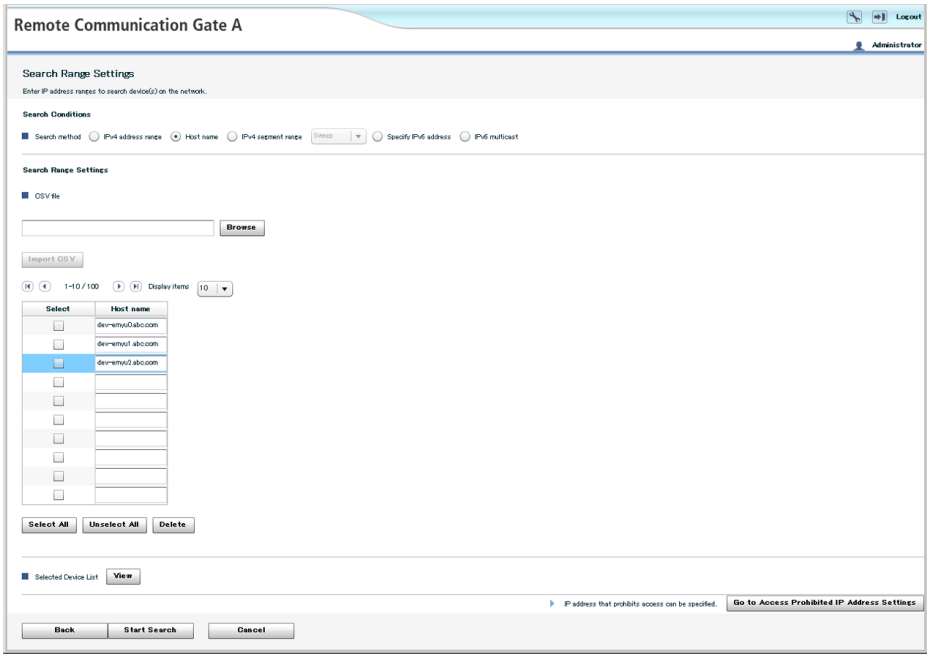
To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

4. Select [Host name] for the search method.



5. Set the search ranges.



- When entering the ranges directly:

Enter host names. You can enter up to 100 names (1,000 names if you have installed optional memory and storage).

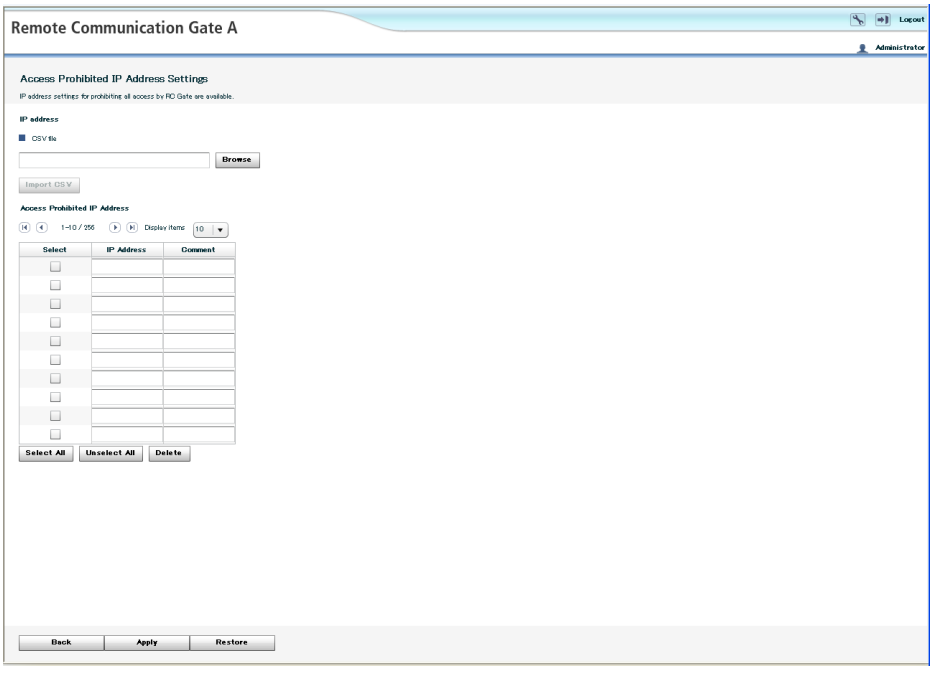
- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified IPv4 addresses will be deleted.

6. **Click [Go to Access Prohibited IP Address Settings], and then specify the IPv4 address that you want to prohibit the RC Gate from accessing.**

   If you do not need to prohibit any IPv4 addresses, proceed to Step 8.



- When entering the IPv4 address directly:

  Enter the IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 256 addresses.

- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified IPv4 addresses will be deleted.

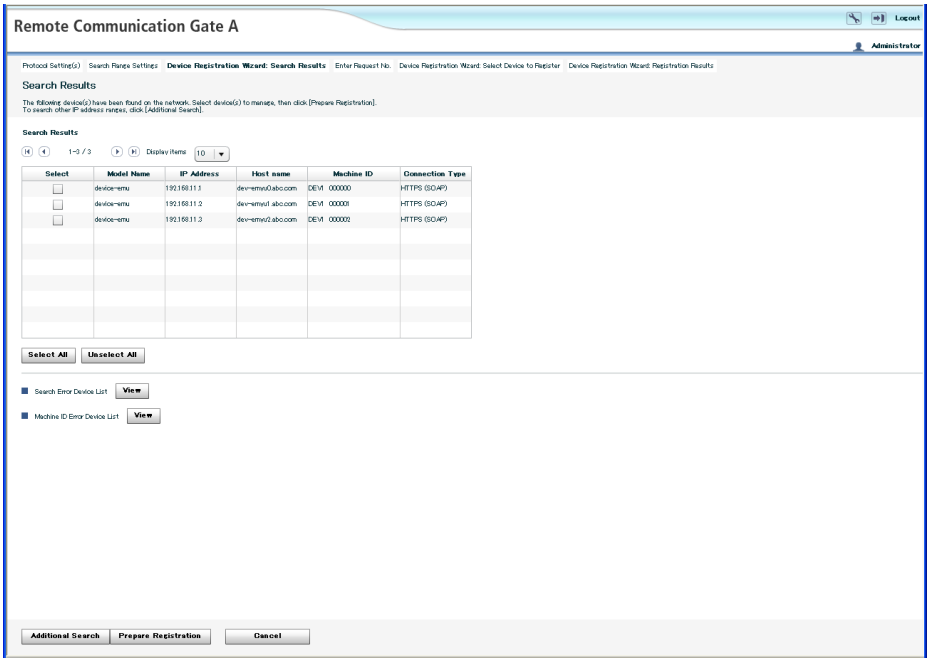
7. **Select the check boxes of the IPv4 address you want to prohibit, and then click [OK].**

   The screen returns to "Search Range Settings".

8. **Click [Start Search].**

   Device searching starts.

9. **Select the check boxes of the devices you want to register, and then click [Prepare Registration].**



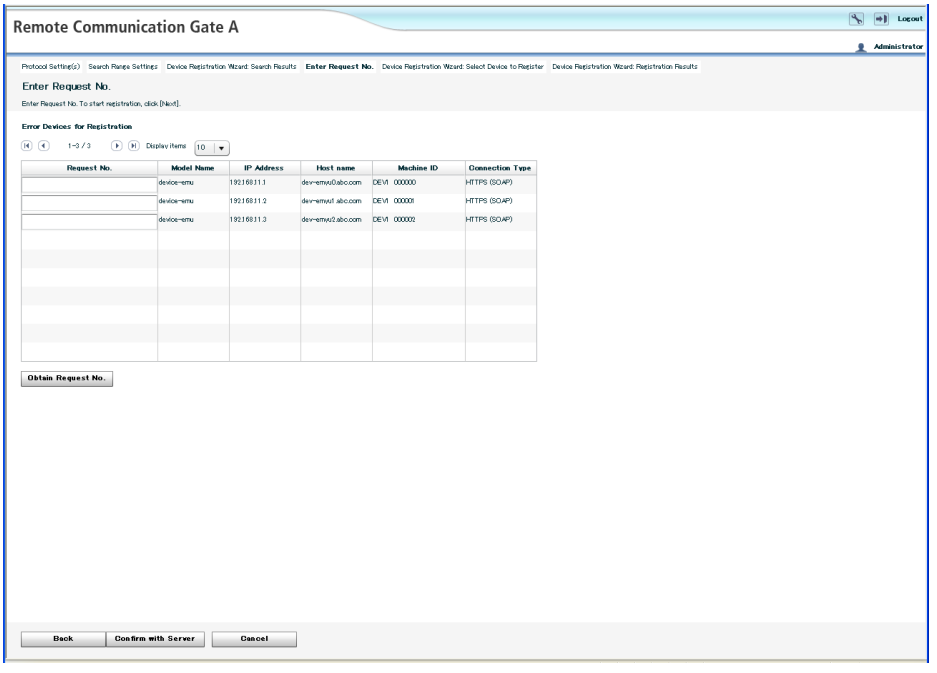
You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

The [Select] box masked in grey indicates that the device has been already registered to the Communication Server.

- [Select All]: Select all devices including the devices which are not on the current page.
- [Unselect All]: Cancel the selection of all devices including the devices which are not on the current page.
- [Additional Search]: Repeat searching and selecting of devices. Return to Step 5, and specify the searching ranges you want to add.
- [Search Error List]: Displays the hostname and IP address for which the RC Gate could not found.
- [Machine ID Error Device List]: Display a list of the IP Address, MAC Address, Model Name of the devices for which the equipment could not identify the Machine ID.

10. **Enter request numbers for each device, and then click [Confirm with Server].**

To have "Request No." automatically filled in, click [Obtain Request No.].



11. **Select the check boxes of the devices you want to register, and then click [Register].**

    To see the details of the confirmed devices, click [Machine ID]. Be sure to check the location of the devices when using multiple models of the same type.

    If "Failed" is displayed in "Confirmation Result", device registration has failed. Click [Machine ID] of a device whose result is "Failed".

12. **Confirm the registered items, and then click [Complete].**

    The screen returns to "Initial Settings"

Note

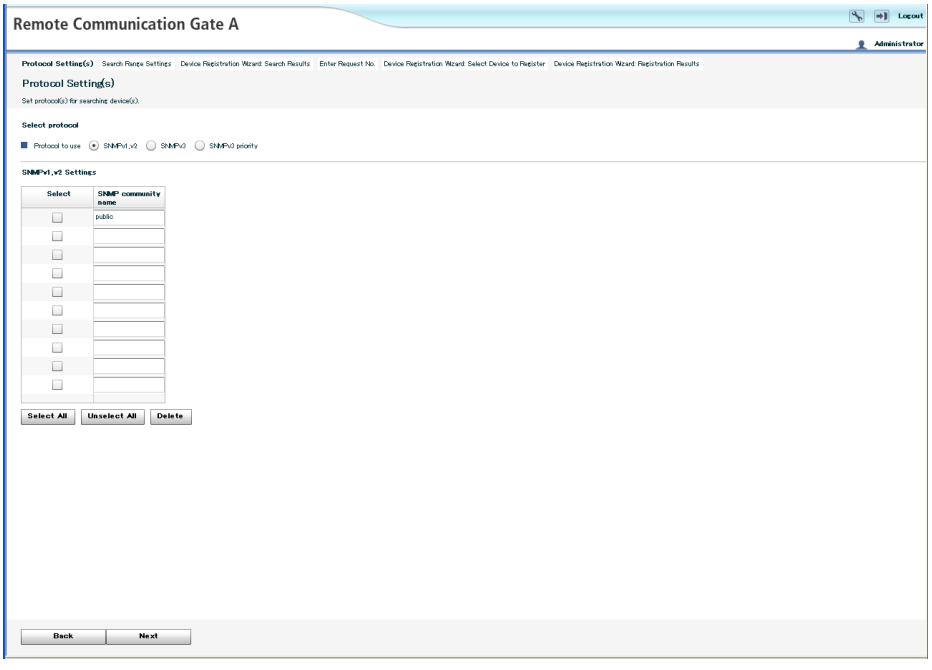
- You can specify the IPv4 addresses of the devices you want to prohibit the RC Gate from accessing after finishing "Device Registration Wizard". For details, see page 97 "Access Prohibited IP Address".

Searching for Devices by Segment

This section explains how to search for devices you want to register with the Communication Server by specifying network segments.

1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Device Registration Wizard].**

3. **Select a protocol for searching, and then click [Next].**



- If you select [SNMPv1,v2]:

  The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

  Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

  Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

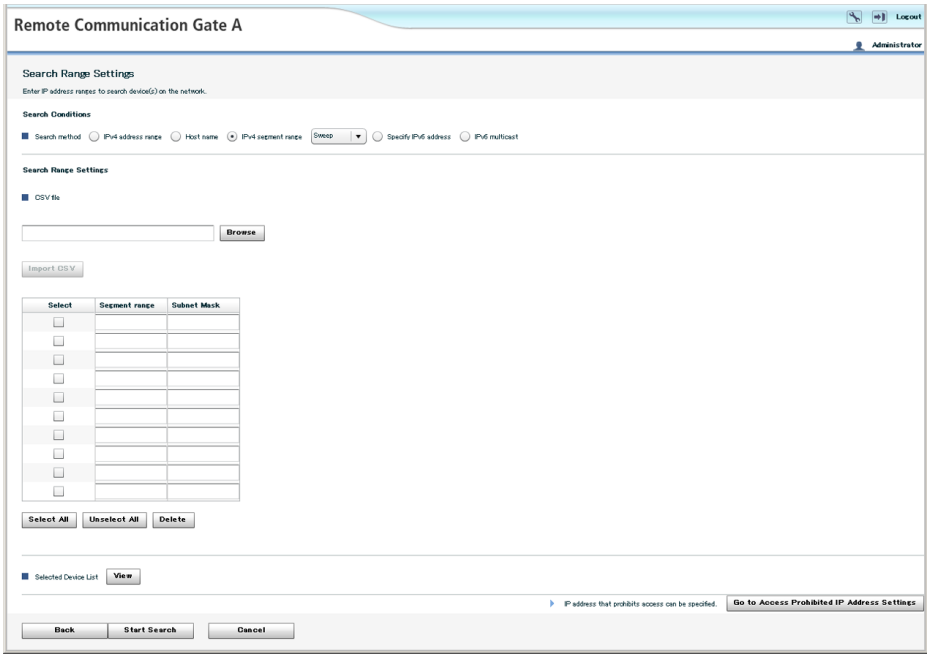
- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

4. Select [IPv4 segment range] for the search method.



Select one of the following search methods:

- Segment search by Sweep

  The RC Gate sends a ping to each IPv4 address (host addresses 1 to 254) in a specified network segment.

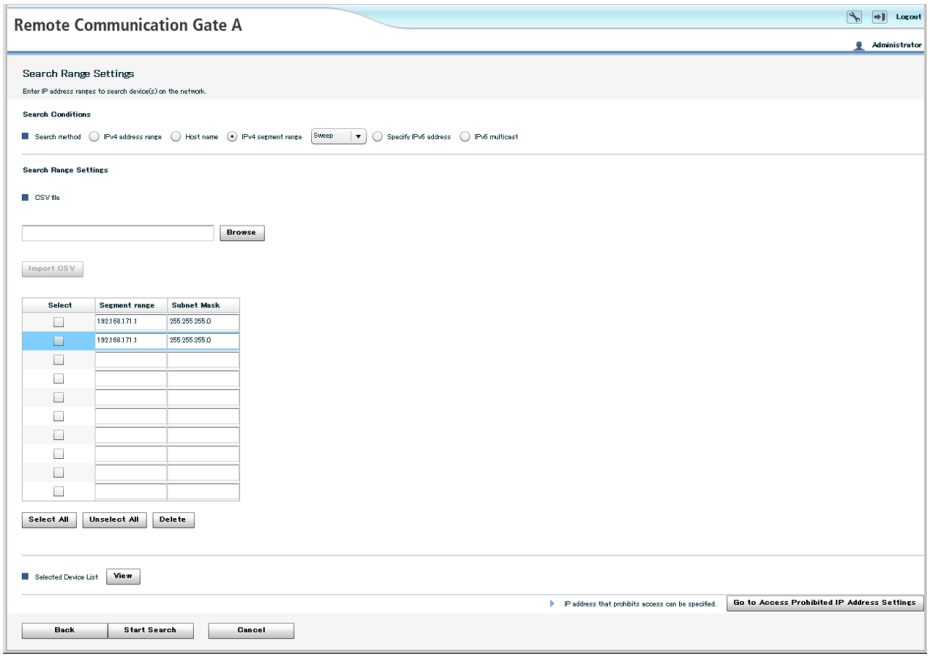
- Segment search by Broadcast

  The RC Gate issues an SNMP broadcast and searches any responding IPv4 addresses within the specified network segment.

To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

5. **Set the search ranges.**



- When entering the ranges directly:

  Enter the searching ranges and subnet mask as segment information. You can enter up to 10 sets of information.

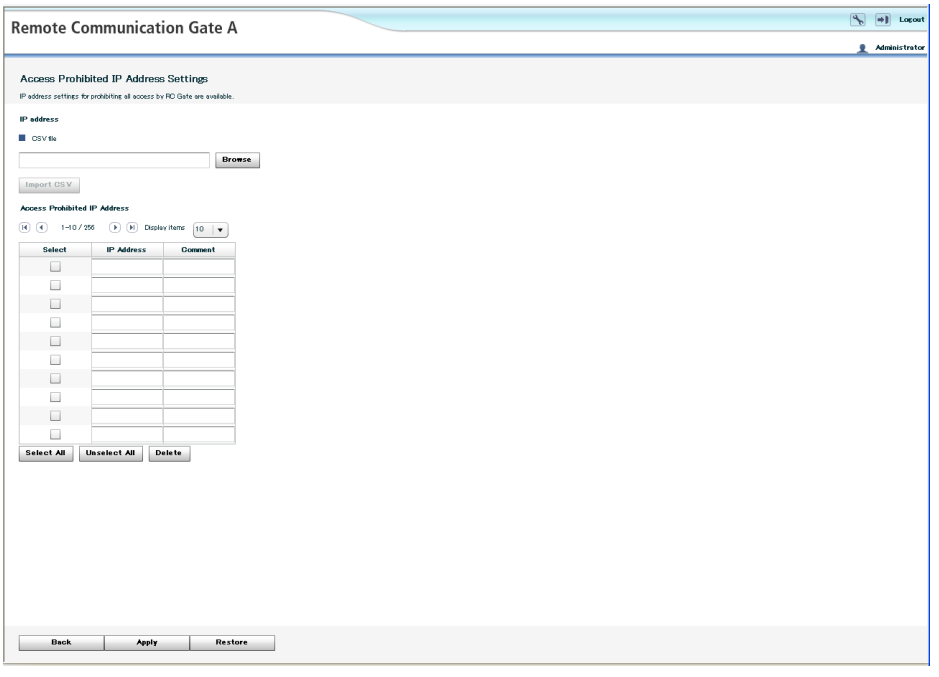
- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified ranges will be deleted.

6. **Click [Go to Access Prohibited IP Address Settings], and then specify the IPv4 address that you want to prohibit the RC Gate from accessing.**

   If you do not need to prohibit any IPv4 addresses, proceed to Step 8.



- When entering the IPv4 address directly:

  Enter the IPv4 address in "x.x.x.x" format ("x" standing for any number from 0 to 255). You can enter up to 256 addresses.

- When importing from a CSV file:

  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified IPv4 addresses will be deleted.

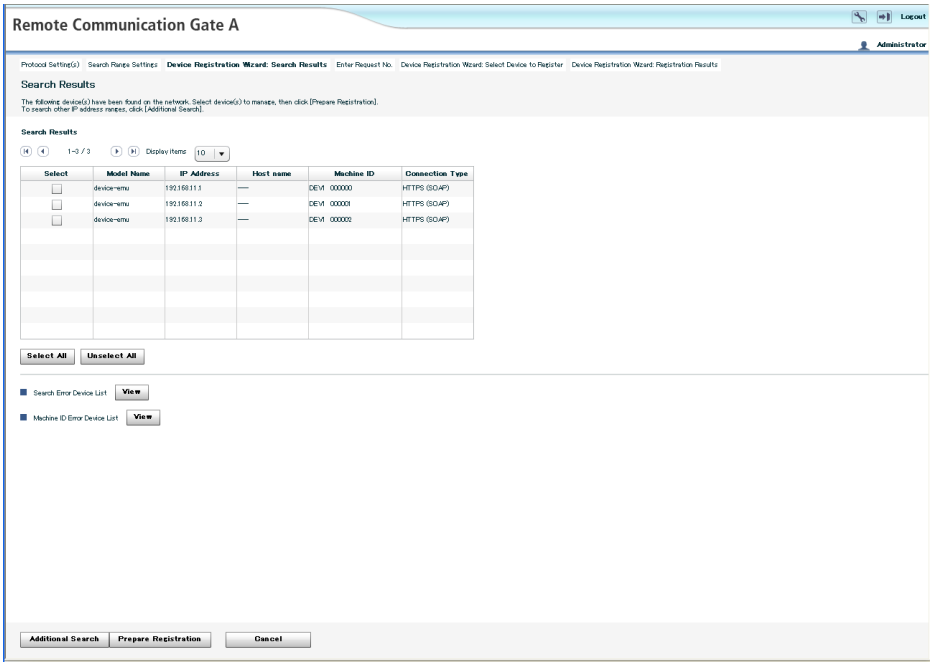
7. **Select the check boxes of the IPv4 address you want to prohibit, and then click [OK].**

   The screen returns to "Search Range Settings".

8. **Click [Start Search].**

   Device searching starts.

9. **Select the check boxes of the devices you want to register, and then click [Prepare Registration].**



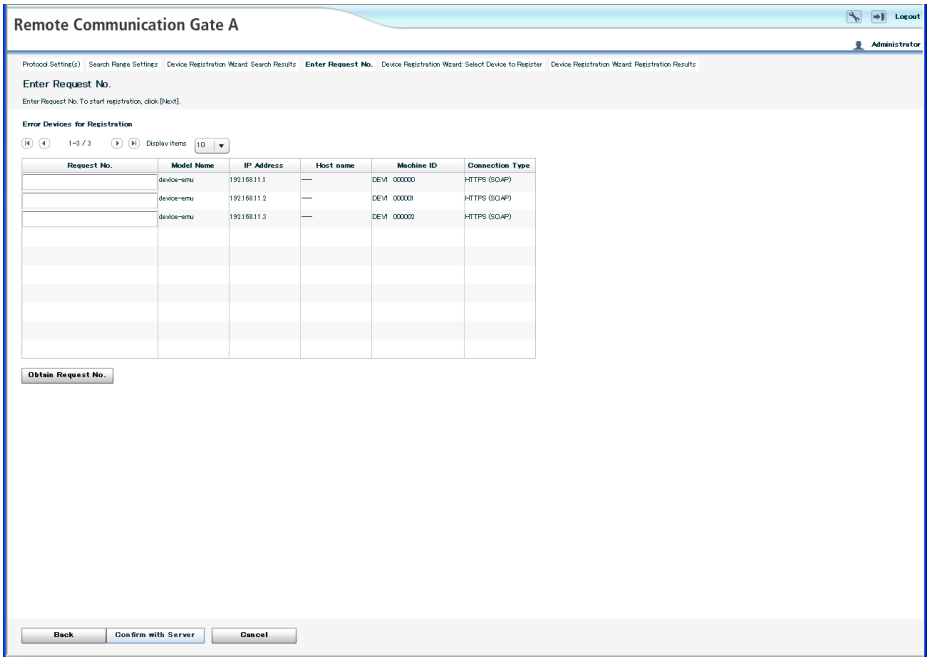
You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

The [Select] box masked in grey indicates that the device has been already registered to the Communication Server.

- [Select All]: Select all devices including the devices which are not on the current page.
- [Unselect All]: Cancel the selection of all devices including the devices which are not on the current page.
- [Additional Search]: Repeat searching and selecting of devices. Return to Step 5, and specify the searching ranges you want to add.
- [Machine ID Error Device List]: Display a list of the IP Address, MAC Address, Model Name of the devices for which the equipment could not identify the Machine ID.

10. **Enter request numbers for each device, and then click [Confirm with Server].**

To have "Request No." automatically filled in, click [Obtain Request No.].



11. **Select the check boxes of the devices you want to register, and then click [Register].**

    To see the details of the confirmed devices, click [Machine ID]. Be sure to check the location of the devices when using multiple models of the same type.

    If "Failed" is displayed in "Confirmation Result", device registration has failed. Click [Machine ID] of a device whose result is "Failed".

12. **Confirm the registered items, and then click [Complete].**

    The screen returns to "Initial Settings".

Note

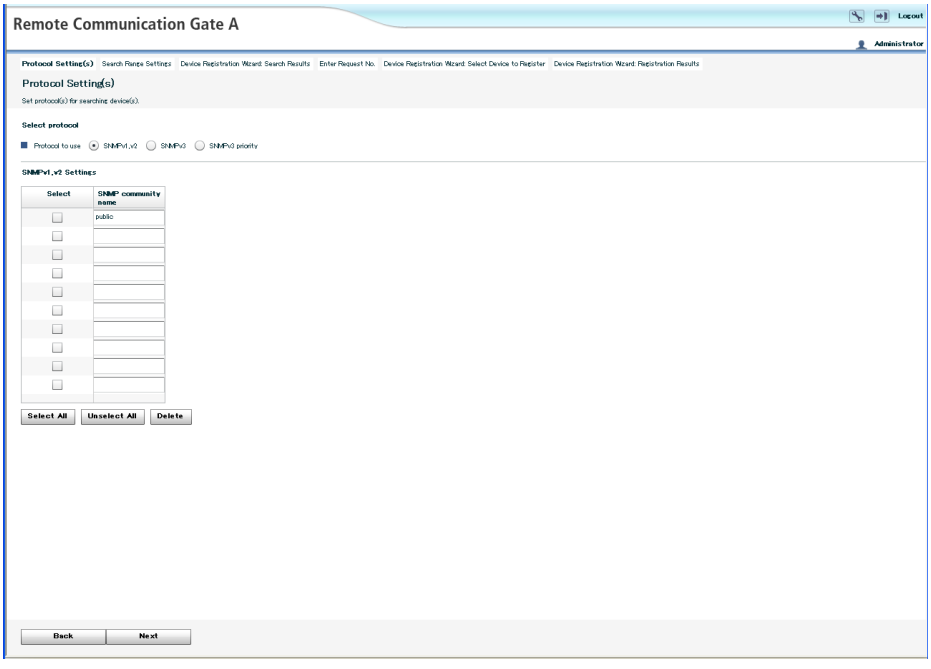
- You can specify the IPv4 addresses of the devices you want to prohibit the RC Gate from accessing after finishing "Device Registration Wizard". For details, see page 97 "Access Prohibited IP Address".

Searching for Devices by IPv6 Address

This section explains how to search for devices you want to register with the Communication Server by specifying IPv6 address.

1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Device Registration Wizard].**

3. **Select a protocol for searching, and then click [Next].**



- If you select [SNMPv1,v2]:

  The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

  Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

  Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

- If you select [SNMPv3 priority]:

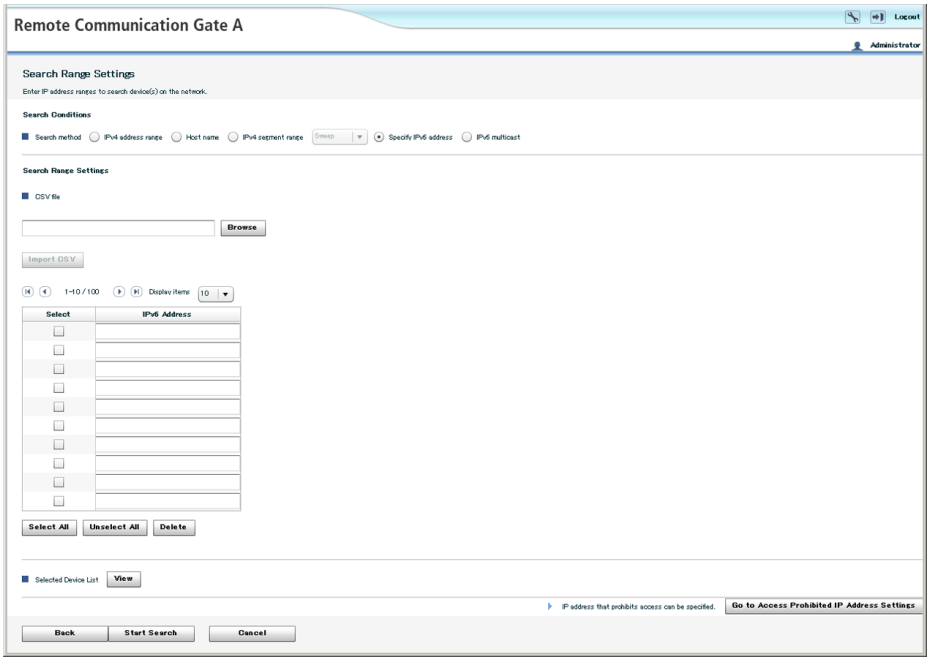
  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

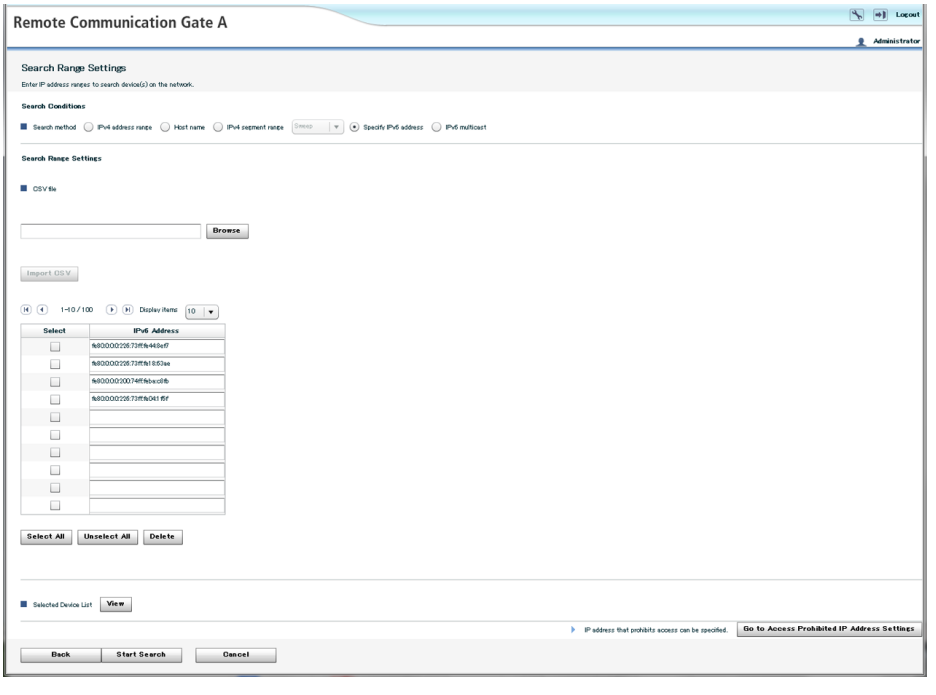
To cancel all selected items in the list, click [Unselect All].

4

4. Select [IPv6 address] for the search method.



5. Set the search ranges.



- When entering IPv6 addresses directly:

Enter IPv6 addresses in “xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx” format (”x” standing for hexadecimal number. Consecutive “0” can be omitted.). You can enter up to 100 sets of addresses (1,000 sets of addresses if you have installed optional memory and storage).

- When importing from a CSV file:

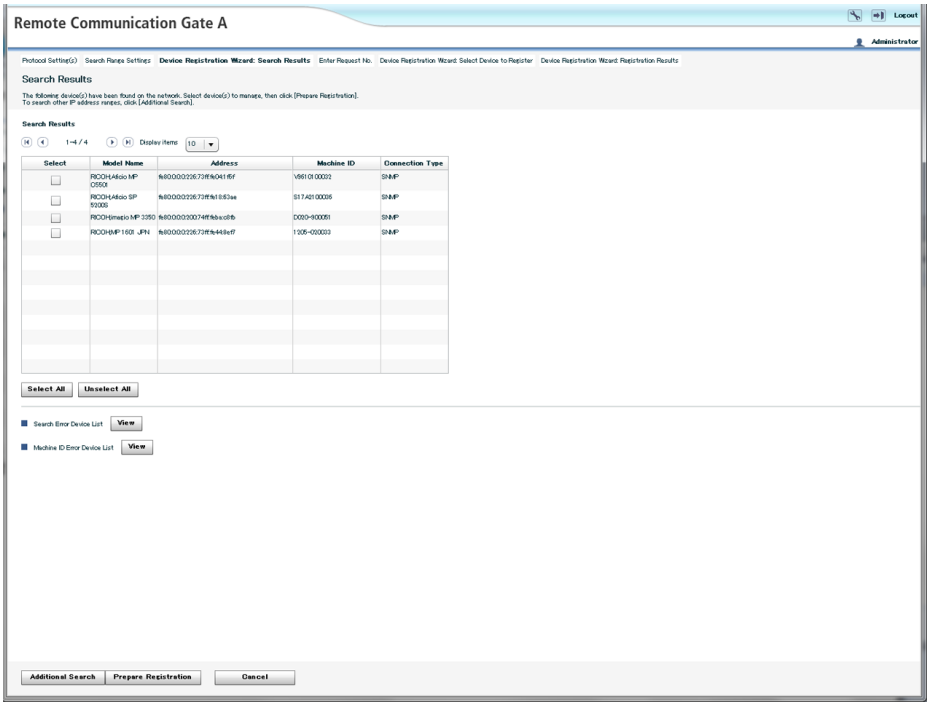
  Click [Browse], locate your CSV file, and then click [Import CSV].

  Once the search ranges have been imported from the CSV file, all previously specified ranges will be deleted.

6. **Click [Start Search].**

   Device searching starts.

7. **Select the check boxes of the devices you want to register, and then click [Prepare Registration].**



You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

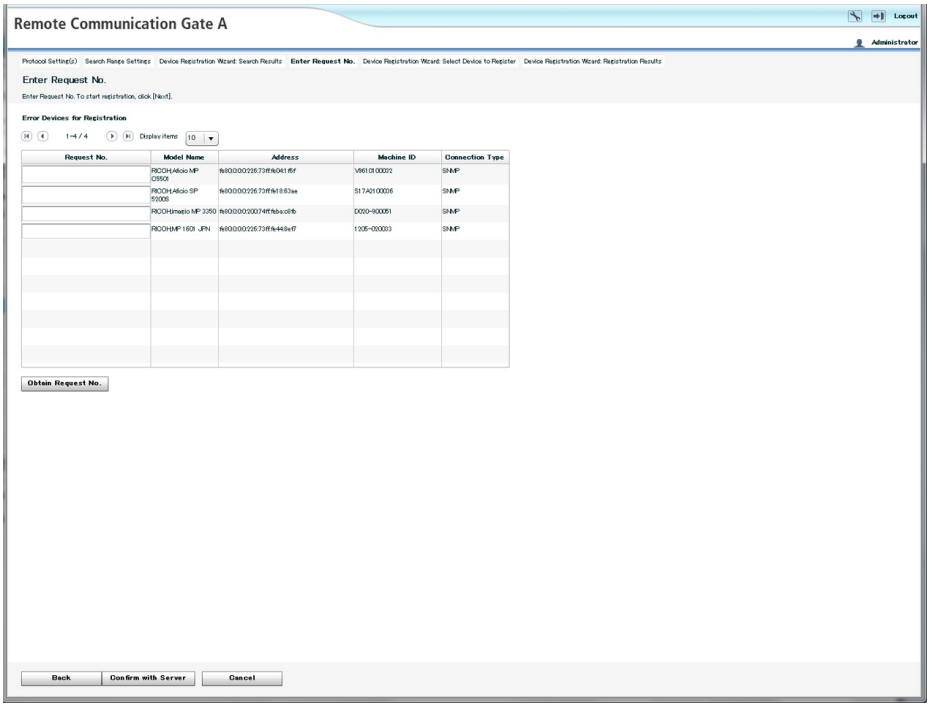
The [Select] box masked in grey indicates that the device has been already registered to the Communication Server.

- [Select All]: Select all devices including the devices which are not on the current page.
- [Unselect All]: Cancel the selection of all devices including the devices which are not on the current page.

- [Machine ID Error Device List]: Display a list of the IPv6 Address, MAC Address, Model Name of the devices for which the equipment could not identify the Machine ID.

8. **Enter request numbers for each device, and then click [Confirm with Server].**

   To have "Request No." automatically filled in, click [Obtain Request No.].



9. **Select the check boxes of the devices you want to register, and then click [Register].**

   To see the details of the confirmed devices, click [Machine ID]. Be sure to check the location of the devices when using multiple models of the same type.

   If "Failed" is displayed in "Confirmation Result", device registration has failed. Click [Machine ID] of a device whose result is "Failed".

10. **Confirm the registered items, and then click [Complete].**

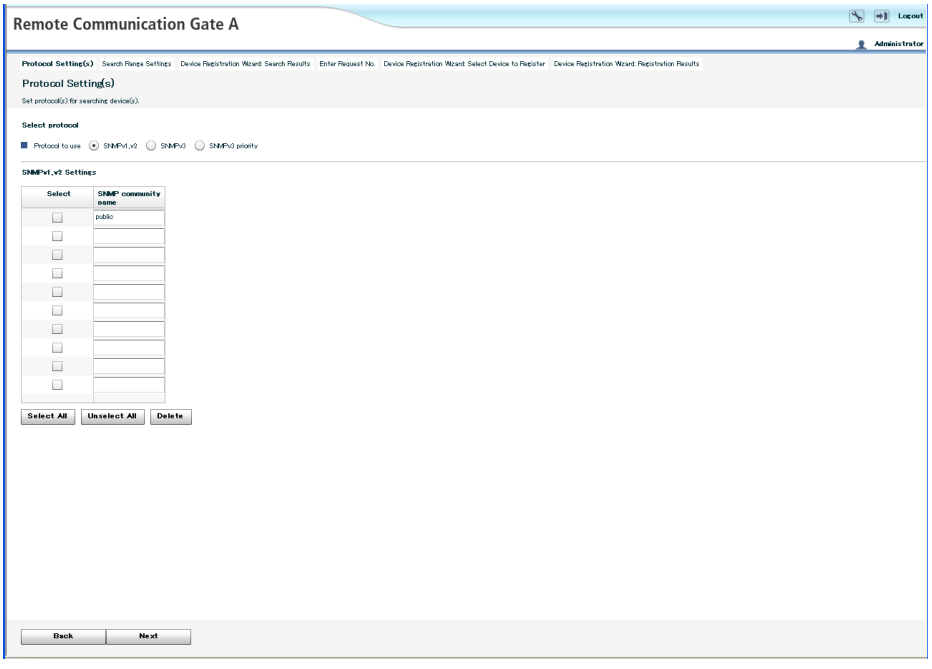
    The screen returns to "Initial Settings".

Searching for Devices by IPv6 Multicast Address

This section explains how to search for devices you want to register with the Communication Server by IPv6 multicast addresses “FF02::1.”

1. **Start the RC Gate Monitor, and then log in as [Administrator].**
2. **Click [Device Registration Wizard].**

3. **Select a protocol for searching, and then click [Next].**



- If you select [SNMPv1,v2]:

  The SNMP community name serves as a password when the RC Gate tries to access the SNMP-compatible devices. For details, see the operating instructions for each device.

  Enter the SNMP community name in order of highest frequency to lowest frequency. (You can enter up to 30 ASCII characters per name. You can enter up to 10 names). Remove any SNMP community names that are not in use on your network.

  Leave the item blank if the managing devices are only HTTPS-compatible devices.

- If you select [SNMPv3]:

  Enter at least one set for user name, authentication password, and encryption password. You can enter up to 10 sets.

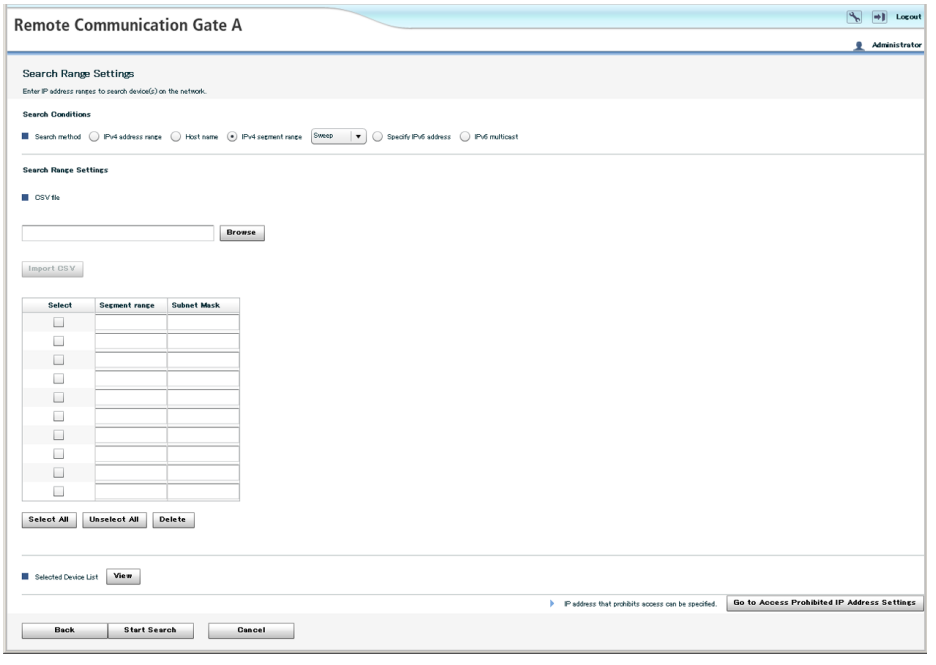
- If you select [SNMPv3 priority]:

  This protocol uses the SNMPv3 and SNMPv1,v2 protocols. The RC Gate will first attempt to search a device using the SNMPv3 protocol. If a device does not support SNMPv3, the RC Gate will attempt to search a device using the SNMPv1,v2 protocol.

To select all items in the list, click [Select All].

To cancel all selected items in the list, click [Unselect All].

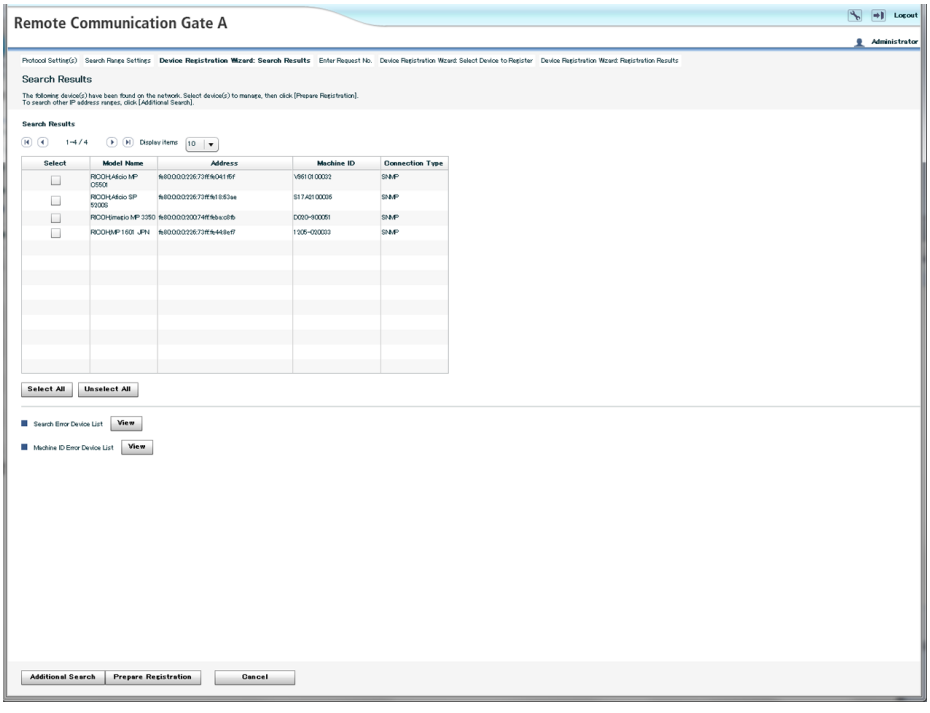
4. Select [IPv6 multicast] for the search method.



5. Click [Start Search].

Device searching starts.

6. **Select the check boxes of the devices you want to register, and then click [Prepare Registration].**



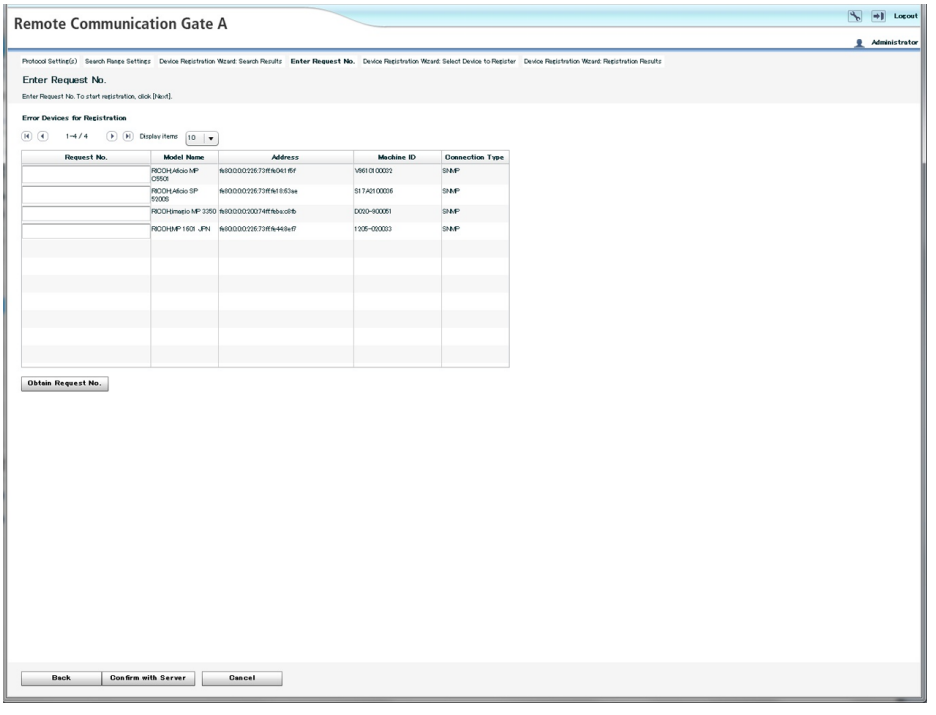
You can switch pages by clicking the button on the left/right of the displayed number. The number of displayed ranges on the current page can be changed using the "Display items" list.

The [Select] box masked in grey indicates that the device has been already registered to the Communication Server.

- [Select All]: Select all devices including the devices which are not on the current page.
- [Unselect All]: Cancel the selection of all devices including the devices which are not on the current page.
- [Machine ID Error Device List]: Display a list of the IPv6 Address, MAC Address, Model Name of the devices for which the equipment could not identify the Machine ID.

7. **Enter request numbers for each device, and then click [Confirm with Server].**

To have "Request No." automatically filled in, click [Obtain Request No.].



8. **Select the check boxes of the devices you want to register, and then click [Register].**

   To see the details of the confirmed devices, click [Machine ID]. Be sure to check the location of the devices when using multiple models of the same type.

   If "Failed" is displayed in "Confirmation Result", device registration has failed. Click [Machine ID] of a device whose result is "Failed".

9. **Confirm the registered items, and then click [Complete].**

   The screen returns to "Initial Settings".

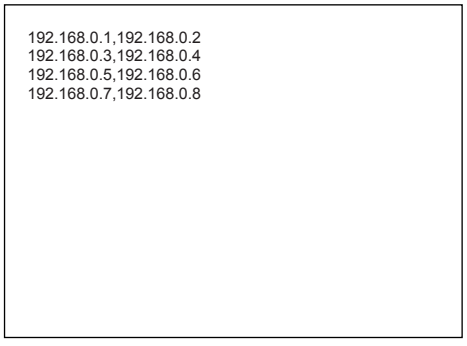
To Create a CSV File

To import a CSV file, you must create a CSV file.

CSV file for specifying the search ranges by IPv4 address:

For each IPv4 address range, enter the starting IPv4 address and finishing IPv4 address, separated by a comma. Enter each address range on a separate line. You can enter up to 256 sets of addresses.

Example:

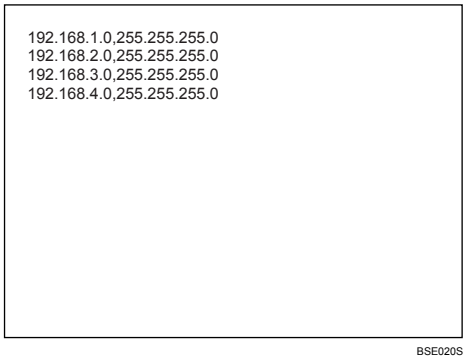


BSE019S

CSV file for specifying the search ranges by network segment:

To create the CSV file, enter the information for each network segment by separating it with a comma. Each line should contain the subnet IP address and subnet mask. You can enter up to 256 sets of information.

Example:



BSE020S

CSV file for specifying the search ranges by host name:

To create the CSV file, enter host names in each line. You can enter up to 100 names.

Example:

```
host0
host1
host2
host3
host4
```

BSE017S

CSV file for specifying IPv6 addresses:

To create the CSV file, enter the IPv6 address in each line. You can enter up to 100 addresses.

Example

```
2001:DB8::1:0
2001:DB8::2:0
2001:DB8::3:0
2001:DB8::4:0
```

BSE023S

CSV file for specifying access prohibited IP addresses:

To create the CSV file, enter the information for each IP address by separating it with a comma. Each line should contain the IP address and comment. You can enter up to 256 sets of addresses.

Example

```
192.168.0.1,GatewayRouter
192.168.0.2,FileServer
```

BSE018S

5. Configuring the Details of the Registered Information

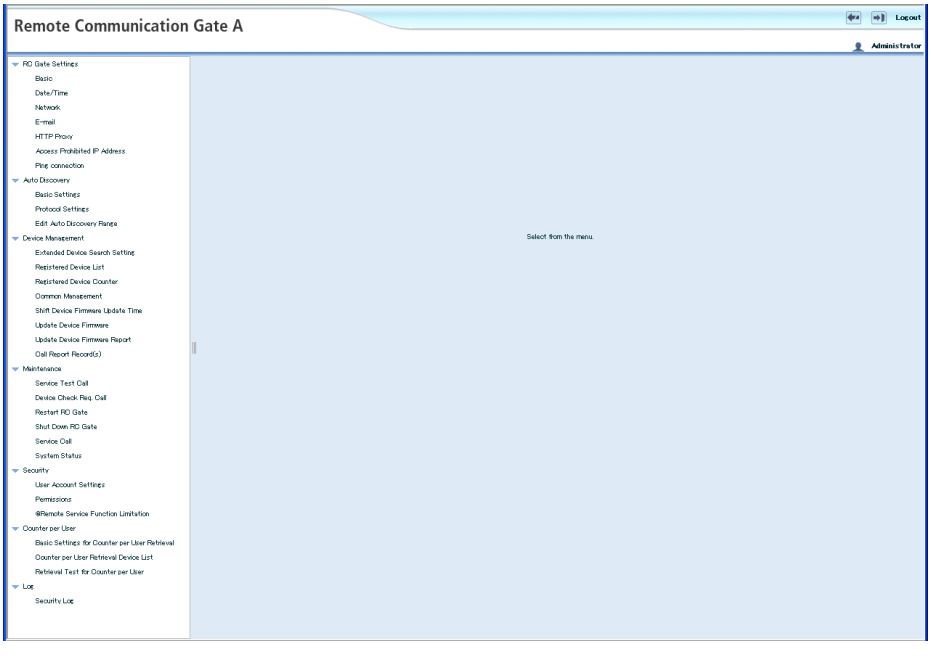
This chapter explains operations that can be done from each screen of the "RC Gate Configuration".

Name of Screens Displayed from [RC Gate Configuration]

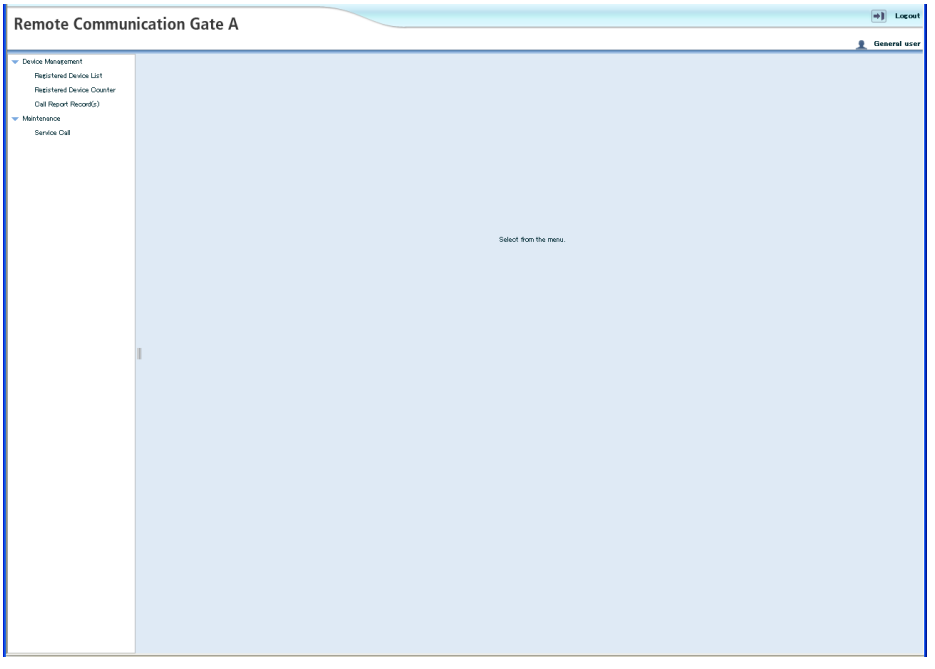
The following tables provide the menus that are displayed when [RC Gate Configuration] has been selected at login.

Menus and the screens differ whether the logged in user is [Administrator] or [General user].

Administrator



General User



RC Gate Settings

Screen Name	Outline
Basic	Displays the detailed information of the RC Gate.
Date/Time	Adjusts the clock inside the RC Gate.
Network	Configures the network settings.
HTTP Proxy	Sets the HTTP Proxy.
E-mail	Configures the types of e-mail sent to the administrator.
Access Prohibited IP Address	Specifies the IP address of devices that you want to prohibit the RC Gate from accessing.
Ping connection	Sets whether to allow ping transmission for searching for devices on the network.

Auto Discovery

Screen Names	Outline
Basic Settings	Sets basic item for Auto Discovery, such as usage and schedule.

Screen Names	Outline
Protocol Settings	Sets the search protocol for Auto Discovery.
Edit Auto Discovery Range	Sets the ranges of IP address or network segments for Auto Discovery.

Device Management

Screen Names	Outline
Extended Device Search Setting	Sets whether to enable the extended device searching.
Registered Device List	Displays the information of the devices managed by the RC Gate.
Call Report Record(s)	The dates and types of calls received from devices managed by the RC Gate Monitor are displayed together with the device information.
Registered Device Counter	Displays device counter list screen.
Common Management	Displays settings common to all devices managed by the RC Gate.
Shift Device Firmware Update Time	Specifies the time of device firmware update for each segment.
Update Device Firmware	When a notice comes from the Communication Server, updates the firmware of the devices managed by the RC Gate.
Update Device Firmware Report	Displays the previous device firmware update history.

Maintenance

Screen Names	Outline
Service Test Call	Tests communications with the Communication Server.
Device Check Req. Call	Tests communications with the Communication Server and sends the results to the Communication Server.
Restart RC Gate	Reboots the RC Gate.
Shut Down RC Gate	Shuts down the RC Gate.
Service Call	Displays the substances of the errors.

Screen Names	Outline
System Status	Displays the system status of the RC Gate.

Security

Screen Names	Outline
User Account Settings	Sets the user accounts that can access to the RC Gate monitor.
Permissions	Limits the login of the customer engineer.
@Remote Service Function Limitation	Restricts "@Remote service functions".

Counter per User

Screen Names	Outline
Basic Settings for Counter per User Retrieval	Used to make settings for obtaining information from a device needed to retrieve the counter for each user.
Counter per User Retrieval Device List	Displays a list of devices from which to obtain the information needed to retrieve the counter for each user.
Retrieval Test for Counter per User	Determines whether the information needed to retrieve the counter for each user can be obtained from the device.

Log

Screen Names	Outline
Security Log	Displays the log information of users.

Details of Screens Displayed from [RC Gate Configuration]

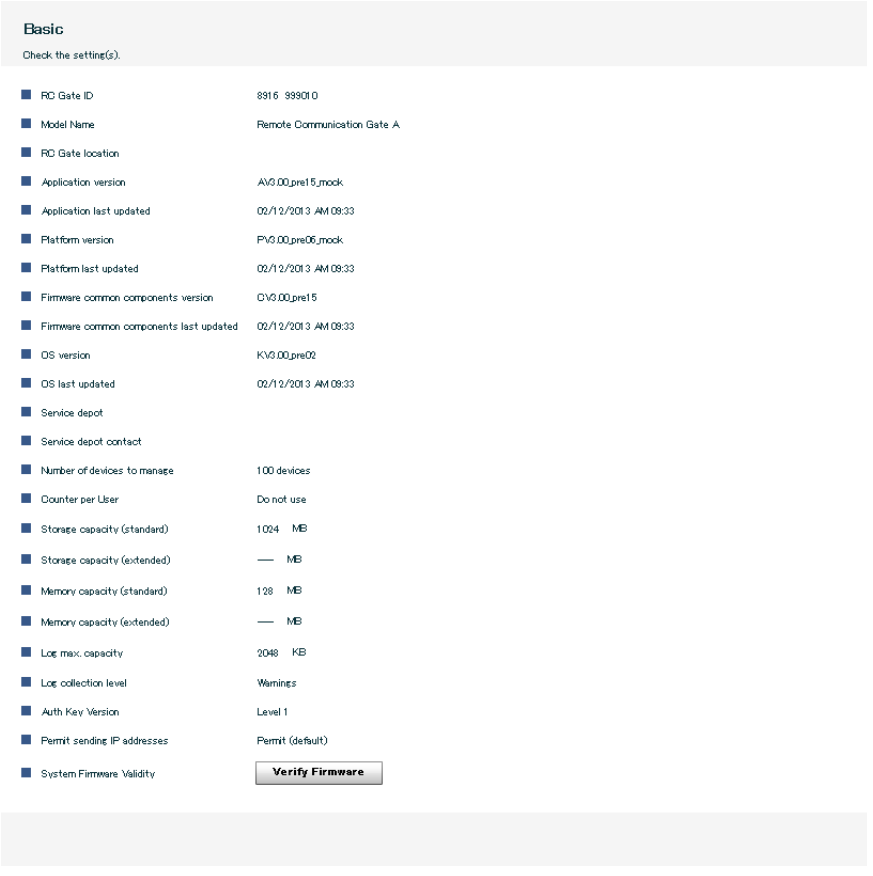
This section explains the items displayed on each screen.

Buttons Displayed on Each Screen

Button Names	Outline
Apply	Applies the current settings. The clock starts when you click this button on the "Date/Time" screen.
OK	Displays a confirmation dialog.
Back	Returns to the previous screen without applying the current settings.

Basic

You can confirm the detailed information of the RC Gate. To display the screen, click [RC Gate Settings] - [Basic].



Item	Description
RC Gate ID	A serial number to identify the RC Gate. A unique ID is set to the RC Gate.
Model name	A model name for the RC Gate.
RC Gate location	A place/section where the RC Gate is set.
Application version	Software version that is built into the RC Gate.
Application last updated	The last update date of the built-in software.
Platform version	The version of the base software that operates the built-in applications.
Platform last updated	The last update date of the platform.
Firmware common components version	The version of the common software used by the RC Gate.

Item	Description
Firmware common components last updated	The last update date of the common software.
OS version	The current operating system version of the RC Gate.
OS last updated	The last update date of the operating system that is built into the RC Gate.
Service depot	The service depot of the RC Gate.
Service depot contact	The phone number of the service depot.
Number of devices to manage	The number of devices that can be managed by the RC Gate.
Counter per User	Counter information on a per-user basis.
Storage capacity (standard)	The storage capacity, not including expanded storage.
Storage capacity (extended)	The storage capacity of the expanded storage. Does not include the standard storage capacity.
Memory capacity (standard)	The memory capacity, not including expanded memory.
Memory capacity (extended)	The memory capacity of the expanded memory. Does not include the standard memory capacity.
Log max. capacity	The maximum value of the log files which the RC Gate collects.
Log collection level	The log level for which the RC Gate collects (Errors, warnings, operation, and information).
Auth Key Version	The current authentication certificate version of the RC Gate.
Permit sending IP addresses	The current condition if sending the IP addresses of the RC Gate and the registered devices to the Communication Server is permitted or not.
System Firmware Validity	Click [Verify Firmware] to check the validity of the software included in the RC Gate.

Date/Time

You can confirm and change the clock of the RC Gate. To display the settings screen, click [RC Gate Settings] - [Date/Time].

Important

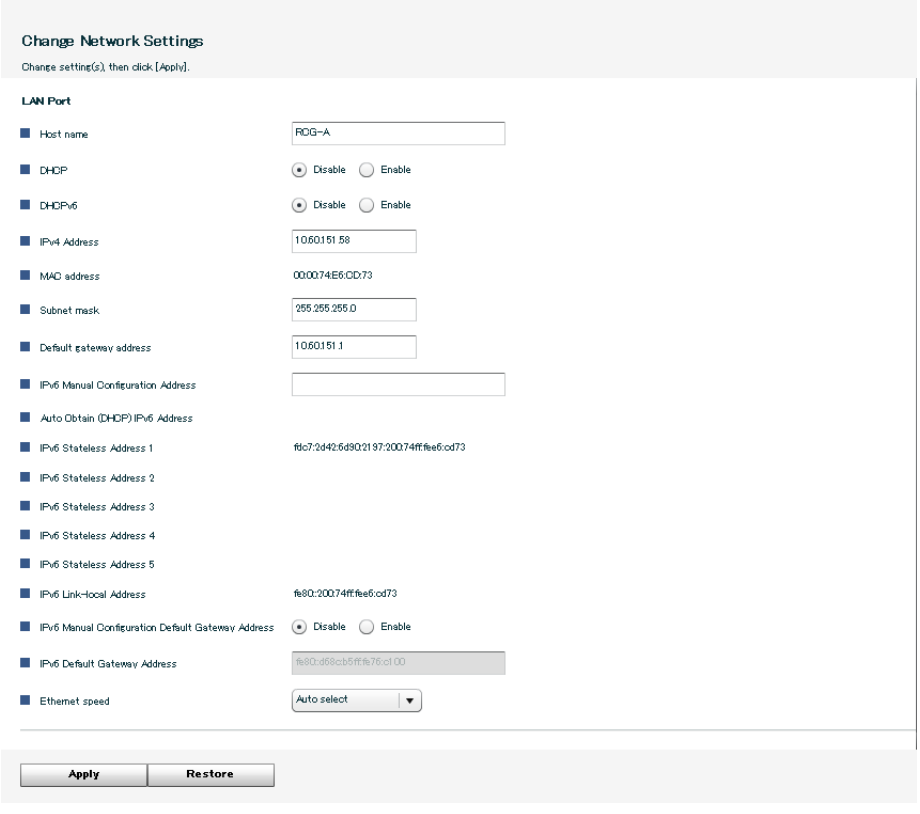
- **Check the time and date regularly, and correct them if necessary.**

Item	Description
Time zone	The standard time of the place where the RC Gate is set (The time zone indicates the time difference from Universal Coordinated Time).
Set date	Set the current date of the place where the RC Gate is set.
Set time	Set the current time of the place where the RC Gate is set. Set it to the current time.

Network

You can change and confirm the network settings of the RC Gate. To display the settings screen, click [RC Gate Settings] - [Network].

After changing the network settings, you have to log in to the RC Gate again. Click the URL that appears on the screen to re-open the Web browser. If you are using a DHCP server, directly enter the URL that appears on the screen in the address bar of your browser.



LAN Port

Item	Description
Host name	A host name for the RC Gate.
DHCP	Select [Enable] for the environment using the DHCP server.
DHCPv6	Select [Enable] for the environment using the DHCPv6 server.
IPv4 address	An IPv4 address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, an IPv4 address that is assigned by the DHCP server will be displayed.
MAC address	A MAC address of the RC Gate (LAN port).
Subnet mask	A subnet mask for the RC Gate. If [Enable] is selected for the DHCP, a subnet mask that is assigned by the DHCP server will be displayed.

Item	Description
Default gateway address	A gateway address for the RC Gate. If [Enable] is selected for the DHCP, an IPv4 address that is assigned by the DHCP server will be displayed.
IPv6 Manual Configuration Address	An IPv6 address for the RC Gate (LAN port).
IPv6 Stateless Address 1	An IPv6 address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, an IPv6 address that is assigned by the DHCP server will be displayed.
IPv6 Stateless Address 2	An IPv6 address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, an IPv6 address that is assigned by the DHCP server will be displayed.
IPv6 Stateless Address 3	An IPv6 address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, an IPv6 address that is assigned by the DHCP server will be displayed.
IPv6 Stateless Address 4	An IPv6 address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, an IPv6 address that is assigned by the DHCP server will be displayed.
IPv6 Stateless Address 5	An IPv6 address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, an IPv6 address that is assigned by the DHCP server will be displayed.
IPv6 Link-local Address	A link local address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, a link local address that is assigned by the DHCP server will be displayed.
IPv6 Default Gateway Address	A gateway address for the RC Gate (LAN port). If [Enable] is selected for the DHCP, a gateway address that is assigned by the DHCP server will be displayed.
Ethernet speed	Select the Ethernet speed for the LAN port of the RC Gate.

DNS Server

Item	Description
Main DNS server	Enter the IP address of the DNS server which the RC Gate mainly uses. Enter the IP address in "x.x.x.x" format ("x" stands for a number from 0 to 255). This is not required when you enter the proxy server or SMTP server by its IP address instead of its name.
Sub DNS server	Enter the IP address of the Sub DNS server to use a secondary DNS Server when the main DNS server cannot be used for some reason. Enter the IP address in "x.x.x.x" format ("x" stands for a number from 0 to 255).

IEEE802.1x authentication

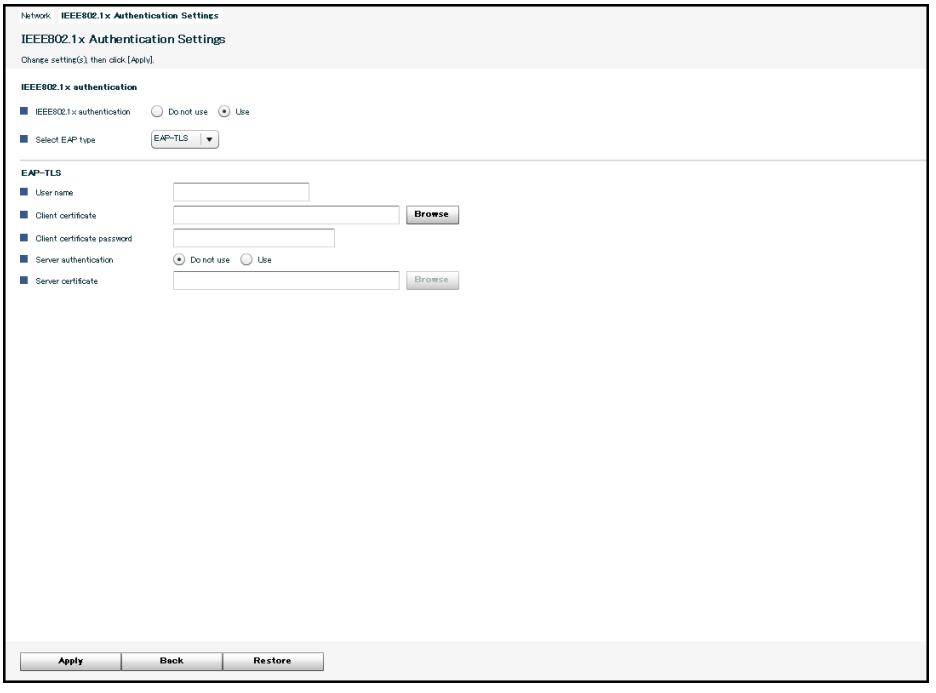
Item	Description
IEEE802.1x authentication	To change IEEE802.1x authentication settings, click [Set] to display the setting screen.

Maintenance Port

Item	Description
IP address	An IP address for the PC port (maintenance port). If you cannot use 192.168.10.1 for the PC port in your environment, contact your service representative.
MAC address	A MAC address for the PC port.
Subnet mask	A subnet mask for the PC port.

IEEE802.1x Authentication Settings

You can specify whether to use IEEE802.1x user authentication. To display the settings screen, click [RC Gate Settings] - [Network], and then [Use] in "IEEE802.1x authentication".



IEEE802.1x authentication

Item	Description
IEEE802.1x authentication	Set whether to enable IEEE802.1x authentication.
Select EAP type	Select the authentication type.

EAP-TLS

Item	Description
User name	The login user name for the authentication server.
Domain name	The login domain name for the authentication server.
Client certificate	Enter the certificate password or click [Browse] to select the certificate.
Client certificate password	Enter the password required on server authentication. This is displayed only when the authentication is enabled.
Server authentication	Set whether to enable the server authentication that uses route certificate. This is displayed only when the authentication is enabled.

Item	Description
Server certificate	Enter the certificate password or click [Browse] to select the certificate. This is displayed only when the authentication is enabled.

PEAP

Item	Description
User name	The login user name for the authentication server.
Domain name	The login domain name for the authentication server.
Tunneling user name	Set the user name for the tunneling authentication. This is displayed only when the authentication is enabled.
Tunneling password	To use IEEE802.1x authentication, enter the certificate password. This is displayed only when the authentication is enabled.
Server authentication	Set whether to enable the server authentication that uses route certificate. This is displayed only when the authentication is enabled.
Server certificate	Enter the certificate password or click [Browse] to select the certificate. This is displayed only when the authentication is enabled.

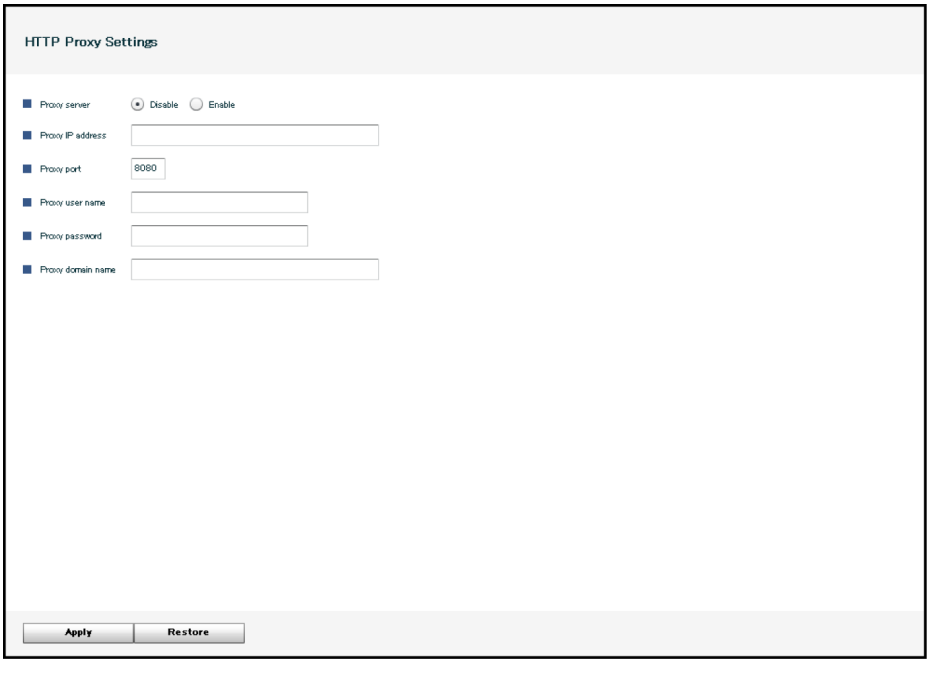
EAP-TTLS

Item	Description
User name	The login user name for the authentication server.
Domain name	The login domain name for the authentication server.
Tunneling method	Set the tunneling method.
Tunneling user name	Set the user name for the tunneling authentication. This is displayed only when the authentication is enabled.
Tunneling password	To use IEEE802.1x authentication, enter the certificate password. This is displayed only when the authentication is enabled.

Item	Description
Server authentication	Set whether to enable the server authentication that uses route certificate. This is displayed only when the authentication is enabled.
Server certificate	Enter the certificate password or click [Browse] to select the certificate. This is displayed only when the authentication is enabled.

HTTP Proxy

You can specify whether to use the HTTP proxy for communication between the RC Gate and Communication Server. To display the settings screen, click [RC Gate Settings] - [HTTP Proxy].



Item	Description
Proxy server	Select whether to enable the HTTP proxy. Set the items below when [Enable] is selected. If [Disable] is selected, setting the items below is not required.

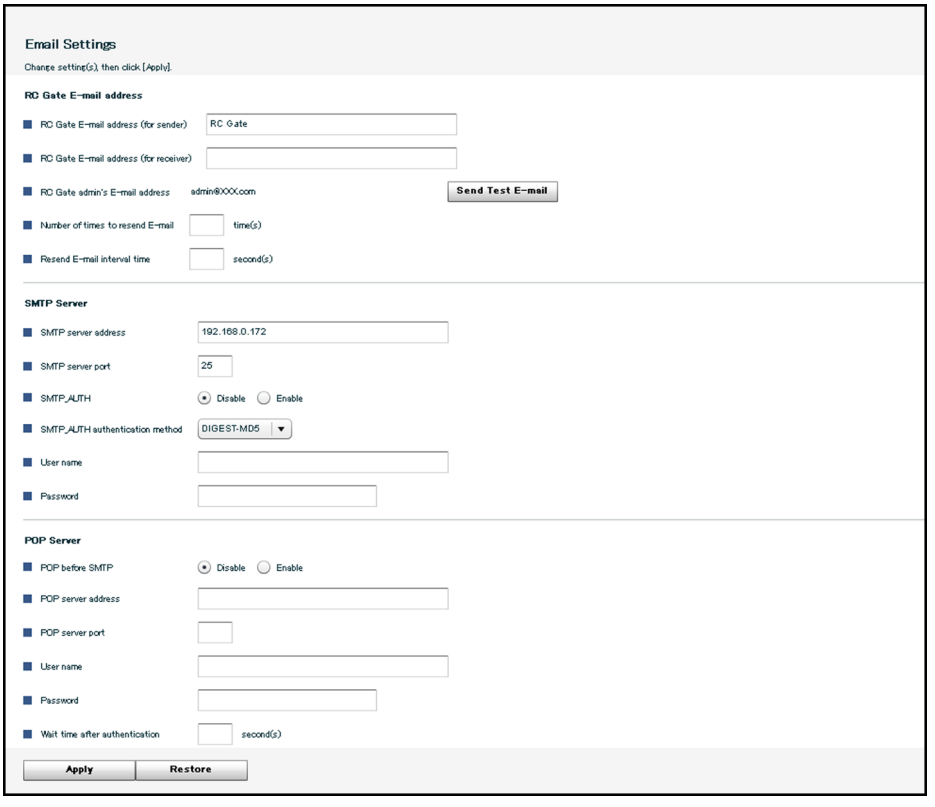
Item	Description
Proxy IP address	Enter the HTTP proxy server name in "x.x.x.x" format ("x" stands for a number from 0 to 255) format. To specify the HTTP proxy server by the domain name, make DNS server settings explained on page 86 "Network".
Proxy port	Enter the port number of the HTTP proxy. The default setting is 8080.
Proxy user name	Enter the user name for the HTTP proxy authentication within 30 characters (ASCII character).
Proxy password	Enter the password for the HTTP proxy authentication within 30 characters (ASCII character).
Proxy domain name	Enter the proxy domain name within 255 characters (ASCII character) to use the Windows authentication (NTLMv2 authentication only).

E-mail

You can change and confirm the e-mail settings for the RC Gate. To display the settings screen, click [RC Gate Settings] - [E-mail].

Important

- **E-mail for the administrator is sent in plain text.**



RC Gate E-mail address

Item	Description
RC Gate E-mail address (for sender)	An e-mail address for the RC Gate that is used to send the following types of e-mail: • Communication suspend/recovery notice • Device suspend notice • Device firmware update notice Default: rc_gate Enter the e-mail address within 126 characters (ASCII character).
RC Gate E-mail address (for receiver)	An e-mail address to send a reply e-mail to the RC Gate. You can set a different e-mail address from the RC Gate e-mail address (for sender). You can set multiple addresses by dividing each e-mail address with a comma. Enter the addresses within 255 characters (ASCII character).

Item	Description
Send Test E-mail (button)	Send a test e-mail to check the settings. The RC Gate will send a test e-mail to [RC Gate admin's E-mail address] when you click this button. This button will not be displayed until the RC Gate setting is completed.
RC Gate admin's E-mail address	An e-mail address of the administrator that receives e-mail messages such as "communication suspend notice" and "communication recovery notice". This item will not be displayed until the RC Gate setting is completed.
Number of times to resend E-mail	Set the number of retries to the SMTP server when an e-mail transmission fails. Set the item from 1 to 10.
Resend E-mail interval time	Set the period of retries to the SMTP server when an e-mail transmission fails. Set the item from 1 to 60 seconds.

SMTP Server

Item	Description
SMTP server address	Specify the IP address for the SMTP server to send the following e-mails to the administrator: • Communication suspend/recovery • Device suspend • Device firmware update To specify using the IP address: Enter the address in "x.x.x.x" format ("x" stands for a number from 0 to 255) format. To specify using the domain name: Make DNS server settings explained on page 86 "Network".
SMTP server port	A port number for the SMTP server. Generally, set the item to 25.
SMTP_AUTH	Select [Enable] if your SMTP Server uses the SMTP authentication. Select [Disable] if your SMTP does not use the SMTP authentication or uses the POP before SMTP authentication.

Item	Description
SMTP_AUTH authentication method	Set the item when "SMTP_AUTH" is set to [Enable]. Select the item from [Auto], [DIGEST-MD5], [CRAM-MD5], [LOGIN] and [PLAIN].
User name	The user name (user ID) used for the SMTP_AUTH authentication. Generally, the same e-mail address as [RC Gate E-mail address (for sender)] is applied, but it may differ for security reasons.
Password	A password for [User name] used for the SMTP_AUTH authentication. Generally, the same password as [RC Gate E-mail address (for sender)] is applied, but it may differ for security reasons.

POP Server

Item	Description
POP before SMTP	Select [Enable] if your SMTP uses the POP before SMTP authentication. Select [Disable] if your server does not use the SMTP authentication or uses the SMTP_AUTH authentication.
POP server address	The IP address or the name of the POP server for using the "POP before SMTP" authentication.
POP server port	The number of the POP server port for using the "POP before SMTP" authentication. Generally, set the item to 110.
User name	The user name (user ID) used for the POP before SMTP authentication.
Password	The password used for the POP before SMTP authentication.
Wait time after authentication	Set the wait time longer if an error occurs with the POP before SMTP authentication. Set the time between 0 to 30 seconds.

Note

- For details about the types of e-mails that are sent to the administrator, see "Setup Guide".

Checking the Settings with the Test E-mail

Follow the following procedure to check that an e-mail can be sent without an error.

Before setting the items, contact the network administrator for the authentication method of the SMTP server.

1. **Click [Send Test E-mail].**
2. **Check if the administrator has received the test e-mail.**

   If the test e-mail has been received, operate with the current settings.

   If the test e-mail has not been received, enter the e-mail address for the administrator in "RC Gate E-mail address (for sender)", and repeat steps 1 and 2.

   Ask your service representative if the e-mail has not been received even after correction of the settings.

   Note

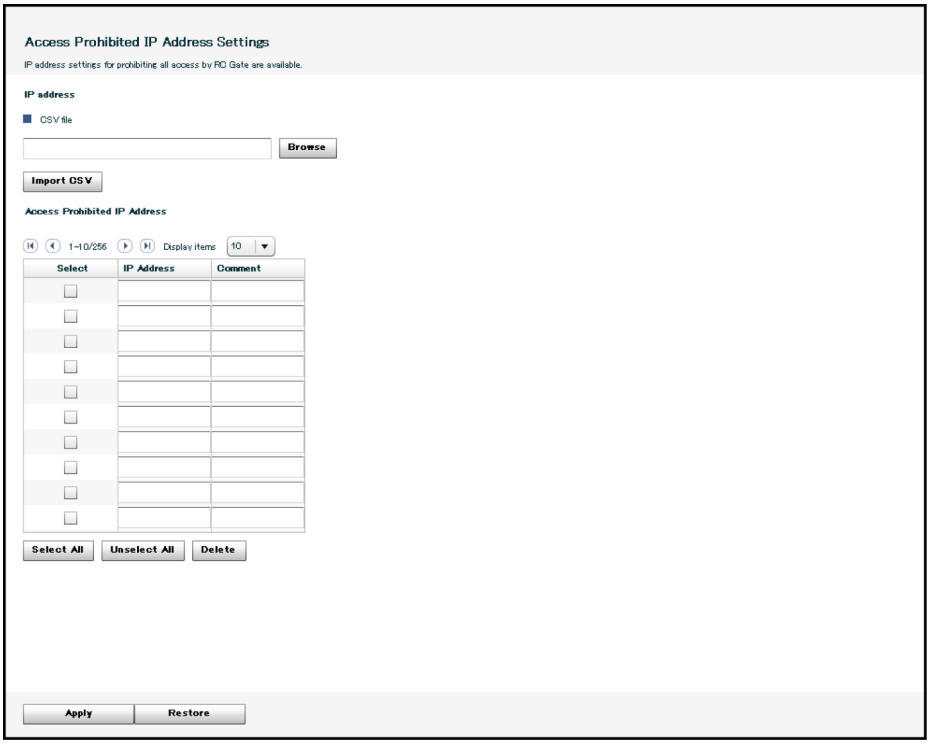
   - Make sure to enter the characters that follow "@" of the e-mail address.
   - When an error occurs with the POP before the SMTP authentication, set the [Wait time after authentication] longer.

Access Prohibited IP Address

You can prohibit certain IP addresses from being accessed by the RC Gate. To display the settings screen, click [RC Gate Settings] - [Access Prohibited IP Address].

Important

- **When using the DHCP server, the prohibited IP addresses might be assigned to the managing devices. In this case, the RC Gate cannot collect the device information.**



IP address

Item	Description
CSV file	Click [Browse] to locate the CSV file for specifying access prohibited IP addresses.
Browse (button)	Specify a CSV file location for importing.
Import CSV (button)	Start importing the specified CSV file.

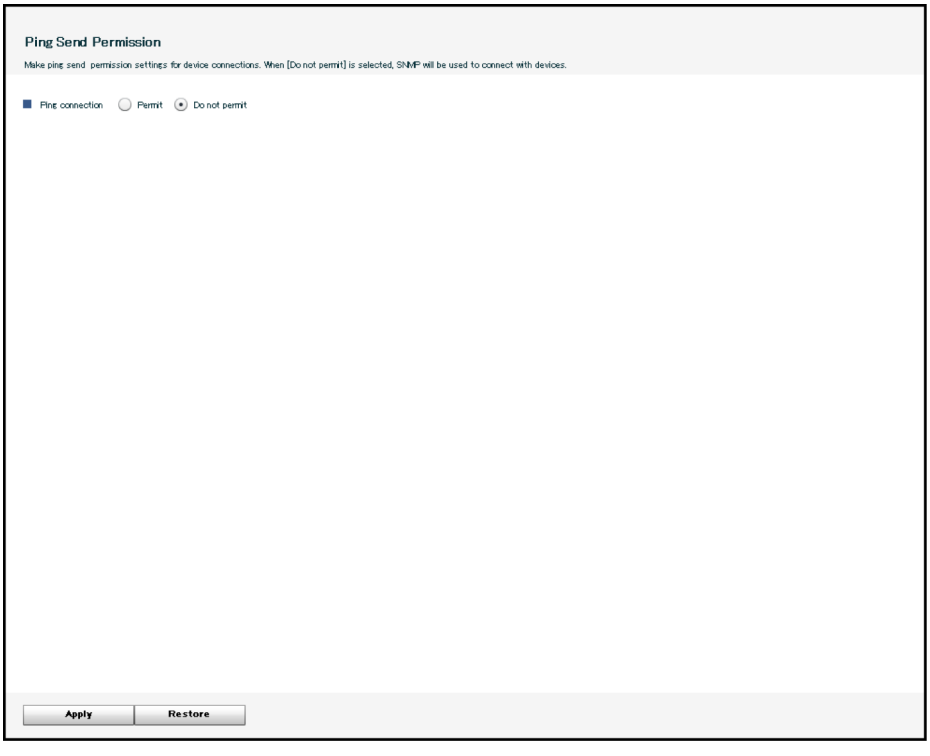
Access Prohibited IP Address

Item	Description
IP Address	Specify the IP address that you want to prohibit the RC Gate from accessing.
Comment	You can enter a comment for each IP address, using up to 61 characters (ASCII character).
Select All (button)	Select all the items in the list.
Unselect All (button)	Deselect all the selected items in the list.

Item	Description
Delete (button)	Delete all the selected items in the list.

Ping connection

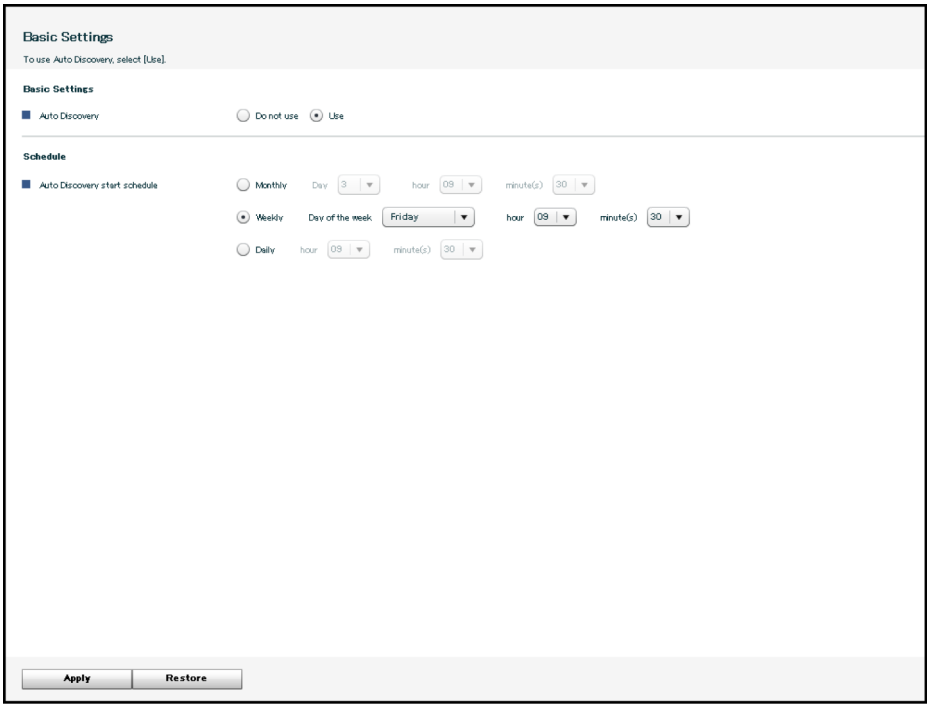
You can select whether to allow ping transmissions for device searching. To display the settings screen, click [RC Gate Settings] - [Ping connection].



tem	Description
Ping connection	Select [Do not permit] to prohibit ping transmission. When [Do not permit] is selected, SNMP will be used instead of Ping.

Auto Discovery Basic Settings

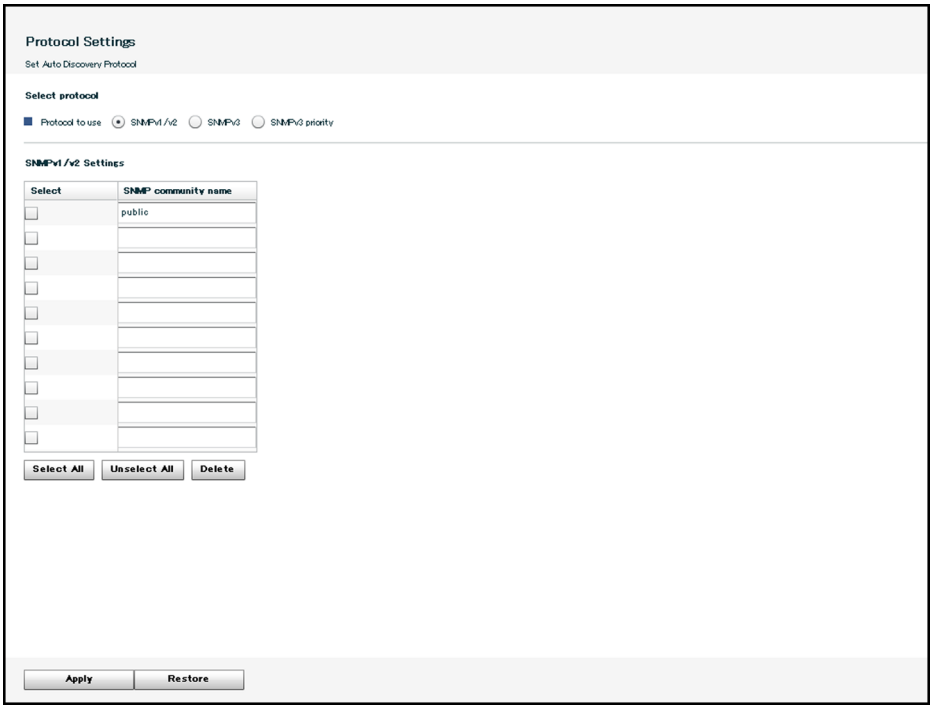
This section explains basic settings for Auto Discovery. To display the settings screen, click [Auto Discovery] - [Basic Settings].



Item	Description
Auto Discovery	Set whether to use Auto Discovery. The default setting is [Do not use].
Schedule	Set the period of time to run Auto Discovery. The default setting is [Monthly].

Auto Discovery Protocol Settings

You can make protocol information settings used for Auto Discovery. To display the settings screen, click [Auto Discovery] - [Protocol Settings].



Item	Description
SNMP protocol	Set the SNMP protocol to be enabled. The default setting is [SNMPv1,v2].
SNMP community name	Set the community name used for searching the SNMP-compatible devices. SNMP community name works as a password when the RC Gate tries to access the SNMP-compatible devices. The default setting is "public". You can enter a maximum of 30 characters (ASCII character) for each community name.
User name	The user name used for the SNMP authentication method. The item has not been set at the factory. Enter the name with ASCII characters.
Authentication password	Enter the password for the "User name" used for the SNMP authentication method. The item has not been set at the factory. Enter the password with ASCII characters.
Authentication protocol	Set the protocol used for the SNMP authentication method.

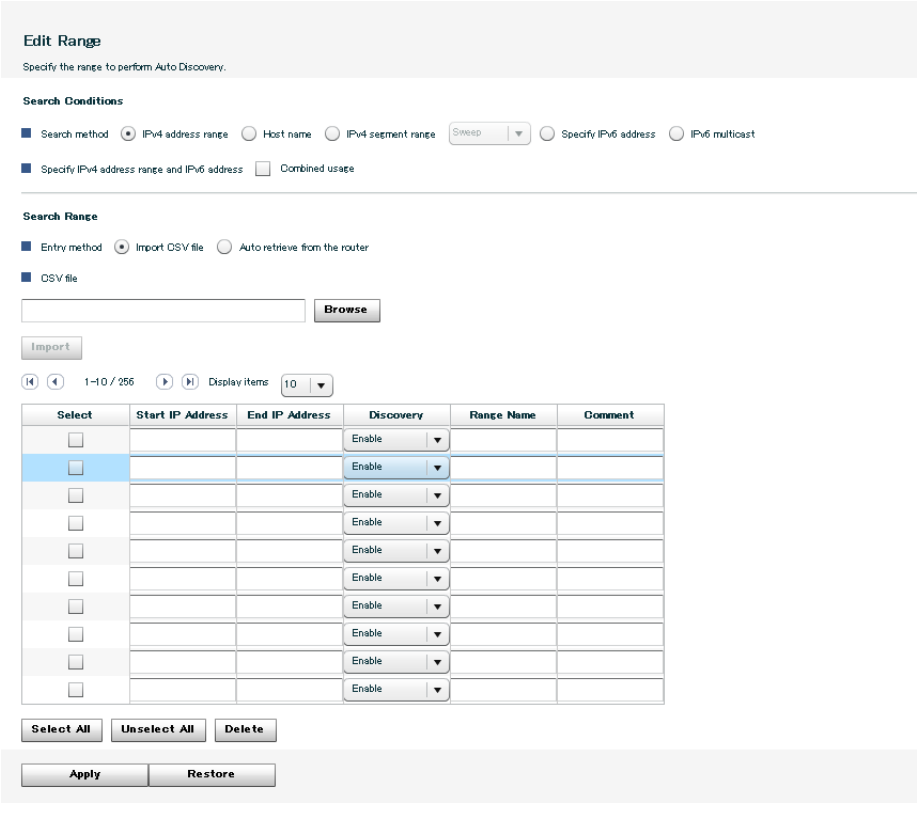
Item	Description
Encryption password	Enter the encrypted password used for the SNMP authentication method. The item has not been set at the factory. Enter the password with ASCII characters.
Encryption protocol	Set the encrypted protocol used for the SNMP authentication method.
Context Name	Set the name used for accessing the device information in SNMPv3 authentication. Set the name within 32 characters (ASCII character).

Edit Auto Discovery Range

Set the range of devices on the network to use Auto Discovery. To display the settings screen, click [Auto Discovery] - [Edit Auto Discovery Range].

Item	Description
Search method	Select [IPv4 address range], [Host name], [IPv4 segment range], [Specify IPv6 address], or [IPv6 Multicast] to specify a method for searching method. If you have specified to [IPv4 segment range], select [Sweep] or [Broadcast].
Specify IPv4 address range and IPv6 address	If you specify IPv4 address range and IPv6 address, select [Combined usage].
Entry method	If you have specified to [IPv4 address range] or [IPv4 segment range], select [Import CSV file] or [Auto retrieve from the router] to specify the entry method.
CSV file	Specify a CSV file used for setting the IP addresses.
Search hop number (0-10)	Enter the router layer to be searched (to what extent the search should be performed) when [Auto retrieve from the router] has been selected.
Go to Access Prohibited IP Address Settings (button)	Displays "Access Prohibited IP Address Settings" screen. You can set the IP addresses to prohibit the RC Gate from accessing. For details, see page 97 "Access Prohibited IP Address".

When IPv4 Address Range is Selected



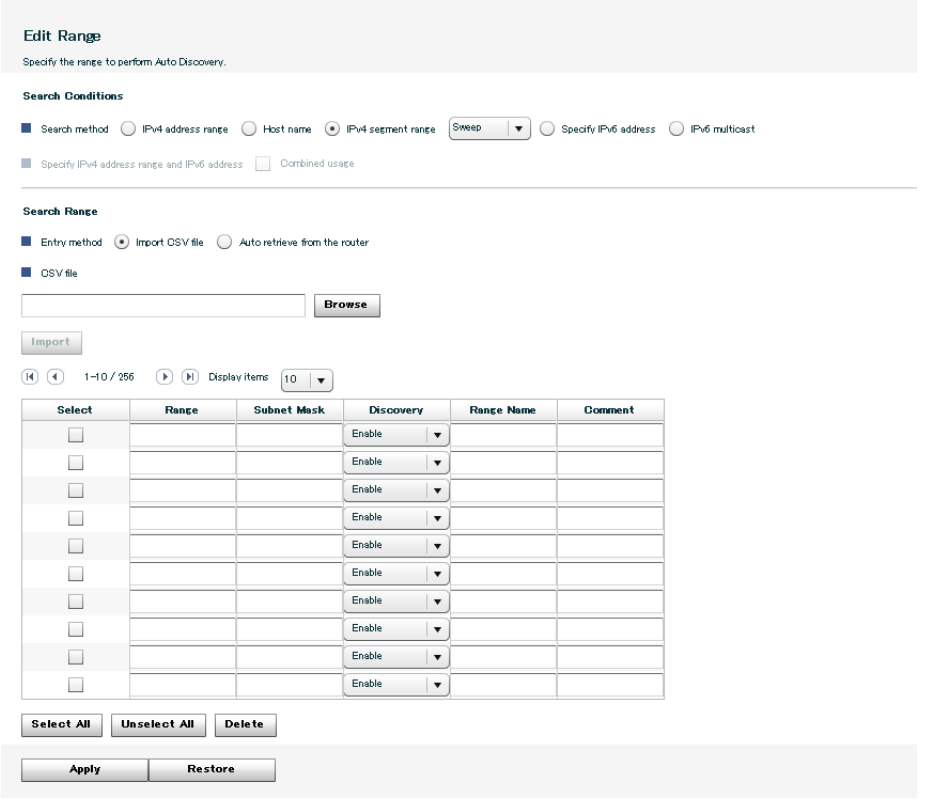
Item	Description
Start IP Address	Beginning of the IPv4 address range. Enter the IPv4 address in "x.x.x.x" format ("x" stands for a number from 0 to 255).
End IP Address	End of the IPv4 address range. Enter the IPv4 address in "x.x.x.x" format ("x" stands for a number from 0 to 255).
Discovery	Select whether or not to use the IPv4 address range for Auto Discovery.
Range Name	You can enter a name for each range, using up to 61 characters.
Comment	You can enter a comment for each range, using up to 61 characters.
Select All (button)	Select all the ranges in the list.
Unselect All (button)	Deselect all the selected items in the list.

Item	Description
Delete (button)	Delete the ranges whose check boxes are selected.

When Host name is Selected

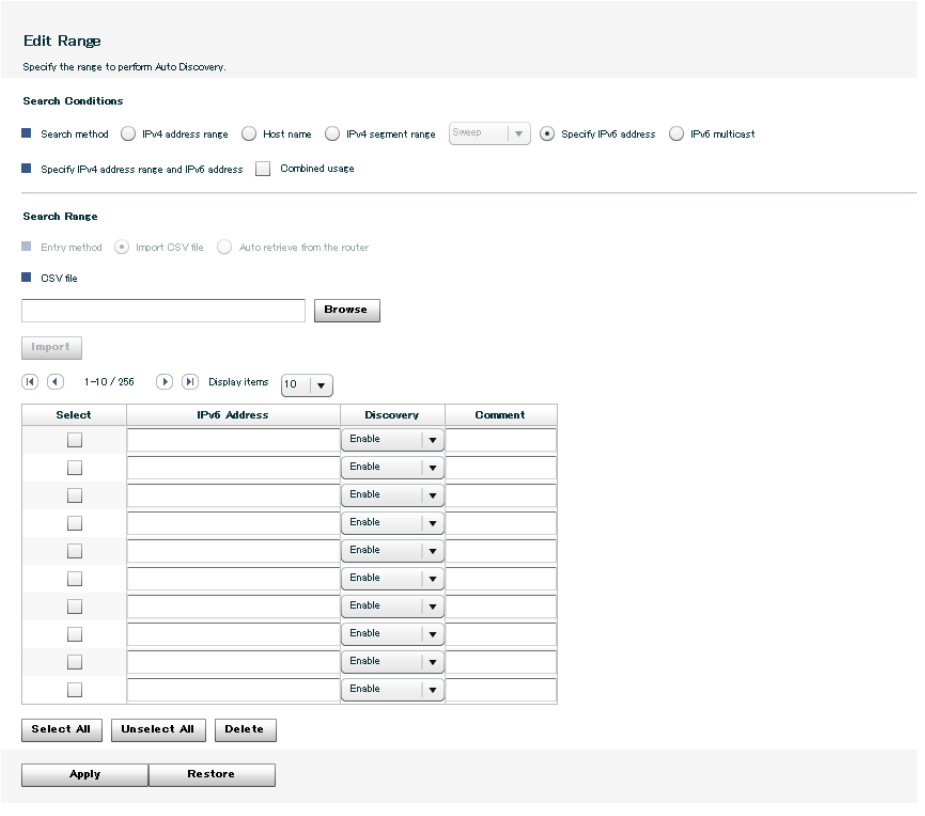
Item	Description
Host name	Enter a host name of a device to be searched for.
Discovery	Select to set Auto Discovery enable for the device or not.
Comment	Enter comments for each [Host name] within 61 characters.

When IPv4 Segment Range is Selected



Item	Description
Range	The network address to use Auto Discovery. Enter the IPv4 address in "x.x.x.x" format ("x" stands for a number from 0 to 255).
Subnet Mask	The subnet mask to determine the enable range for the "Range". Enter the subnet mask in "x.x.x.x" format ("x" stands for a number from 0 to 255).
Discovery	Select to set Auto Discovery enable for the device or not.
Range Name	The network address name entered for the IPv4 address in [Range].
Comment	Enter comments for each [Range] within 61 characters.
Select All (button)	Select the all the ranges in the list.
Unselect All (button)	Deselect the all selected items in the list.
Delete (button)	Delete the ranges whose check boxes are selected.

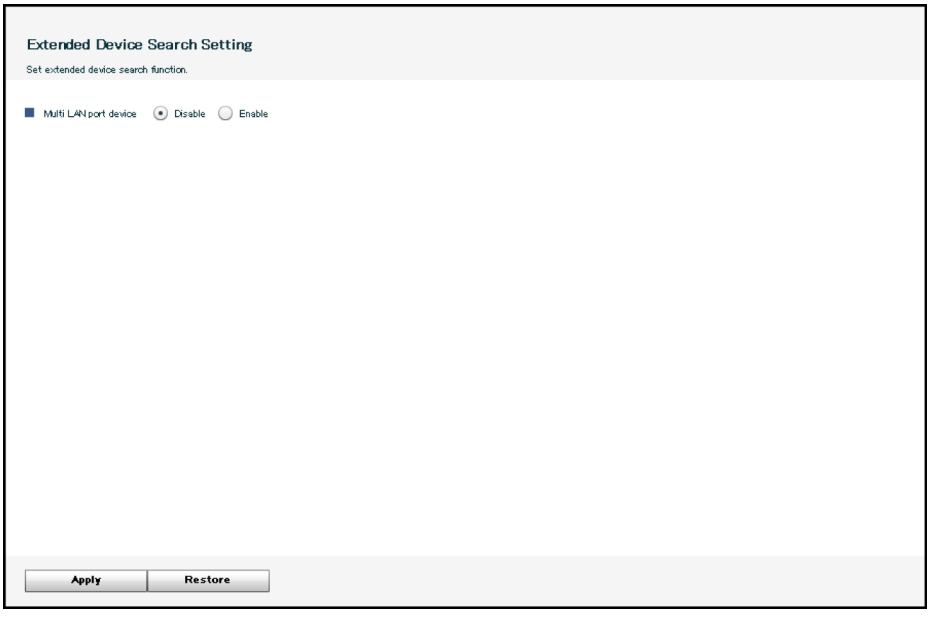
When Specify IPv6 Address is Selected



Item	Description
IPv6 address	Enter a host name of a device to be searched for.
Discovery	Select to enable Auto Discovery for the device or not.
Comment	Enter comments for each [IPv6 address] within 61 characters.

Extended Device Search Setting

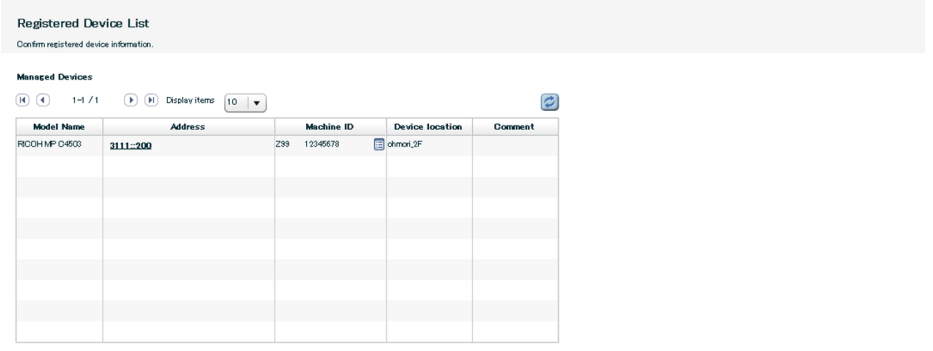
You can specify whether to extend the device search ranges. To display the screen, click [Device Management] - [Extended Device Search Setting].



Item	Description
Multi LAN port device	The following devices may not be found at searching the Auto Discovery ranges: • The device manufactured by this company with no printer application installed. • The device with multiple network interfaces. Although the above devices may be found if this item is enabled, it will take a longer time for searching. For details, contact your service representative.

Registered Device List

This is the list of devices managed by the RC Gate. To display the screen, click [Device Management] - [Registered Device List]. To display the settings screen, click [Refresh].

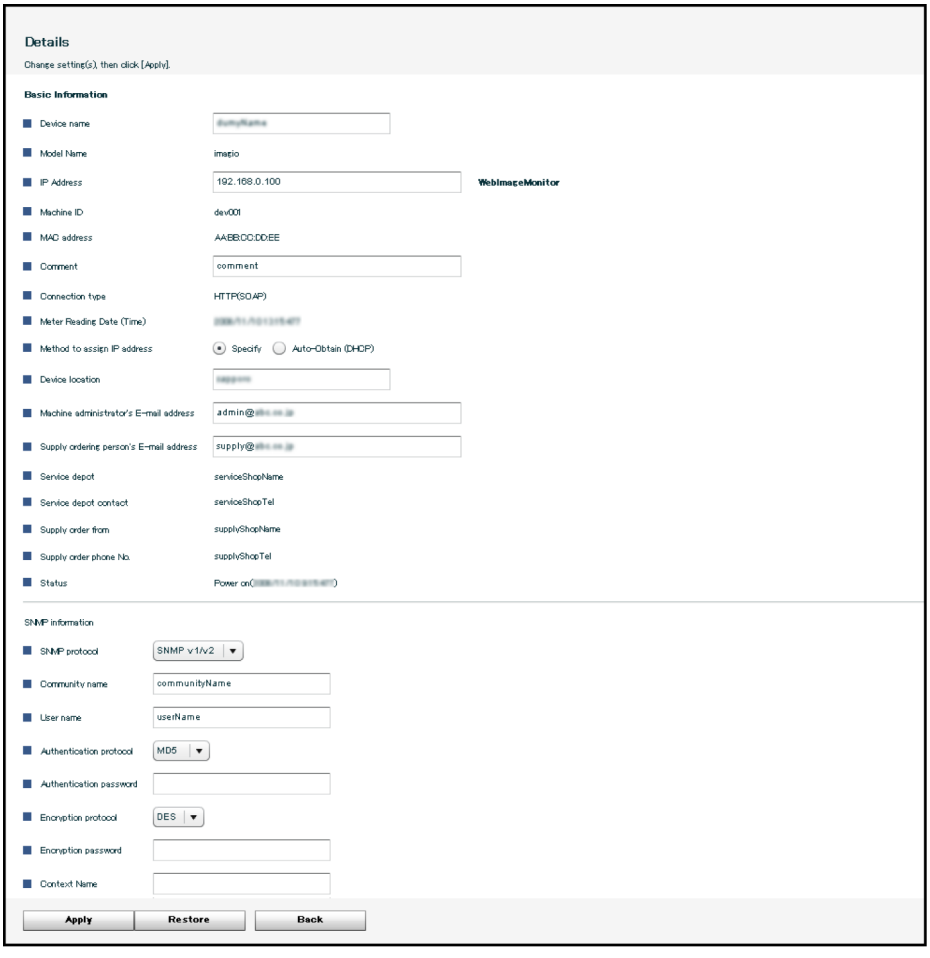


5

Item	Description
Model Name	The model name of the device. If the RC Gate could not collect the model name, the item will be indicated with "---".
IP Address	The IPv4 address, IPv6 address or host name for the device.
Machine ID	The machine ID for the device. The "Details" screen appears by clicking .
Device location	The location where the device is placed.
Comment	The device comment information.

Details

You can confirm and change the information details of devices managed by the RC Gate. To display the settings screen, click [Device Management] - [Registered Device List]. Click of the machine ID you want to confirm and change.



Item	Description
Device name	The name for the device. To change the name, enter a new name within 30 characters (ASCII characters).
Model Name	The model name of the device.
IPv4 Address	The IPv4 address of the device.
IPv6 Address	The IPv6 address of the device.
Host name	The host name of the device.
Machine ID	The machine ID of the device.
MAC address	The MAC address of the device.

Item	Description
Comment	The comment information for the device. Enter the comment within 61 characters (ASCII character).
Connection type	The connection type of the devices.
Meter Reading Date (Time)	The date and time when the RC Gate reads the counter of the device.
Method to assign IP address	The method to assign IP address for the devices on the network. Select from [Specify] and [Auto-Obtain (DHCP)].
Device location	The name of the place where the device is located. To change the name, enter a new name within 30 characters (ASCII character).
Machine administrator's E-mail address	The e-mail address for the device administrator. Notice e-mails such as "updating device firmware" and "device suspension" are sent to this address. Enter the address within 120 characters (ASCII character).
Supply ordering person's E-mail address	The e-mail address for the personnel responsible for keeping supplies. Enter the address within 120 characters (ASCII character). Depending on the area and service availability, the address might not be displayed.
Service depot	Your service representative.
Service depot contact	The phone number of your service representative.
Supply order from	Your supply representative. Depending on the area and service availability, the address might not be displayed.
Supply order phone No.	The phone number of your supply representative. Depending on the area and service availability, the address might not be displayed.
Status	Displays the operation status of the device.

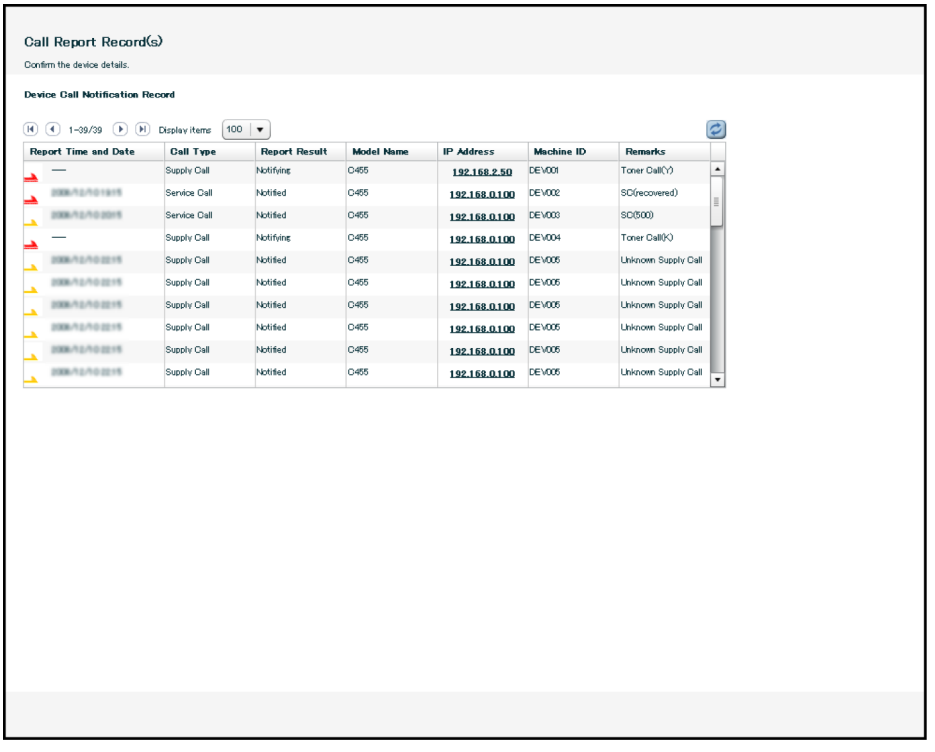
SNMP Information

Item	Description
SNMP protocol	Set the SNMP protocol version that is currently valid.

Item	Description
Community name	The community name for the SNMP-compatible devices which is obtained by the SNMP protocol. To change the name, enter a new name within 30 characters (ASCII character). The default setting is "Public".
User name	The login user name for the SNMP authentication server. To change the name, enter a new name within 32 characters (ASCII character).
Authentication protocol	Set the protocol to be used for the SNMP authentication method.
Authentication password	Enter the password for "User name" to be used for the SNMP authentication within 32 characters (ASCII character).
Encryption protocol	Set the encryption protocol to be used for the SNMP authentication method.
Encryption password	Enter the encryption password to be used for the SNMP authentication within 32 characters (ASCII character).
Context Name	Set the name used for accessing the device information in SNMPv3 authentication. Set the name within 32 characters (ASCII character).

Call Report Record(s)

Displays the date of call report, call type, and the device information on which a call has been reported. A maximum of 100 reports can be stored. To display the screen, click [Device Management] - [Registered Device List] - [Device Call Notification Record].

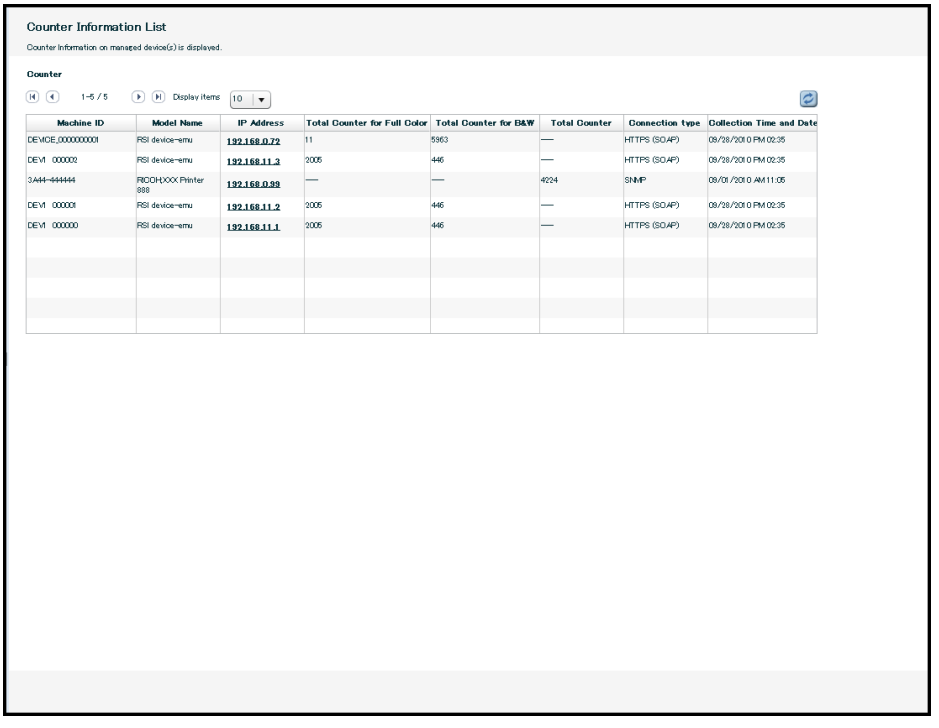


Item	Description
Report Time and Date	The time and date when a call from the device was reported to the Communication Server: • Calls reported within the last hour and calls with "Reporting..." in "Report Result" are shown in red. • Calls reported within the last 24 hours are shown in yellow.
Call Type	There are following types of call type: • Service call • Manual call • Supply call

Item	Description
Report Result	Results of the report from the Communication Server: • Succeeded • Failed • Outside of service time • Reporting failed • Reporting
Model Name	The model name of the device on which a call has been reported.
IP Address	The IP address of the device on which a call has been reported.
Machine ID	The device ID on which a call has been reported.
Remarks	Detailed information such as the service call number and supply call.

Registered Device Counter

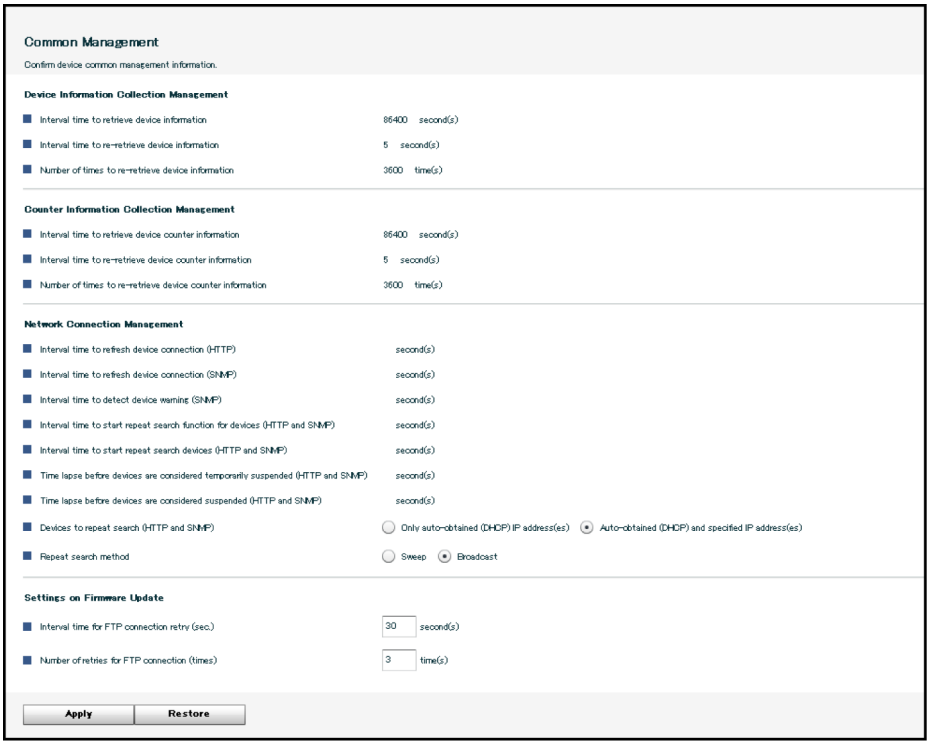
This is the list of the managed devices. You can confirm the counter information of the managed devices. To display the settings screen, click [Device Management] - [Registered Device Counter].



Item	Description
Machine ID	The machine ID for the device.
Model Name	The model name of the device. If the RC Gate could not collect the model name, it will be indicated with "---".
IP Address	The IP address for the device.
Total Counter for Full Color	Displays the total counter of full color.
Total Counter for B&W	Displays the total counter of monochrome.
Total Counter	Displays the total counter of the managed device.
Connection Type	Displays the connection type of the managed device.
Collection Time and Date	Displays the latest date and time when the counter information was collected.

Common Management

You can confirm the settings to manage the registered devices. To display the screen, click [Device Management] - [Common Management].



Device Information Collection Management

Item	Description
Interval time to retrieve device information	The period of time to receive the information from devices.
Interval time to re-retrieve device information	The period of time to retry when the RC Gate could not receive information from devices.
Number of times to re-retrieve device information	The number of times to retry when the RC Gate could not receive information from devices.

Counter Information Collection Management

Item	Description
Interval time to retrieve device counter information	The period of time to receive counter data from devices.
Interval time to re-retrieve device counter information	The period of time to retry when the RC Gate could not receive counter information from devices.

Item	Description
Number of times to re-retrieve device counter information	The number of times to retry when the RC Gate could not receive counter information from devices.

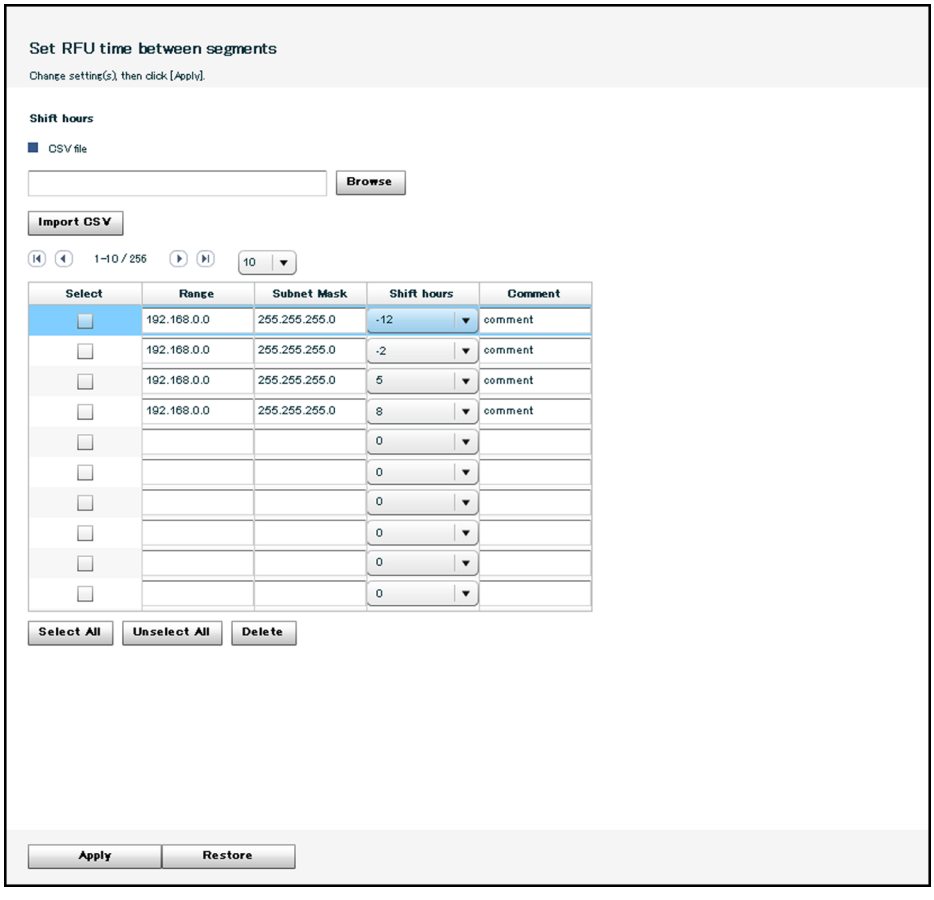
Network Connection Management

Item	Description
Interval time to refresh device connection (HTTP)	The period of time to check the connection to HTTPS-compatible devices communicated with HTTP protocol.
Interval time to refresh device connection (SNMP)	The period of time to check the connection to SNMP-compatible devices communicated with SNMP protocol.
Interval time to detect device warning (SNMP)	The period of time to detect the warnings from SNMP-compatible devices communicated with SNMP protocol.
Interval time to start repeat search function for devices (HTTP and SNMP)	The period of time to start searching again for lost devices connected to the network.
Interval time to start repeat search devices (HTTP and SNMP)	The period of time to start searching again for lost devices connected to the network.
Time lapse before devices are considered temporarily suspended (HTTP and SNMP)	The period of time to decide on lost devices connected to the network being temporarily suspended.
Time lapse before devices are considered suspended (HTTP and SNMP)	The period of time to decide on lost devices connected to the network being suspended.
Devices to repeat search (HTTP and SNMP)	Select the target device on the network on which to repeat searching from [Only auto-obtained (DHCP) IP address(es)] and[Auto-obtained (DHCP) and specified IP address(es)].
Repeat search method	Displays the method for repeat searching when the device on a network has been lost.

Shift Device Firmware Update Time

Considering time zone or work starting time difference, you can set time at which device firmware update is performed by network segment. To display the settings screen, click [Device Management] – [Shift Device Firmware Update Time]. A maximum of 255 segments can be set.

You can import the segment information from a CSV file stored on your computer. To create a CSV file, enter the network address, subnet mask, shift time (hour), and comment by separating them with a comma.



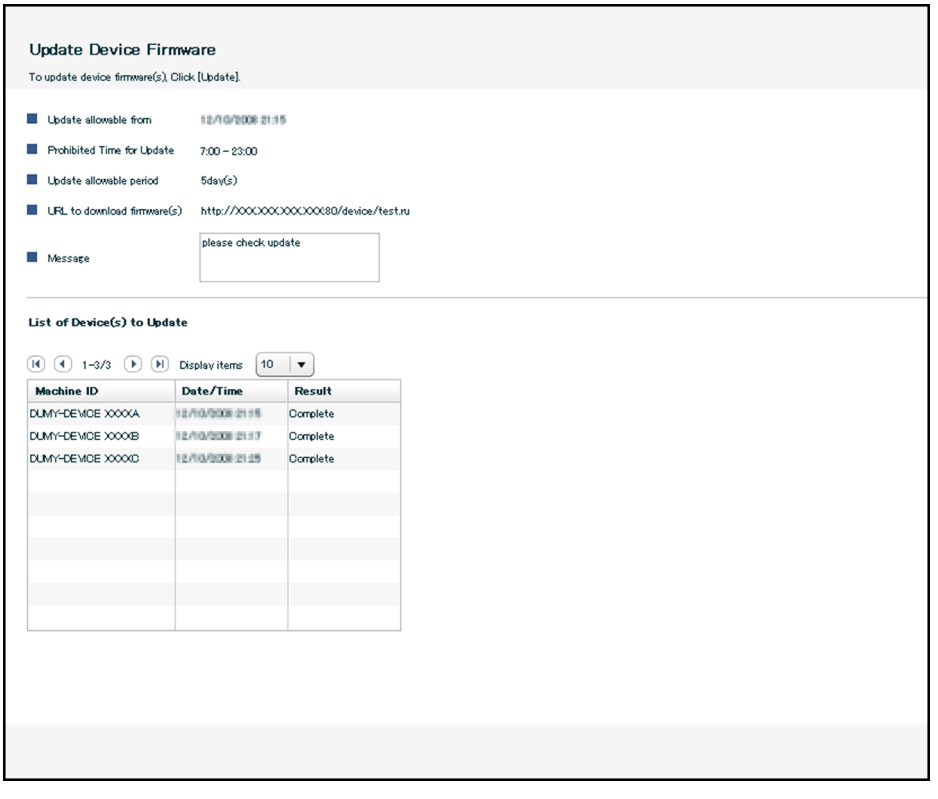
Item	Description
CSV file	Specify a CSV file for importing.
Browse (button)	Specify a CSV file location for importing.
Import CSV	Start importing the specified CSV file.
Range	Set the network address of the segment for which firmware update time will be changed.
Subnet Mask	Set the subnet mask of the segment for which firmware update time will be changed.

Item	Description
Shift hours	Set the shift time for firmware update. You can set between -12 and 12 hours on an hour to hour basis.
Comment	Set the device comment information. You can enter a maximum of 61 characters (ASCII character).
Select All (button)	Select the all the items in the list.
Unselect All (button)	Deselect all the selected items in the list.
Delete (button)	Delete the segment specified by "Select" box.

Update Device Firmware

You can update the device firmware and display the update schedule. To display the settings screen, click [Device Management] - [Update Device Firmware].

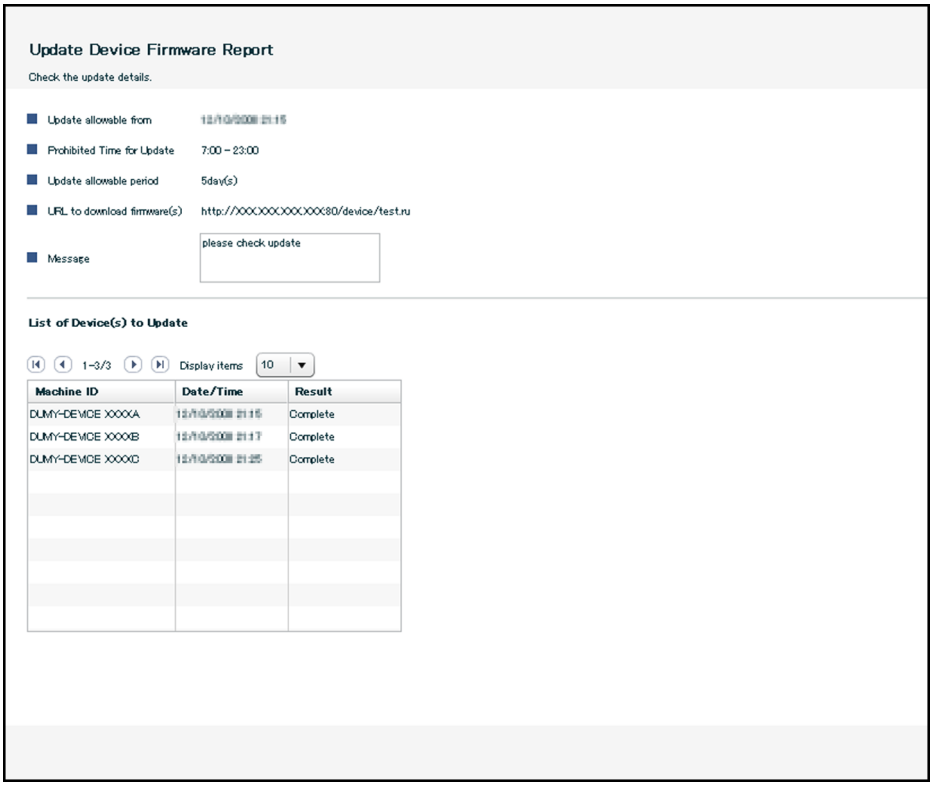
When the administrator receives "<<<Remote Communication Gate A>>> [[[Notice: Update Device Firmware]]]" e-mail and clicks a URL link, the RC Gate monitor starts up, and this screen appears immediately after login.



Item	Description
Update (button)	Execute firmware update. The button will not appear when there is no update schedule, the schedule update is running, or before the update is scheduled.
List of Device(s) to Update (button)	Display the following items: • ID of the device for which update is possible • Update state such as preparing to update/preparing completed • Update time (when update has been completed) • Update results The button will not appear if there is no updating schedule.
Update allowable from	The date and time when the device will be able to update.
Prohibited Time for Update	The period of time when the firmware update will be prohibited.
Update allowable period	The period of time when the firmware can be updated, starting from the first day when the firmware is able to update. If the update is not executed in this period, it will be considered that the update has failed.
URL to download firmware(s)	The location where the firmware is downloaded from.
Message	The message from the Communication Server.

Update Device Firmware Report

You can confirm the result of previous device firmware update. To display the screen, click [Device Management] - [Update Device Firmware Report].



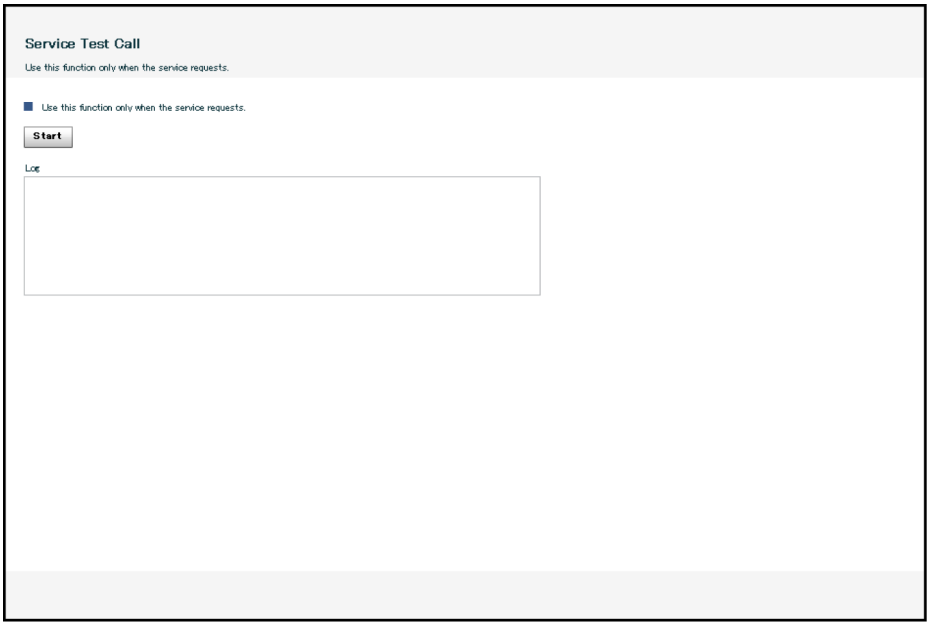
Item	Description
Update allowable from	The starting date when the device firmware can be updated.
Prohibited Time for Update	The period of time when the firmware update will be prohibited.
Update allowable period	The available period of time when the device firmware can be updated.
URL to download firmware(s)	The location where the firmware is downloaded from.
Message	The message from the Communication Server.

Service Test Call

You can test the connection between the RC Gate and Communication Server. To display the settings screen, click [Maintenance] - [Service Test Call].

Important

- **Execute [Service Test Call] only when there is a request from your service representative.**



Item	Description
Start (button)	Start a test call to the Communication Server.
Log	Displays the status message from the Communication Server for the results of the test call.

Note

- The results of [Service Test Call] (The contents of [Log]) will not be sent to the Communication Server. This is a communication test only for the RC Gate.

Device Check Request Call

You can test the connection between the RC Gate and Communication Server. The result will be sent to the Communication Server. To display the settings screen, click [Maintenance] - [Device Check Req. Call].

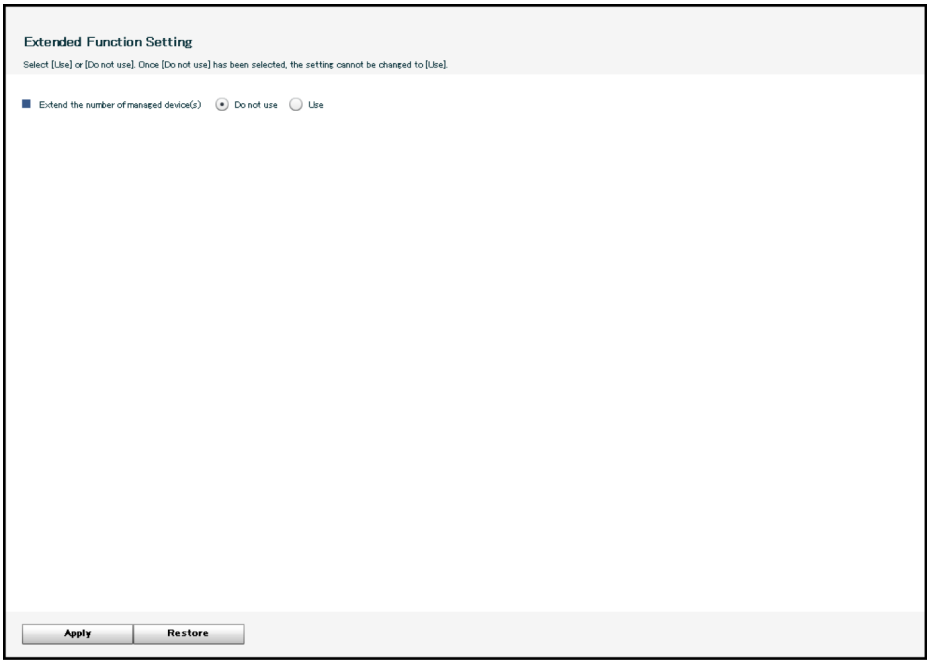
Important

- **Click [Start] only when there is a request from your service representative.**
- **When you make a test call by clicking [Start], the status of the RC Gate will be sent to the Communication Server.**

Item	Description
Start (button)	Start a test call to the Communication Server.

Extended Function Setting

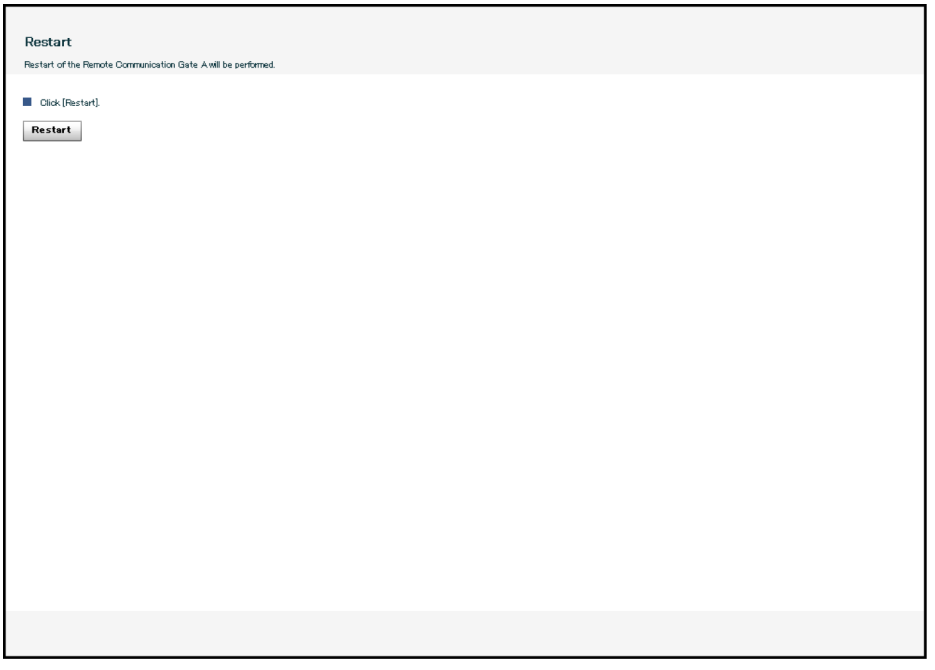
You can increase the number of registerable device from 100 to 1,000. To display the settings screen, click [Maintenance] - [Extended Function Setting]. This item is displayed after the optional memory and storage are installed.



Item	Description
Extend the number of managed device(s)	Set whether to increase the number of registerable devices. To increase the number, select [Use] and restart the RC Gate. Once [Use] has been selected, the setting cannot be reverted to [Do not use]. To reset to [Do not use], contact your service representative.

Restart RC Gate

You can reboot the RC Gate during operation. To display the screen, click [Maintenance] - [Restart RC Gate].



Item	Description
Restart (button)	Reboot the RC Gate. It will take a few minutes to complete. Before restarting your operation, confirm that the green LED on the RC Gate is lit.

Shut Down RC Gate

This section explains the items for shutting down the RC Gate. To display the screen, click [Maintenance] - [Shut Down RC Gate].

Important

- **If the power plug is disconnected before shutting down the RC Gate, the memory/storage will be damaged. In such a case, the latest logs, a maximum of an hour, will be lost. Be sure to shut down the RC Gate before disconnecting the power plug.**

Item	Description
Shut Down (button)	Shut down the RC Gate.
Shut Down (dialog box)	This is displayed by clicking the [Shut Down] button. Click [OK] to start shutting down. Then [Shutting down RC Gate...] screen will appear. Before you turn off the RC Gate, confirm that the orange LED stopped flashing, and the green and orange LEDs are lit.

Note

- You can shut down the RC Gate by using the Shutdown button on the front of this equipment. This equipment is shut down by pressing and holding the button for five or more seconds.

Service Call

You can confirm the error codes and other information with this screen. To display the screen, click [Maintenance] - [Service Call]. Also, the screen will be automatically displayed when an error occurs on operating [RC Gate Configuration]. When an error message appears on operating the RC Gate Monitor, click [Back] to display this screen.

Item	Description
(The Status of the RC Gate)	If the error occurs with the RC Gate, "Error(s) have occurred." is displayed. During a normal operation, "No error has occurred." is displayed, and the items below will not be displayed.
SC code	Error codes for the RC Gate.
Detail code	The service call type by code.
Occurrence date/time	The date and time when the error has occurred.
Communication Server notification	The status of the notification to the Communication Server: • Unnecessary • Notifying • Notified • Failed
Service depot	Your service representative.
Service depot contact	The phone number of the service depot.

Note

- If an error occurs, see page 143 "Troubleshooting".

System Status

You can confirm the system status of the RC Gate. To display the screen, click [Maintenance] - [System Status]. The connection suspension e-mail will be sent to the administrator when the RC Gate is suspended. Also, click hyperlink to the URL in the e-mail which is sent to device administrator. The login page for the RC Gate Monitor will appear and the screen will appear immediately after the login page.

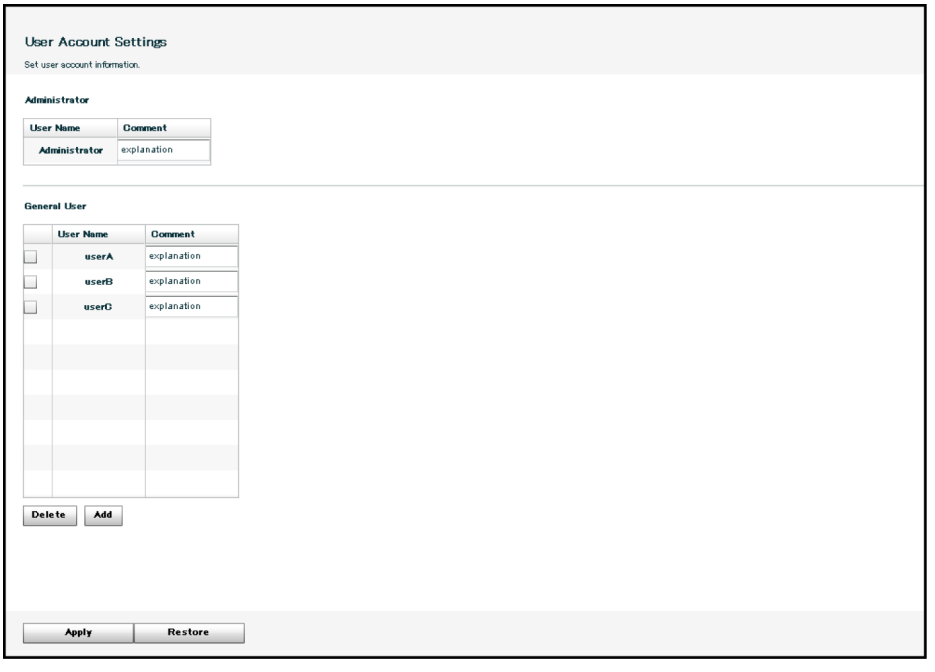
Item	Description
(Status of the RC Gate)	Displays if the RC Gate is in operation or in suspension. If the RC Gate is operating normally, the items below will not be displayed.
Reason	The major reason of suspension and action.
Date/Time of suspension	The date and time when the suspension has occurred.

Note

- When the system has suspended, check the following:
  - The proxy settings, such as the password, have not changed.
  - The Ethernet cable of the RC Gate has not been pulled out.
  - The network devices, such as the power of a hub, are not off.
- If the items above have no problem, contact your service representative.

User Account Settings

You can check the list of user accounts that can access the Web user interface of the RC Gate. To display the screen, click [Security] - [User Account Settings].



Administrator

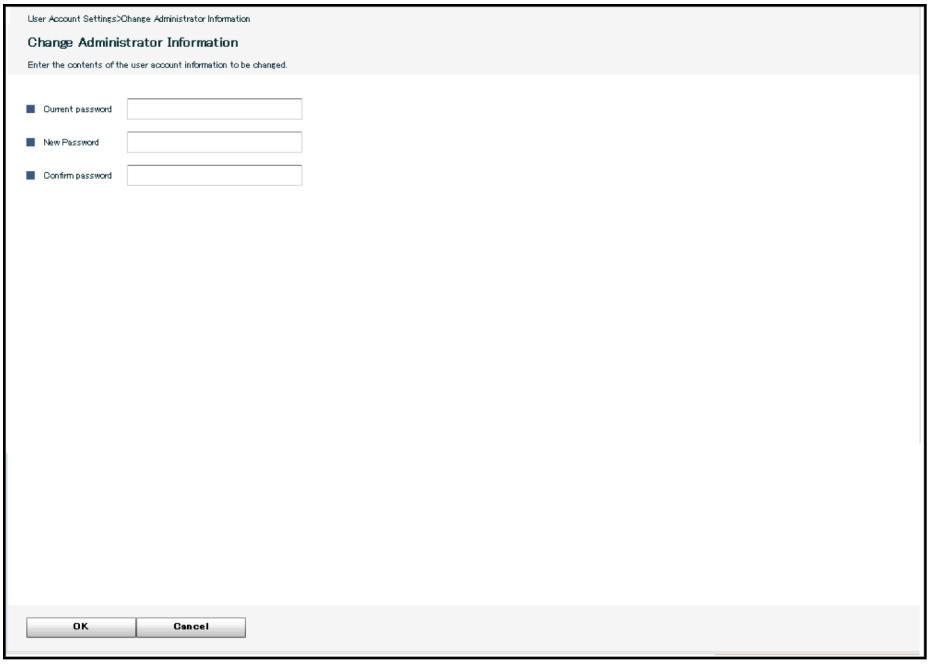
Item	Description
User Name	Click the user name to change the password for the administrator.
Comment	Comments about the user.

General User

Item	Description
User Name	Click the user name to change the password for the user.
Comment	Comments about the user.
Delete (button)	Delete the login user name for general user.
Add (button)	Displays "Add General User" screen. A maximum of 10 users can be registered.

Password

You can change the RC Gate Monitor login password. To display the settings screen, click [Security] - [User Account Settings] - [Change password], then click the applicable user name.



Important

- Specify a user name using 1 to 13 characters (ASCII character).
- Only the following ASCII characters (alphanumeric, (space), '-', or '_') can be used for the user name: space - 0 1 2 3 4 5 6 7 8 9 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 _ 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
- Characters other than those listed above cannot be used for the user name.
- Never use the default password. Specify a new password using 8 to 13 characters (ASCII character).
- You can use the following ASCII characters for password: space ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ 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 [\ ] ^ _ ` 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 { | } ~
- If the error message "The following item(s) are invalid. Click [OK] to return to the previous screen, then specify correctly." appears, make sure that the user name and the password are made up of valid characters and numerals, and that each contains a valid number of characters and numerals.
- Change the passwords for the administrator and general users at intervals of 6 months or less.
- Avoid using well known words or phrases, or repeated characters that can easily be guessed.
- Do not leave passwords written where they can be seen.

Note

- New passwords become valid at next login.

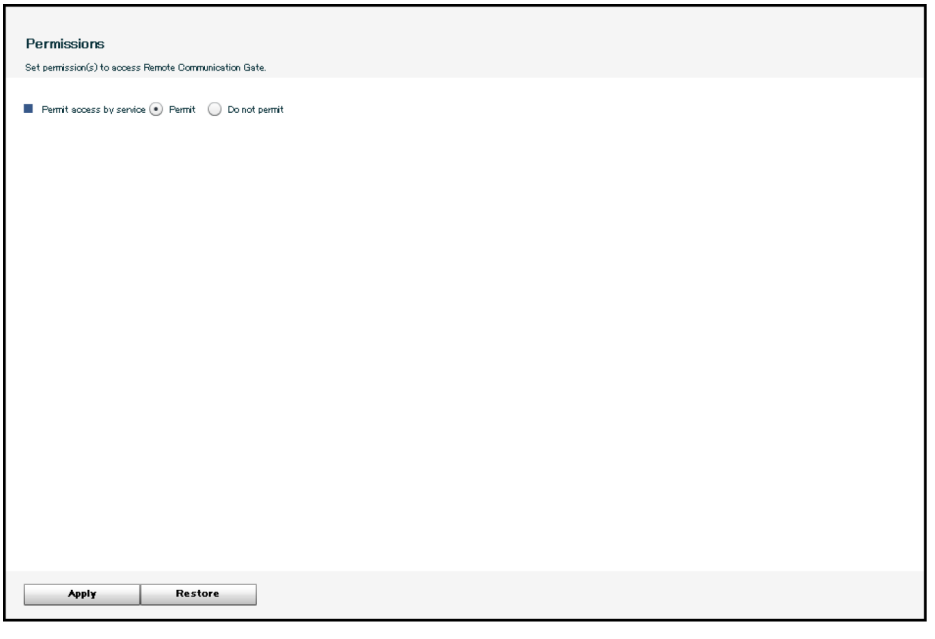
Item	Description
Current password	Enter the current password.
New Password	Enter the new password.
Confirm password	Enter the new password again to avoid typing error.

Permissions

You can permit or deny service access by the customer engineer and firmware updates from the Communication Sever. To display the screen, click [Security] - [Permissions].

Important

- **You can permit or deny the customer engineer's inspection and repair access to the RC Gate. If you select [Do not permit], customer engineer access is denied until the administrator sets [Permit access by service] to [Permit]. If you deny service access, the RC Gate may not be properly serviced. On the other hand, if you select [Permit], the RC Gate will be open to impersonation attacks. For safer management, we recommend you normally keep [Do not permit] active and switch to [Permit] only when you need an inspection or repairs. For maintenance, contact a maintenance-specialist customer engineer.**



Item	Description
Permit access by service	Select [Do not permit] to deny service access to the RC Gate. Select [Permit] to permit service access.

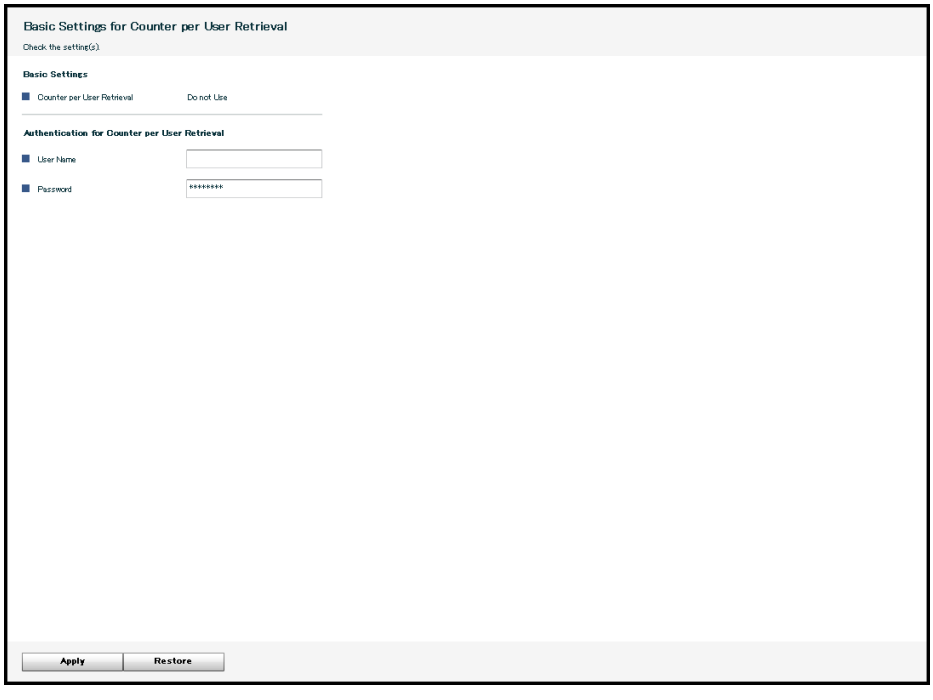
Basic Settings for Counter per User Retrieval

The counter information can be acquired and processed on a per-user basis for devices specified by the Communication Server. To display the screen, click [Counter per User] - [Basic Settings for Counter per User Retrieval].

This function becomes available under the following two conditions:

- Optional memory has been expanded.
- Application version is 2.05 or later.

Communication data sent between the devices and the RC Gate when acquiring a per-user counter is not encrypted.



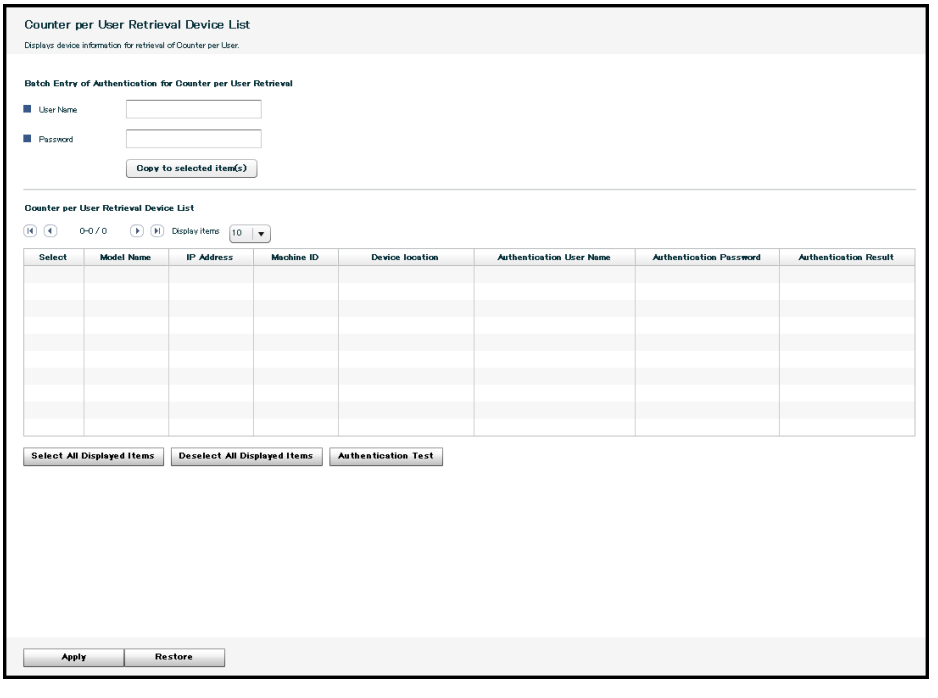
Item	Description
Counter per User Retrieval	Shows whether the counter per user retrieval function works properly.

Item	Description
User name	Enter the machine administrator's user name used for authentication when you access a device to acquire a per-user counter.
password	Enter the machine administrator's password used for authentication when you access a device to acquire a per-user counter.

To acquire a per-user counter, the device administrator's user name and password must be entered. However, if you are using this machine as a CC certified product, do not enter the device administrator's user name and password.

Counter per User Retrieval Device List

Displays a list of devices from which to obtain the information needed to retrieve the counter for each user. To display this screen, Click [Counter per User] and then [Counter per User Retrieval Device List].



Item	Description
User Name	To retrieve the counter for each user, enter the user name of the device administrator used to authenticate access to the device.
Password	To retrieve the counter for each user, enter the password of the device administrator used to authenticate access to the device.
Copy to selected item(s)	Click [Copy to selected item(s)] to update the device information selected in the Device List by using the user name and password entered.
Select All Displayed Items	Click [Select All Displayed Items] to select all the items in the Device List.
Deselect All Displayed Items	Click [Deselect All Displayed Items] to deselect all the items in the Device List.
Authentication Test	Click [Authentication Test] to verify whether you can retrieve information about the counter for each user from the devices selected in the Device List. The verification results are then displayed.

Retrieval Test for Counter per User

Checks whether the per-user counter information can be obtained. To display the screen, click [Counter per User] - [Retrieval Test for Counter per User].

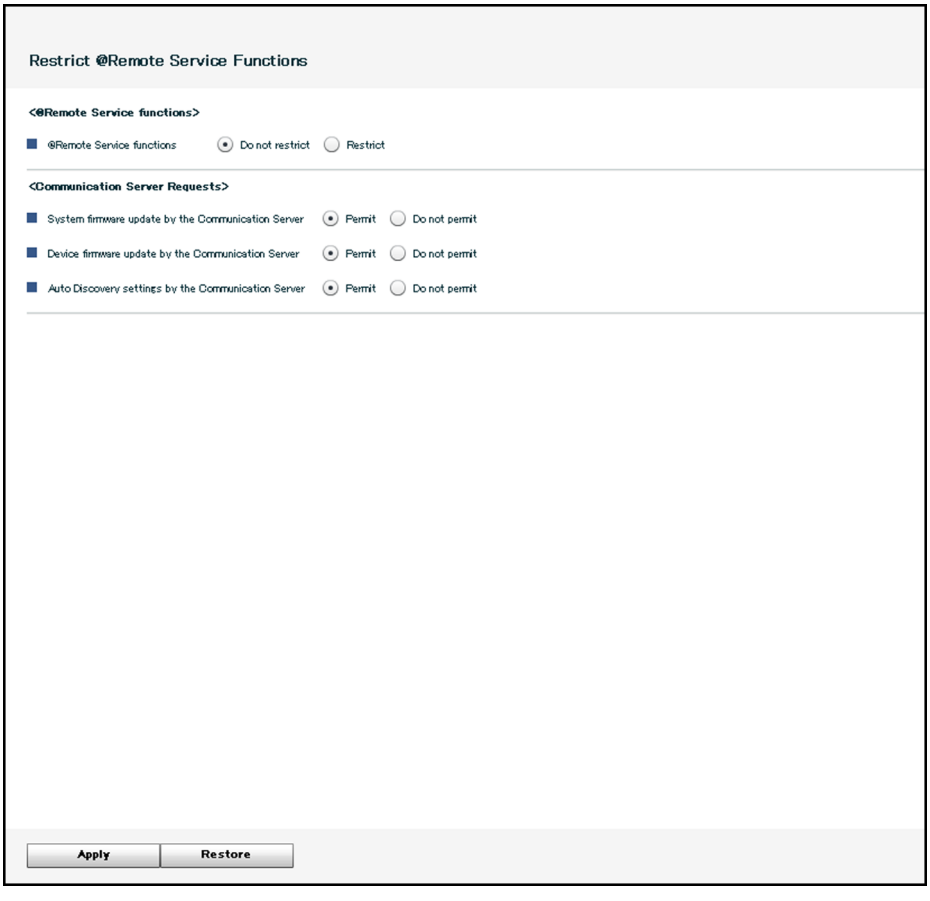
Item	Description
IP Address	Enter the IP address of the device used to determine whether the counter for each user can be retrieved.
User Name	To retrieve the counter for each user, enter the user name of the device administrator used to authenticate access to the device.
Password	To retrieve the counter for each user, enter the password of the device administrator used to authenticate access to the device.
Retrieval Test	Click [Retrieval Test] to display the test results.
Result	Shows whether the counter per user information has been retrieved successfully.
Machine ID	Displays the ID of the device used to retrieve information about the counter for each user.
Counter Details	Displays the information retrieved about the counter for each user.

@Remote Service Function Limitation

You can suspend the @Remote Service function. To display the settings screen, click [Security] - [@Remote Service Function Limitation].

Important

- **To receive the latest RC Gate firmware (application, firmware common components, platform, OS) updates from the Communication Server, set [Permit access by service] to [Permit]. To use the default version, select [Do not permit].**



@Remote Service functions

Item	Description
@Remote Service functions	If you select [Restrict], communication between the Communication Server and devices is restricted.

Communication Server Requests

Item	Description
System firmware update by the Communication Server	Select whether to allow system firmware to be updated by the Communication Server.
Device firmware update by the Communication Server	Select whether to allow device firmware to be updated by the Communication Server.
Auto Discovery settings by the Communication Server	Select whether to allow the Communication Server to use the Auto Discovery function.

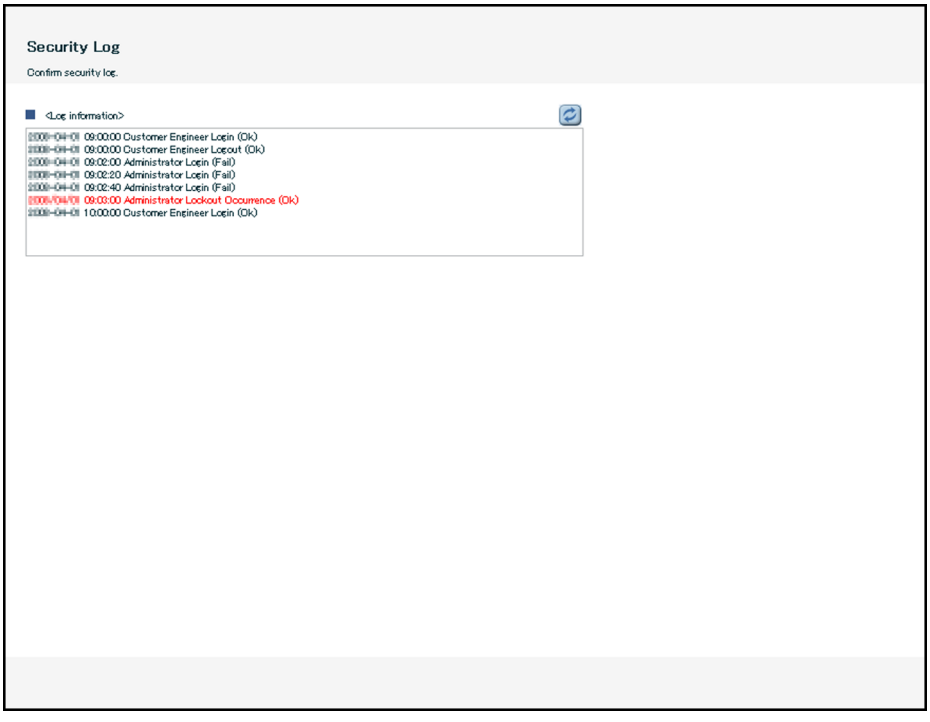
Security Log

The security log contains a list of security-related events, such as logins, logouts, and system changes. To display the security log, click [Security] - [Security Log].

Click [Refresh] to obtain the latest log.

Important

- Under the following operating conditions, about 28 log entries are generated each day. Because the minimum number of security log entries is 5,824, about 208 days of records can be stored in the security log (5,824 divided by 28 = 208).
  - The administrator and general users each log in and log out once a day.
  - Device polling occurs once an hour.
- It is recommended that you check the security log at least once every 104 days (about 15 weeks) to ensure that logs are not overwritten before you view them. Check the security log more frequently if your usage is greater than that given above.
- If the number of security log entries exceeds the maximum, new entries will overwrite the oldest entries, regardless of whether or not the log has been checked.
- When checking the log, confirm that your most recent login information is displayed. If your most recent login information is not displayed, contact your service representative.



The following table explains the information that is displayed for one entry in the security log.

Item	Description
Date and time	The UTC (universal coordinated time) date and time that the log entry was recorded. The format is as follows: y-m-d H:M:S y: year, m: month, d: day, H: hour, M: minute, S: second
User	The type of user who accessed RC Gate. • Center: "Communication Server" • System: "System"[1] • Customer engineer: "Customer Engineer" • RC Gate administrator: "Administrator" • General user: "User (**********)"[2]

Item	Description
Access contents	The event that caused the log to be recorded. • Power on (startup): "Logging Start" • Power off (shutdown, restart): "Logging End" • Readout of the system log: "Get SystemLog"[3] • Readout of the communication log: "Get CommunicationLog"[3] • Readout of the security log: "Get SecurityLog" • Login: "Login" • Logout: "Logout" • Lockout occurrence: "Lockout Occurrence" • CE account information changed: "Changes to CE Account"
Access contents	• Administrator account information changed: "Changes to ADMIN Account" • General user account information changed: "Changes to USER (**********) Account"[2] • General user account added: "Add USER (**********) Account"[2] • General user account deleted: "Delete USER (**********) Account"[2] • System time changed: "Adjust Clock" • System firmware updated: "System Firmware Update" • SSL communication error occurred: "SSL Communication"
Access contents	• Device certificate information updated: "Device Certificate Update" • Certification information updated: "System Certificate Update" • Performed self diagnosis: "Self Check" • System firmware correctness checked: "System Firmware Check"
Access result	• Operation was successful: "(Ok)" • Operation failed: "(Fail)"

Item	Description
Item separator	(whitespace)
Item separator	":" (colon)
Record separator	"\n" (linefeed)

1 "System" refers to the RC Gate itself.

2 "**********" is the first 13 characters of the user's account name.

3 The administrator cannot confirm the system log and communication log. These logs are used for maintenance.

6. Appendix

LCD Messages

The following table shows the messages that will be displayed on the LCD.

First Line

Message	Description
Warming Up	The system boot process is being performed.
Not Set Up	The @Remote service registration has not been completed.
Normal	The @Remote service registration has completed and the RC Gate is operating normally.
Off-line	The communication with the Communication Server has been suspended.
Error	A system error has occurred.
Call Service Rep	An error has occurred, and reboot has failed after trying it for the specified number of times.
Not in Service	The @Remote service has been limited due to @Remote Service Function Limitation.
Reboot	The system reboot is being performed.
Shutdown	The system completion process is being performed.

Second Line

Message	Description
SC:	System error has occurred, or the system has stopped due to abnormal conditions. Error status code will be displayed in maximum of 6-digit numbers. Contact your service representative.
Cable Disconnect	The cable is broken or improperly connected. Check the cable connection.
802 Server Error	Unable to connect to the IEEE802.1 x authentication server when using IEEE802.1 x authentication. Contact your network administrator.

Message	Description
802 Auth.Failure	IEEE802.1 x authentication has been failed when using IEEE802.1 x authentication. Contact your network administrator.
DHCPv6 Error	DHCPv6 setting is enabled but failed to obtain IP address. Contact your network administrator.
DHCPv4Error	DHCPv4 setting is enabled but failed to obtain IP address. Contact your network administrator.
----------	Displayed while starting up or exiting.
Network Information/Host name “host name” Network Information/IPv6 setting xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Network Information/IPv4 setting xxx.xxx.xxx.xxx (This figure shows the IP address)	Host name of the RC Gate, the IPv6 address of the RC Gate (LAN port), and the IPv4 address of the RC Gate (LAN port) are displayed in sequence.

Troubleshooting

When Error Messages Appear

Message	Reason and Action
Some item(s) have not been selected. Click Back to return the previous screen, then select the item(s).	Clicked [Next] without making a check to "Select" for the search results on the "Device Registration Wizard". Click [Back] to return to the previous screen, and check "Select" of the device(s) to register.
Internal errors System error(s) have occurred. Please call service for instructions. (error code of four digits)	An error has occurred in the system. Contact your service representative to notify the error code.
Processing was incomplete as the line was busy. Retry later. If the same error occurs, please call service for instructions.	An error such as a database error or a program malfunction has occurred in the Communication Server. If the Communication Server does not recover after while, contact your service representative.
Check Request No. If the same error occurs, call service for instructions.	If this error occurs even if you entered the correct request number, the error might be caused by a mismatch of registered information registered to the Communication Server. Contact your service representative. • You have entered the device that has already been registered, or the device that has not been registered to the RS center. • You are trying to register a device as a different group.
Invalid access. Log in again.	Other than invalid access, this error occurs when you open multiple windows by a Web browser and make settings with one window and give a request on the other. Do not open multiple windows with a Web browser.
You do not have privileges to use this function. Contact Remote Communication Gate administrator to check the settings.	Access will be forbidden for a minute because there were three login failures within five minutes. Wait for a minute until the access lock will automatically be released.

If Problems Described in Error Messages Persist

Contact your service representative if problems described in error messages persist.

When the Office or Devices are Moved

Registration to the Communication Server is required in the following cases. Contact your service representative.

- When your office has moved (The RC Gate has moved.)
- When managed devices are moved (Except Auto Discovery)
- When managed devices are newly connected (Except Auto Discovery)
- When managed devices are deleted (Except Auto Discovery)

To Return the RC Gate

Contact your service representative when you no longer require the RC Gate. Your service representative will collect it and, for security purposes, will erase all information it has stored.

Error Codes

Code	Message
0001	Cannot connect to the network. Check the LAN cable connection.
0002	Cannot connect to the Network. If DHCP is enabled, check the network settings. If the same error occurs, call service for instructions.
0003	Cannot authenticate IEEE802.1x. Confirm with the network administrator. If the same error occurs, please call service for instructions.
0004	Cannot authenticate IEEE802.1x. Confirm the settings of IEEE802.1x authentication. If the same error occurs, please call service for instructions.
0005	Cannot connect to the Network. Check DNS on the network settings. If the same error occurs, call service for instructions.
0006	Cannot connect to the network. Confirm the proxy server name and port number.
0007	Cannot connect to the Network. Check proxy user name, proxy password or proxy domain name.

Code	Message
1001	Cannot connect to the Communication Server. If the same error occurs, please call service for instructions.
1002	Cannot connect to the Communication Server. If the same error occurs, please call service for instructions.
1003	Cannot connect to the Communication Server. If the same error occurs, please call service for instructions.
1004	Cannot communicate with the Network. Please call service for instructions.
1005	Cannot communicate with the Network. Please call service for instructions.

Default Settings

Item	Default Value	Remarks
IP Address Send Permission	Permit (default)	
DHCP	Disable	
Subnet Mask	255.255.255.0	See the network setup screens.
Ethernet speed	Auto select	
Proxy server	Disable	
Proxy port	8080	
RC Gate e-mail address (for sender)	rc_gate	
Number of times to resend E-mail	3 times	
Resend E-mail interval time	15 seconds	
SMTP server port	25	
SMTP_AUTH	Disable	
POP before SMTP	Disable	
POP server port	110	
Permit access by service	Permit	

Item	Default Value	Remarks
System firmware update by the Communication Server	Permit	
Device firmware update by the Communication Server	Permit	
Auto Discovery settings by the Communication Server	Permit	
IP address search range	0.0.0.0 to 0.0.0.0	If using "Auto Discovery Setting Wizard "and "Device Registration Wizard".
SNMP Community Name	public	If using "Auto Discovery Setting Wizard "and "Device Registration Wizard".
Display items	10 addresses	If using "Auto Discovery Setting Wizard "and "Device Registration Wizard".

Note

- The default display language and time zone settings vary depending on where the RC Gate is used.

Specifications for the Main Unit

Item	Descriptions	
Type	Box type	
Interface	Ethernet interface × 2 (10BASE-T or 100BASE-TX)	
Options	• Remote Communication Gate Memory 1000 • Remote Communication Gate Storage 1000	
Indicator	LED	2 (Error Status, Power)
	Display	LCD (16 digits × 2 lines)
Protocols	TCP/IP, SNMP, HTTP, SOAP, SMTP, DHCP	
Managing Devices	Digital multifunction devices, copiers, and printers correspondent to the service	
Maximum Number of Devices to be Supported	• Controlled devices registered to the Communication Server 100 devices (1,000 devices when the optional memory and storage have been installed) • Auto Discovery 1,000 devices (including the devices registered to the Communication Server on the network)	
Environment	10 - 32 °C (50 - 89.6 °F), 15 - 80 %RH	
Power	• For Users in Countries Outside of North America: 220-240 Vac, 50/60 Hz, 2.5 A or more • For Users in North America: 120 Vac, 60 Hz, 3.0 A or more	
Power Consumption	20 W or less	
Dimensions	Width 253 mm (10") /Depth 160 mm (6.3") /Height 48 mm (1.9")	
Weight	800 g (1.8 lbs)	

Information about Installed Software

The following is a list of the software included in this equipment:

- WPASupplicant
- OpenSSL
- busybox
- dosfstools
- glibc
- knopflerfish
- corelib
- as3crypto
- as3httpclientlib
- SNMP4J
- kxml2
- Apache commons
- kSOAP2
- linux-kernel
- Dibbler
- BouncyCastle
- AspectJ

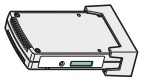
You can check the information about license and copyright of each software by clicking [License and Copyright Information] in the login page.

INDEX

MEMO

MEMO

Remote Communication Gate A Operating Instructions



EN GB EN US
D459-8502B