Albacore
Machine Code: D3AR
Field Service Manual

October, 2015

Important Safety Notices

Prevention of Physical Injury

1. Before you start any of the procedures in this manual, disconnect all power cable and network cables.
2. The wall outlet should be near the equipment and easily accessible.
3. If any adjustment or operation check has to be made with exterior covers off or open while the main switch is turned on, keep hands away from electrified or mechanically driven components.
4. The inside and the metal parts of the equipment may become extremely hot during operation. Be careful to avoid touching those components with your bare hands.
5. Before you start any of the procedures in this manual, touch a grounded object or put on an anti-static wristband. This is to prevent static electricity from damaging the internal components.

Observance of Electrical Safety Standards

1. The equipment and its peripherals must be installed and maintained by a customer service representative who has completed the training course on those models.
2. DO NOT replace or try to recharge the lithium battery. If the battery does not operate, replace the entire mainframe. This is because the battery can explode if it is replaced incorrectly.

Safety and Ecological Notes for Disposal

1. Dispose of replaced parts in accordance with local regulations.
2. When keeping used lithium batteries in order to dispose of them later, do not put more than 100 batteries per sealed box. Storing larger numbers or not sealing them apart may lead to chemical reactions and heat build-up.

Symbols, Abbreviations and Trademarks

This manual uses the following symbol. The meaning of the symbol is as follows:

	Screw

Trademarks

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

Firefox is a registered trademark of the Mozilla Foundation.

Google and Chrome™ are trademarks of Google Inc.

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

TABLE OF CONTENTS

3. Maintenance of @Remote-Connected Devices

4. Troubleshooting

5. Features

1. Product Information

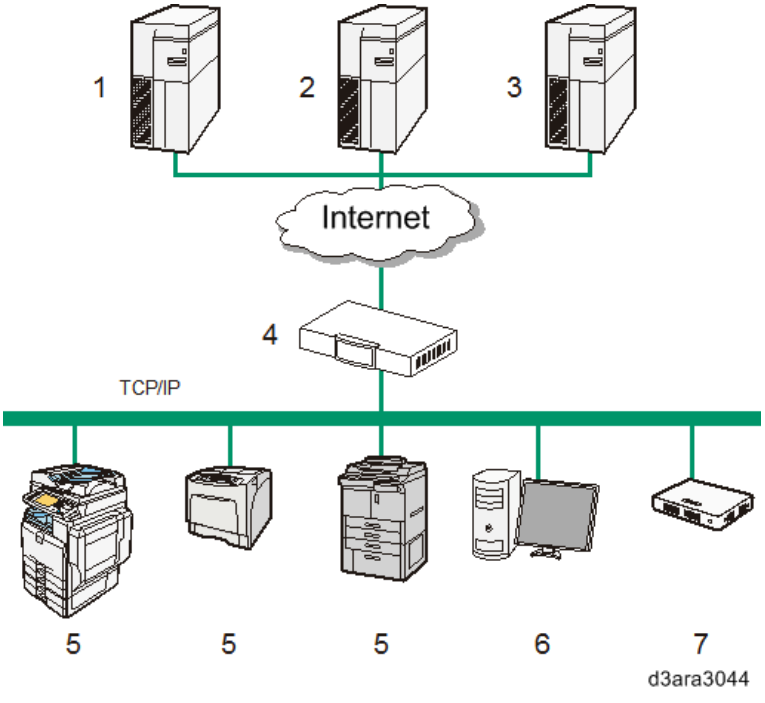
Outline of the System

The RC Gate A2 communicates with the @Remote Center over the Internet using HTTPS.

Authentication by HTTPS ensures the security of communication between the RC Gate and the @Remote Center. The @Remote Center serves as the HTTPS server, and the RC Gate works as the HTTPS client.

Communication is possible when the following conditions are satisfied:

- The customer environment is arranged to be able to access Web sites outside their network.
- The configuration for access to the proxy server is properly done (only if a proxy server is used).



No.	Name	Function
1	@Remote Center	Information sent for various services will be aggregated to this server.
2	Global Server (SERES)	For firmware distribution
3	eDC Server	For activation of the Accounting Report option

No.	Name	Function
4	Proxy Server and/or Firewalls	The customer can use a proxy server and firewalls with this appliance. The proxy server can be used without authentication or with Basic authentication, Digest authentication, Windows authentication (NTLMv2 only), or Kerberos authentication.
5	Devices	Printers and multifunction products (MFPs) can be managed with this appliance. This appliance can manage a maximum of 100 devices. • Two types of devices can be managed. One is compatible with HTTPS, and the other is compatible with SNMP. The user can identify the type by selecting [@Remote Properties] on the Device List and referring to [Connection Type]. • Mutual authentication in an 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. This is the default setting, but if there is a communication failure with these types of devices, the setting may have been changed. • SNMPv1/v2 or SNMPv3 can be used for communication between the RC Gate and SNMP-compatible devices. • TLS 1.0, TLS 1.1, and TLS 1.2 can be used to communicate between the RC Gate and TLS-compatible devices. If you have installed optional storage to expand the capacity, up to 1,000 devices can be registered.
6	Computer for Administration	You can manage this appliance by accessing the RC Gate Monitor via web browser.
7	This Appliance (RC Gate A2)	Interfaces the managed devices with the @Remote Center. Sends the device information to the @Remote Center, and receives software to update the devices from the @Remote Center.

Precautions for Use

Checking the Customer Environment and Gaining Permission for Installation

- Make sure that the Internet connection is a fixed broadband connection.

  If this appliance is installed in a dial-up connection environment, a fee is charged for each connection.

- Gain permission for installation from the network administrator.

  If the customer company has many branches (offices, factories and so on), the head office may have an organization for network administration. Be sure to gain permission from a network administrator of higher rank, as well as the network administrator of the installation site.

Handling Customer Information

Handling Customer Information Related to Security

Information related to customer security (for example, IP addresses and proxy information) must be collected from the customer on the day you install the equipment. Never take such information outside the customer site.

Precaution about Proxy Server Configuration

Always explain to the customer that there are two ways to configure proxy server information:

1. Entry by the CE on the customer's behalf
2. Direct entry by the customer

Note that there are some customers who do not want to reveal such information to persons outside the organization.

Precaution about the Customer Survey

In the customer survey, make a note of the name of the person who will provide you with security-related information.

When Terminating the @Remote Contract

- To ensure initialization of the data inside, the RC Gate A2 should be processed by the @Remote Center before being returned.
- If returning processing from the @Remote Center was not applied, initialize the RC Gate A2 after receiving it from the customer. See page 132 "Resetting to the Factory Default Settings".
- If returning processing from the @Remote Center cannot be applied, ask the operator to remove the RC Gate A2 from the Center server.

When Devices Are Installed in Different Branches

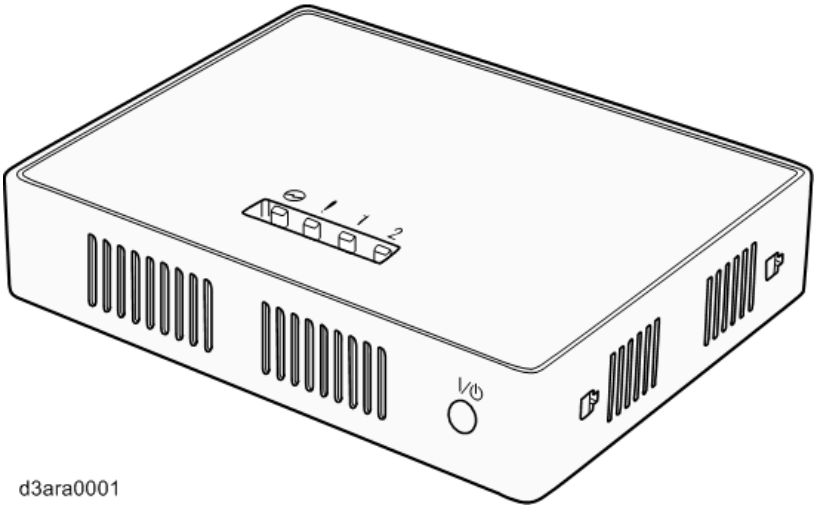
RC Gate A2 is capable of communication with parties outside the local segment. However, if Manual Discovery*1 fails and RC Gate A2 cannot connect to a previously discovered device, check the IP address of the device and change the device information on RC Gate A2.

*1: With this function, you can search for previously registered devices that are currently missing on RC Gate A2.

Appliance Configuration

Appliance

Name	Machine code
RICOH Remote Communication Gate A2 (hereinafter referred to as RC Gate A2)	D3AR



d3ara0001

Option

- RICOH Remote Communication Gate A2 Storage 1000

  The RC Gate can manage a maximum of 100 devices. If you install optional storage to expand the capacity, up to 1,000 devices can be registered.

Name	Machine code
RICOH Remote Communication Gate A2 Storage 1000	D3AX

d3ara0002

- Accounting Report

Name	Machine code
RICOH Remote Communication Gate A2 Accounting Report	-

Specifications for the Main Unit

Differences from the Predecessor Product

- Selectable encryption strength (SSL/TLS)

  For enhanced security, the encryption strength of communications between the appliance and the devices can be selected. This is to counteract the POODLE vulnerability and other problems.

- Simplified installation procedure

  For installation of this appliance, a micro-USB cable is used instead of an Ethernet crossover cable. Also, it is no longer necessary to change the IP address of the CE's computer in "Internet Protocol Version 4 (TCP/IPv4) Properties".

- Accounting Report option

  The counter information of each user can be collected from the devices.

  * A license is required to use this function.

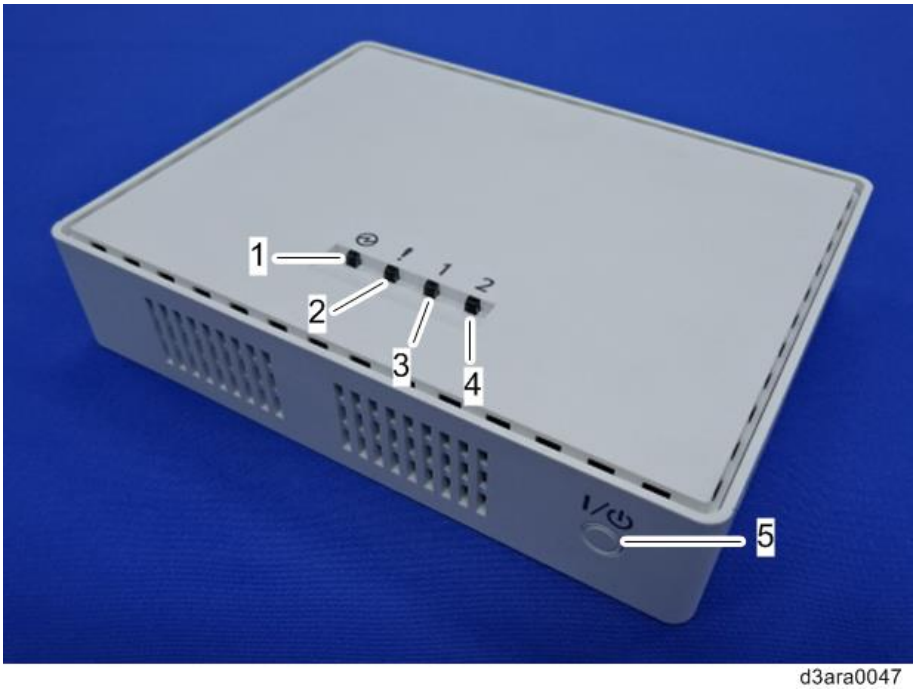
Specifications

Item	Description
Type	Box Type
Interfaces	Ethernet interface x 1 (10BASE-T, 100BASE-TX, or 1000BASE-T) USB 2.0 interface (Type micro-B connector) x 1 USB 2.0 Host interface (Type A connector) x 1 (not used)
Option	• RICOH Remote Communication Gate A2 Storage 1000 • RICOH Remote Communication Gate A2 Accounting Report Option
Indicator	LED x 4 (Blue: Power, Red: Alert, Yellow: Status x 2)
Main service functions	Automatic counter collection Remote maintenance (Remote diagnostics, SC/CC/AC/MC calls) Usage report Toner end information supply Remote firmware update
Protocols	HTTP, HTTPS, SNMP v1/v2/v3, FTP, SMTP, POP

Item	Description
Managing Devices	Digital multifunction devices, copiers, and printers compatible with the service
Maximum Number of Devices to be Supported	• Managed devices registered at the @Remote Center 100 devices (1,000 devices when the optional storage has been installed; 300 devices when the optional storage has been installed and the Accounting Report option is used.) • Auto Discovery 500 devices (1,500 devices when the optional storage has been installed; including the devices registered at the @Remote Center on the network) • Accounting Report option 100 devices (300 devices when the optional storage has been installed)
Environment	Operating ambient temperature range: 10 - 32 °C (50 - 89.6 °F), 15 - 80 %RH Storage temperature range: -10 - 50 °C (14 - 122 °F), 15 - 90 %RH
Power	• For Users in Countries Outside North America: 220-240 V, 50/60 Hz, 2.5 A or more • For Users in North America: 120 V, 60 Hz, 3.w0 A or more
Power Consumption	10 W
Dimensions	Width 155 mm (6.1 inches) /Depth 120 mm (4.7 inches) /Height 32 mm (1.3 inches)
Weight	300 g (0.7 lbs)

Overview

Front



No.	Name	Description
1	Power LED (Blue)*1	The display pattern changes according to the status of the appliance.
2	Alert LED (Red)* 1	The display pattern changes according to the status of the appliance.
3	Status 1 LED (Yellow)* 1	The display pattern changes according to the status of the appliance.
4	Status 2 LED (Yellow)* 1	The display pattern changes according to the status of the appliance.

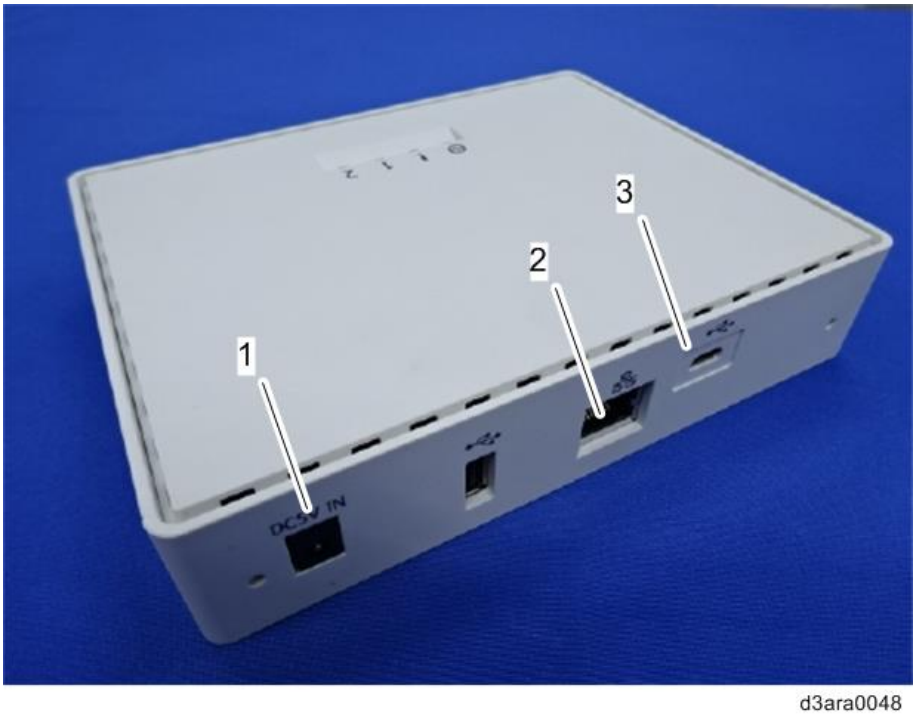
RTB 5 Information added

No.	Name	Description
5	Power button*2	Press the button to turn on the power or switch to standby mode. The power turns on when the power cable is plugged into the wall socket even without pressing the power button. Also, by holding down the power button for 4 seconds, the system shuts down and switches to the standby mode.

*1: If the LEDs light or flash, see page 79 "LED Display".

*2: Before disconnecting the power plug, be sure to shut down the machine to switch to the standby mode. Otherwise, the storage medium may be damaged, causing the most recent log data (up to 1 hour) to be lost.

Back



d3ara0048

No.	Name	Description
1	Power Socket	This socket is used to connect the power cord.

No.	Name	Description
2	LAN Port	This is the network (Ethernet) interface port to connect the RC Gate A2 to the network. The settings are blank when the product is shipped from the factory. Specify the IP address during the initial setting procedure. See page 29 "Initial Settings" for this procedure.
3	USB 2.0 interface (Maintenance port)	This is the port for connecting the micro-USB cable. This port is used when a customer engineer performs maintenance, or connects a PC to start the initial settings and registration of the RC Gate A2.

LAN Port Indicator

You can check the connection condition of the LAN port when power is supplied.

No.	Name	Description
1	LED (connection status)	Lights when the appliance is connected to the network (orange).
2	LED (send/receive status)	Lights when the appliance is sending or receiving data (green).

Inside

d3bhz0024

No.	Name	Description
1	Power switch	When the Power button is pressed, the switch turns the appliance ON or OFF (standby).
2	DIP switch	Use this when resetting the RC Gate A2 to the factory-default settings. See page 132 "Resetting to the Factory Default Settings".
3	Coin cell	-
4	SD card slot	Slot 1: Used (front side) Slot 2: For the optional SD card.
5	Tact switch	There is no CE operation that requires the use of the tact switch. If you happen to press the tact switch while the power is on and the cover is open, any operation will be stopped and the RC Gate A2 will be rebooted in the same way as when the power cord is disconnected and connected again.

2. Installation

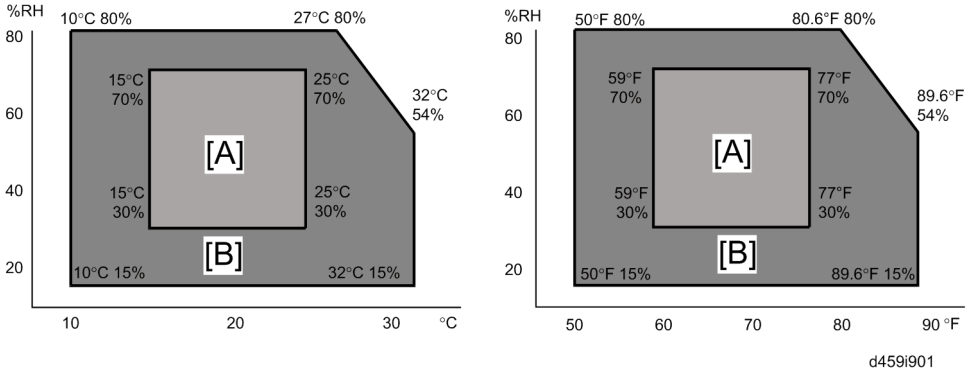
Installation Requirements

Environment

Check if the environment of the customer site meet the following conditions.

Setup environment

- Place the appliance on a level and vibration free surface.
- Install the appliance vertically or horizontally, so that the appliance's vent is not blocked.
- Place the appliance in an area that has the recommended temperature and humidity shown below:

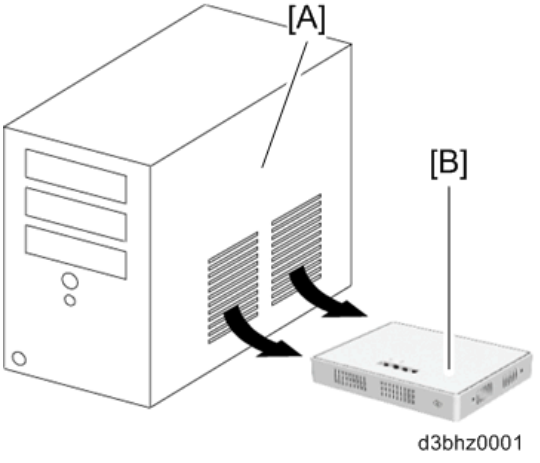


[A]: Recommended range, [B]: Operation range

- Temperature: 10°C to 32°C, 50°F to 89.6°F
- Humidity: 15 to 80% RH

Environments to Avoid

- Areas exposed to direct sunlight or strong light
- Locations near air conditioners or humidifiers
- Locations near other electronic equipment
- Areas that are excessively cold, hot, or humid
- Areas directly exposed to currents of hot, cold, or room-temperature air from air conditioners, or radiant heat from heaters
- Where exhaust from other machines [A] gets to the appliance [B].



IP address

- Make sure that the IP address to be used during the installation of RC Gate A2 is not used in the customer's network environment. See the notes for Step 9 of page 29 "Initial Settings".

Notes on an Environment Using both IPv4 and IPv6

- This product supports the dual-stack environment of IPv4 and IPv6, but it does not support an environment that uses a translator. In an environment using a translator, depending on the MFP or printer in use, no communication with this product can be established. If no communication is possible between the device and the appliance, check whether the environment uses a translator.

Preparation Items

Make sure to bring the following items to the customer site.

Important

- **A micro-USB cable is required when a CE configures the RC Gate A2.**

Name	Product Code	Quantity
RC Gate A2	NA: D3AR-17 EU/AP: D3AR-27 CHN: D3AR-21 KOR: D3AR-28	As requested from the sales department

Name	P/N	Quantity
Micro-USB cable	D3AR5400	1

Request from the sales department

The required number of RC Gate A2 appliances depends on the number of billing companies, calculation date, and number of devices (MFPs and printers) to be managed. Ask the sales department for the number of required RC Gates.

Laptop computer

Operating System:

- Windows 7 or later (both the 32-bit version and the 64-bit version can be used.)

Browser:

- Microsoft Internet Explorer 8.0 or later
- Mozilla Firefox 28.0 or later

In both cases, only the client operating systems of Windows are supported.

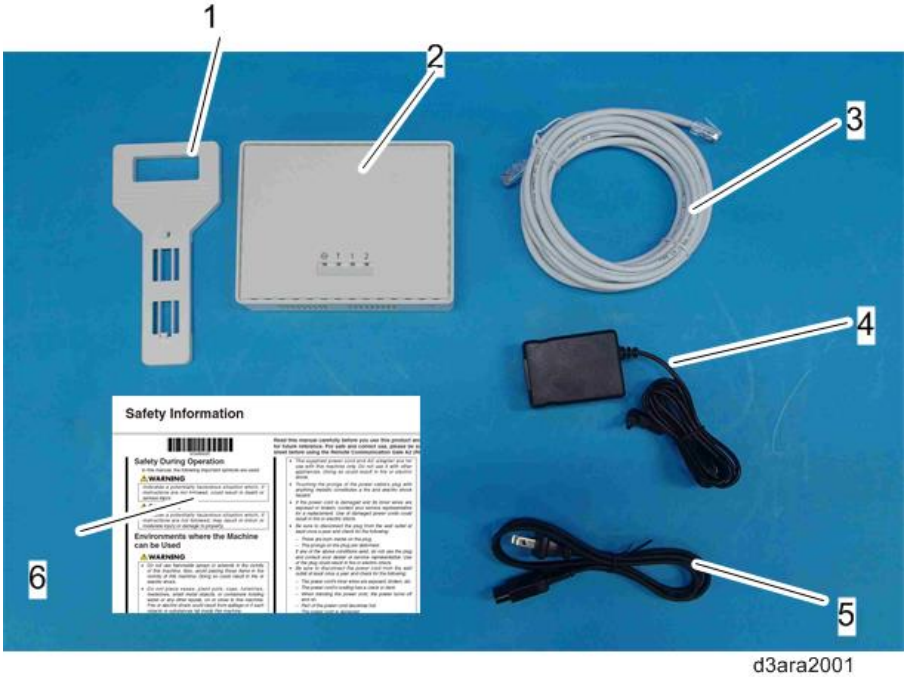
Google Chrome is not supported.

USB port:

- USB 2.0 compatible port

Components Check

No.	Description	Q'ty	P/N
1	Stand	1	D3AR2201
2	RC Gate A2	1	NA: D3AR0017 EU/AP: D3AR0027 CHN: D3AR0021 KOR: D3AR0028
3	Network Cable	1	A7685402
4	AC Adapter	1	NA: D3AR5201 EU/AP, CHN, KOR: D3AR5200
5	Power Cord	1	NA: D3AR5317 EU/AP: D3AR5327 CHN: D3AR5321 KOR: D3AR5328
6	Safety Information/Setup Guide	1	-


1
2
3
4
5
6
Safety Information
Safety During Operation
WARNING
Environments where the Machine can be Used
WARNING

d3ara2001

Installation Overview

Important

- **Before unpacking, check that the unpacking detection seal is not broken (to check that the product has not been unpacked).**
- **For customers who want to use the appliance in an operating environment certified in accordance with CC certification, configure it in accordance with page 65 "Configuration for a CC-Certified Environment".**
- **Be sure to remove the USB cable after installation is completed.**

Installation procedure of RC Gate A2

Follow the 5 steps listed below when installing RC Gate A2.

1. Check the environment and the configuration of the devices to be connected. (page 25 "Checking the Environment and Configuration of Devices (MFPs/Printers) to Be Connected")
2. Install the RC Gate A2 hardware. (page 26 "Installing the RC Gate A2 and Connecting the Power Cord")
3. Make initial settings for the RC Gate A2. (page 29 "Initial Settings")
4. Register the RC Gate A2 with the @Remote Center. (page 38 "Registration with the @Remote Center")
5. Register the devices (MFPs/printers) to be managed. (page 39 "Registering Devices (MFPs/Printers)")

Glossary of Terms

Term	Explanation
RC Gate A2	RICOH Remote Communication Gate A2
RC Gate A	RICOH Remote Communication Gate A
RC Gate Type BN1/BM1	RICOH Remote Communication Gate Type BN1/BM1
RC Gate	A general term for external appliances described above, which provide connection to the @Remote Center.
Storage Option	RICOH Remote Communication Gate A2 Storage 1000
Accounting Report Option	RICOH Remote Communication Gate A2 Accounting Report Option

Checking the Environment and Configuration of Devices (MFPs/Printers) to Be Connected

Browsers Compatible with the Appliance

- Microsoft Internet Explorer 8.0 or later
- Mozilla Firefox 28.0 or later

Compatible Operating Systems

- Windows 7 or later (both the 32-bit version and the 64-bit version can be used.)

The following four items are required when installing the appliance.

Item	Note
Customer survey	Make sure that the request number from the @Remote Center is written on the survey.
RC Gate A2	-
Laptop Computer	• Make sure that it has a USB 2.0 compatible port. • Make sure that one of the compatible browsers works on it. If you cannot bring a laptop computer, configuration can also be done with the customer's computer.
Micro-USB cable	Connects the RC Gate A2 and the computer.

Checking the environment of the customer site

- An open port on the hub (router) for connecting the RC Gate to the network
- A power outlet for the power cord of the appliance

Configuration of the imaging devices (MFPs/printers)

SP5-816-001 must be set to "2".

Value	Remote service setting
0	Remote service off
1	CSS remote service on
2 (default)	@Remote service on

Installing the RC Gate A2 and Connecting the Power Cord

Installation Procedure

1. **Check the environment. See page 19 "Environment".**

   Note

   - Before unpacking, check that the unpacking detection seal is not broken (this checks that the product has not been unpacked).

2. **Check the contents of the package. See page 22 "Components Check".**
3. **Place the RC Gate either horizontally or vertically.**
   - When placing the RC Gate A2 horizontally: Place it so that the LEDs face upward.

d3arz0003

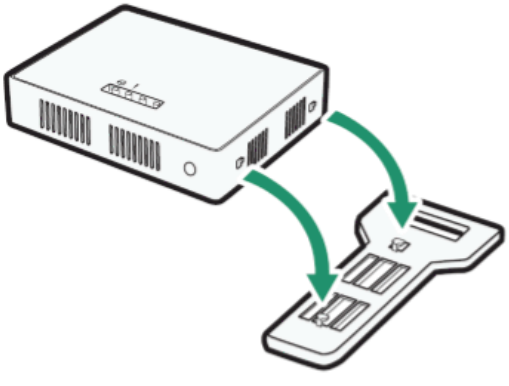
   - When placing the RC Gate A2 vertically: Use the stand to make it stable.

d3arz0015

Note

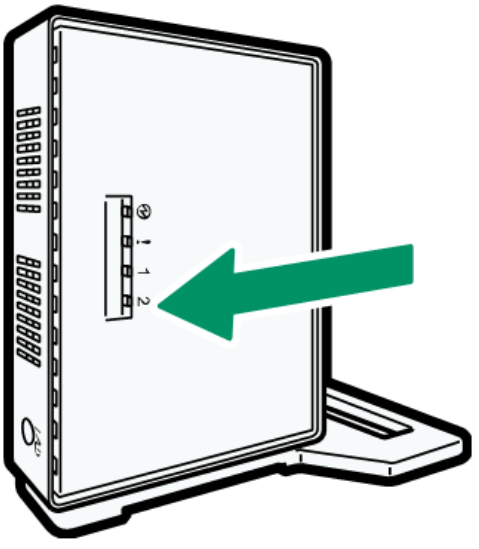
- How to attach the stand

1. Insert the stand's tabs into the holes in the RC Gate A2.



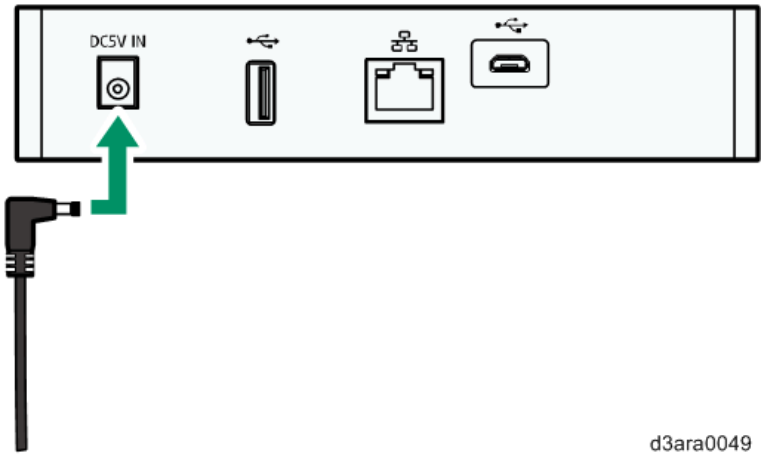
w_d3arz2000

2. Slide the RC Gate A2 till it stops.



d3arz2001

4. **Connect the AC adapter to the power cord.**
5. **Connect the AC adapter securely to the power socket of the RC Gate A2.**



d3ara0049

6. **Plug the power cord into the wall outlet.**

   The RC Gate A2 turns on.

Note

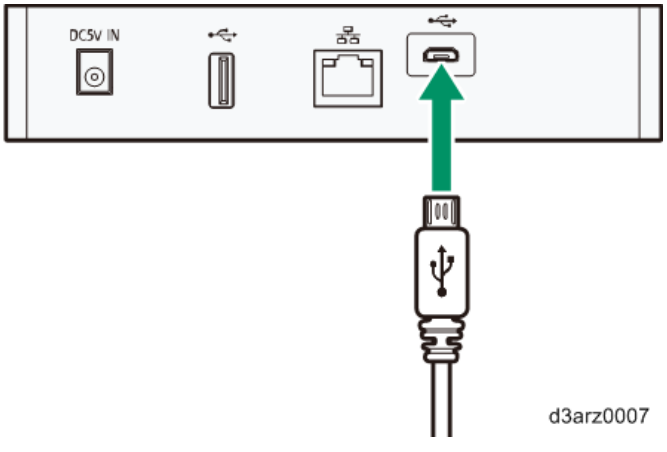
- The startup process takes about 5 minutes. When it is complete, the blue LED flashes at one-second intervals.
- When turning off the RC Gate A2, first shut it down correctly (see page 66 "Shutdown"), and then unplug the power cord.

Initial Settings

Important

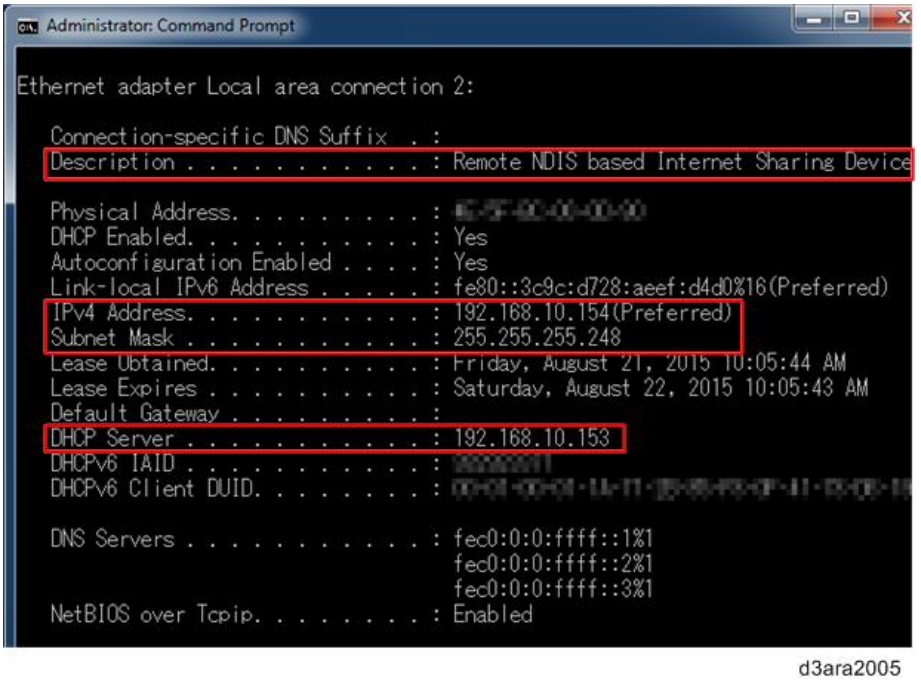
- Depending on the OS of your computer, login as a member of the administrators group may be required.
- Do not use the factory default of the CE password as it is, and never fail to change it (see page 115 "About the Login Password"). After changing the password, be sure to remember it. If you forget the CE password, the RC Gate A2 must be replaced. 'Replaced' means reset by returning the RC gate A2 to the factory default settings (see page 132 "Resetting to the Factory Default Settings"), and then performing a replacement procedure with the @Remote Center (see page 47 "Replacement/Migration").
- For security purposes, if you fail to log in to the RC Gate A2 monitor at least 3 times in 5 minutes, you will have to wait an additional 1 minute before you can try to log in again.
- If a dialog appears, asking "Stop running this script?", always click [No]. Proper operation is not guaranteed if you click [Yes] in this dialog.
- Problems may occur in the following conditions.
  - The web browser being used is older than the recommended version.
  - JavaScript is disabled.
  - Cookies are disabled.
  - Cache files are being used.
  - The page layout may get corrupted depending on the text size setting of the browser. It is recommended that you set it to "Medium" or smaller.
  - Characters may be corrupted if the browser does not support the selected language.

1. Connect one end of the micro-USB cable to the USB 2.0 port of the RC Gate A2 and connect the other end to your computer.



When connecting the RC Gate A2 to the computer for the first time, the message "Installing device driver software" appears on the computer screen. Wait until driver software installation is complete (the message disappears). When the message disappears, the computer is ready for network connection with the RC Gate A2.

2. **Type "ipconfig /all" in a command prompt window and make sure that an IP address is assigned to the computer via DHCP.**



d3ara2005

Item	Displayed value
Description	Remote NDIS based Internet Sharing Device
IPv4 Address	192.168.10.154 (when connected for the first time)
Subnet Mask	255.255.255.248
DHCP Server (this is the Maintenance Port for the RC Gate A2)	192.168.10.153 (default value)

3. **Now we can start to connect with the RC Gate A2 and make initial settings. Start the web browser of the computer.**
4. **Enter "http://192.168.10.153:8080/index.html" in the address bar.**

5. **The login window of the RC Gate A2 appears on the screen. Check the LED display to make sure that the RC Gate A2 has started up completely. Enter "RicohAtRemoteOperator" for [User Name] and enter the password for [Password]. Select the display language in [Language], and then click [Login].**

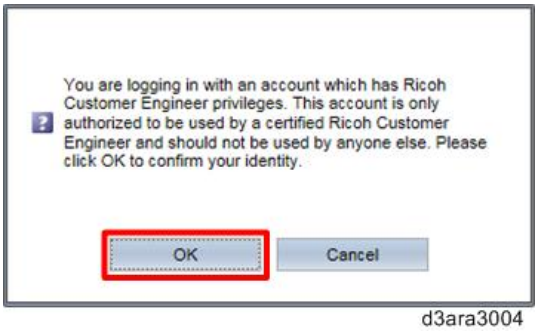
d3ara2006

User Name: RicohAtRemoteOperator

Note

- The user name cannot be changed.

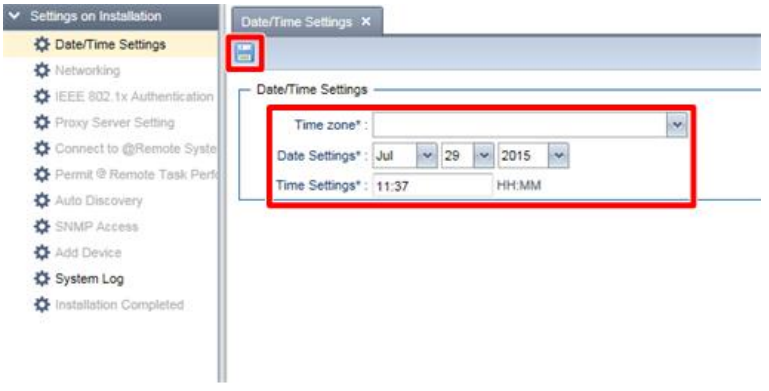
6. **When the following confirmation message appears, click [OK].**



d3ara3004

7. **When [Settings on Installation] appears, select the area in which the RC Gate A2 is installed from the [Time zone] pull-down menu. Make sure the date and time are set correctly, and then click (Save).**

You cannot start configuring the [Networking] settings until you click (Save).

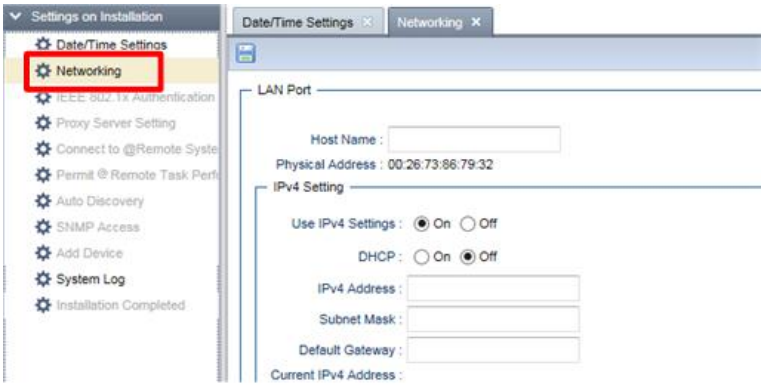


d3ara3005

Note

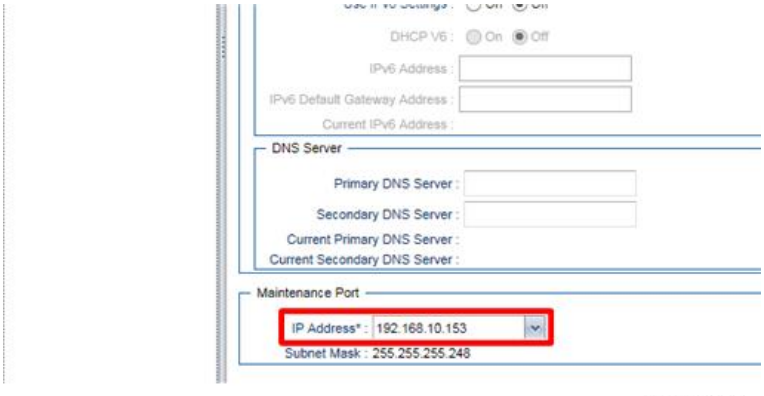
- About Daylight Saving Time
  RC Gate A2 supports Daylight Saving Time (DST) and changes the time displayed on the browser screen and the time at which a task is executed. Whether or not Daylight Saving Time is applied and the implementation period depends on the selected time zone and country or region.
  When the time changes at the beginning or the end of Daylight Saving Time period, tasks are executed as follows:
- Example: When 2:00 becomes 3:00 in local time
  - A task scheduled at 2:00: Will be skipped.
  - A task scheduled at 2:30: Will be skipped.
  - A task scheduled at 3:00: Will be executed at 3:00.
- Example: When 3:00 becomes 2:00 in local time
  - A task scheduled at 2:00: Will be executed again at the second 2:00.
  - A task scheduled at 2:30: Will be executed again at the second 2:30.
  - A task scheduled at 3:00: Will be executed at 3:00.

8. **Click [Networking].**



d3ara3006

9. **Ask the customer whether the IP address of the micro-USB port is being used in the LAN environment of the customer site. If it is being used, change the [IP address] under [Maintenance Port] to an IP address that is not being used.**



d3ara3007

Note

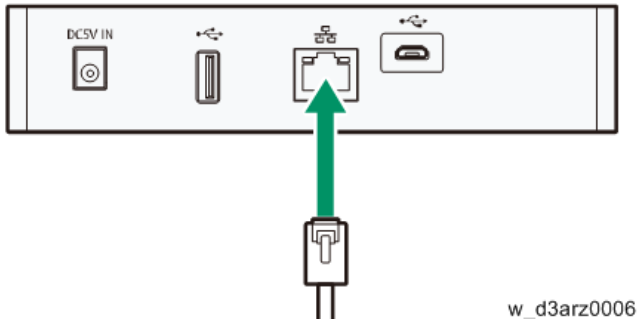
- To avoid an IP address conflict with another device on the customer network, the IP address of the [Maintenance Port] can be changed. The IP address must be "192.168.nnn.153", and any number between 1 and 254 can be selected for "nnn". (Default: 10.)
  Be careful when specifying the address, because the addresses that may conflict with customer devices change depending on the maintenance port address.

Maintenance Port IP Address	IP addresses that may conflict with a device on the customer network
192.168.1.153	192.168.1.152 to 192.168.1.159
192.168.2.153	192.168.2.152 to 192.168.2.159

Maintenance Port IP Address	IP addresses that may conflict with a device on the customer network
:	:
192.168.10.153	192.168.10.152 to 192.168.10.159
:	:
192.168.254.153	192.168.254.152 to 192.168.254.159

- Devices on the customer network with the same network address as the Maintenance Port IP address (192.168.xxx.153) cannot be recognized by the RC Gate A2. Because the Subnet Mask is 255.255.255.248 (prefix length /29), the following IP addresses have the same network address as the Maintenance Port IP address: 192.168.xxx.152 through 192.168.xxx.159.
- The IP address of the computer is assigned by DHCP. The assigned IP addresses are reset after one day. If more than five computers are connected to RC Gate A2 within the reset period (one day), assignable IP addresses will be exhausted and network connection will not work properly. IP addresses can be assigned again after you turn the RC Gate A2 off and on.

10. Connect the network cable to the LAN port of RC Gate A2.



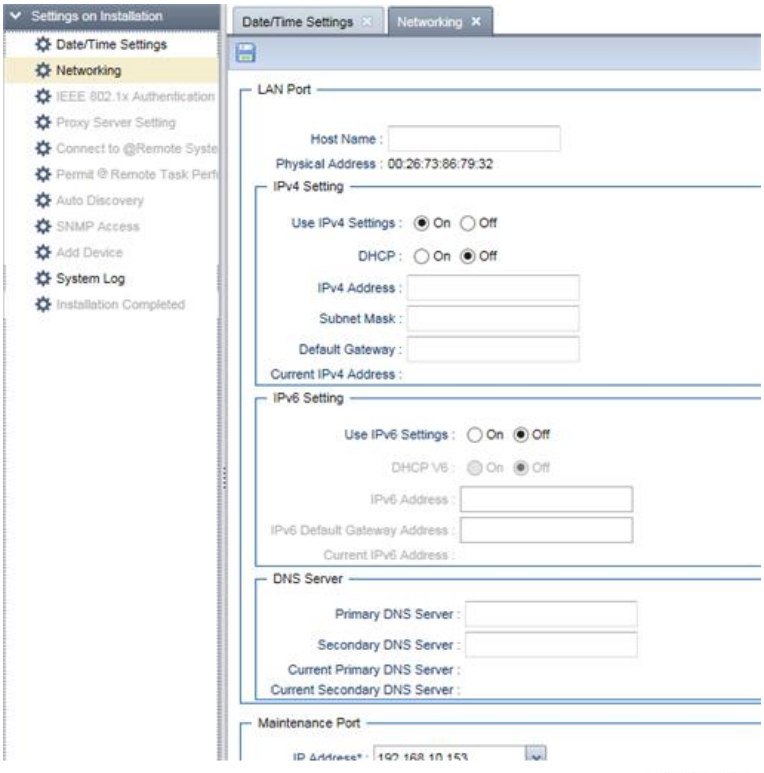
Connect this appliance to the network with the supplied network cable. You can use 10BASE-T, 100BASE-TX or 1000BASE-T network cable instead of the supplied cable. When connecting to the network via a 100BASE-TX or 1000BASE-T network cable, use a Category 5 or higher cable.

11. Connect the other end of the cable to a hub on the customer's network.

12. In [Networking], specify settings for the [LAN Port] group.

When using DHCP, select [On].

When not using DHCP, enter the address directly.

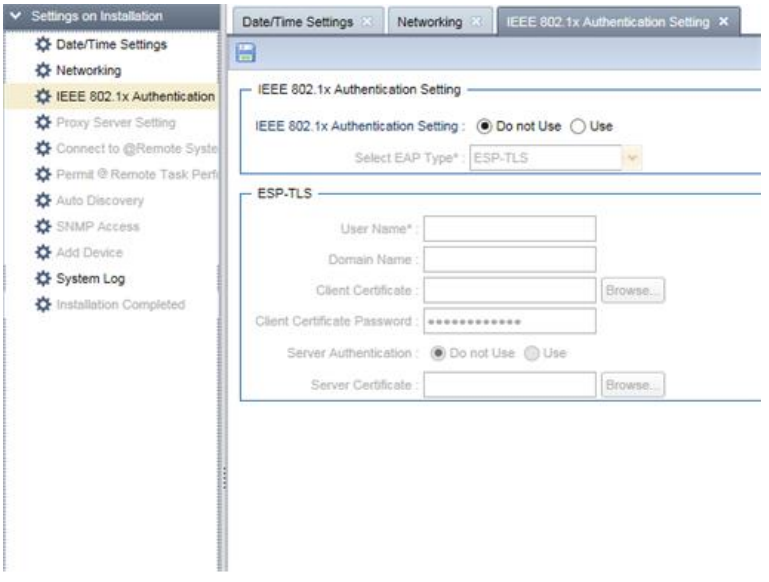


Note

- IPv6 stateless address auto configuration (which means that a router assigns the first part of the address (prefix) to a device) is always enabled. It cannot be disabled.
- After you change the DNS configuration, you must restart the RC Gate A2.

13. **Configure the DNS Server settings. (Required)**
14. **Click (Save).**
15. **Click [IEEE 802.1x Authentication Setting].**
16. **If IEEE802.1x Authentication is to be used, select [Use] and configure the required settings.**

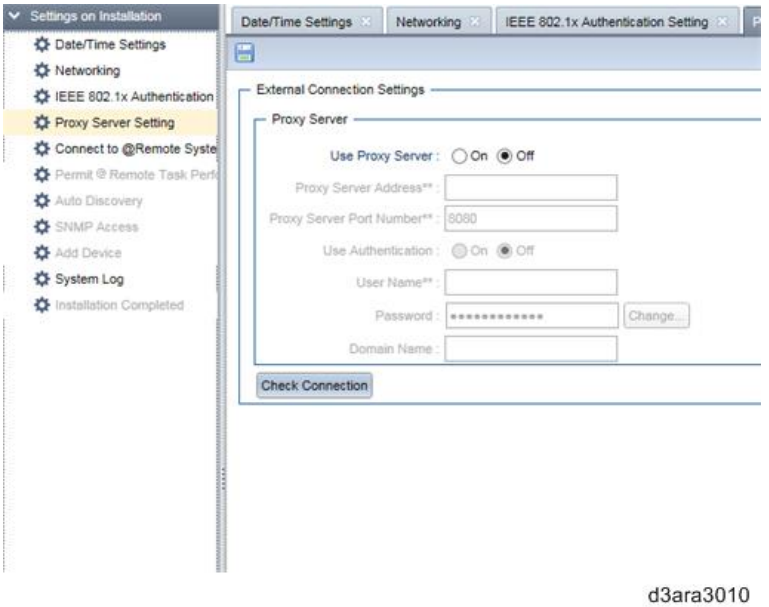
17. Click (Save).



d3ara3009

18. If a proxy server is to be used, click [Proxy Server Setting].

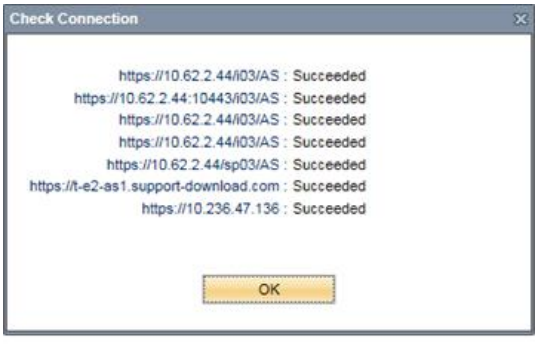
Set "Use Proxy Server" to [On]. Configure other settings as required, and then click (Save).



d3ara3010

Note

- By clicking [Check Connection], you can check whether the RC Gate A2 can connect to the @Remote system servers.

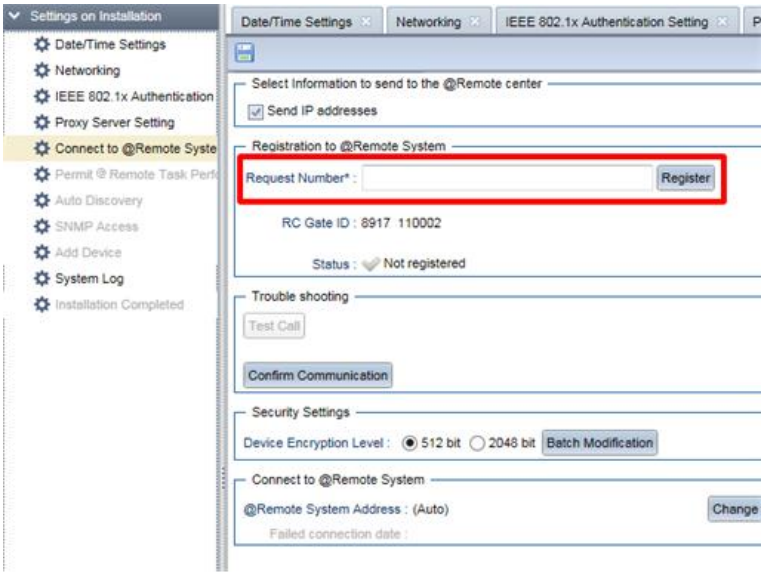


d3ara3011

- When connection fails, see page 75 "How to Check Connection with Related Servers" and take the required action.

Registration with the @Remote Center

1. **Complete the procedure in page 29 "Initial Settings".**
2. **In "Connect to @Remote System", enter the "Request Number" and click "Register".**



"Register is succeeded." appears and the "Status" changes to "Registered".

3. **Click (Save) to save the settings.**

Note

- Configure "Troubleshooting", "Security Settings", or "Connect to @Remote System" if necessary.
- To use this appliance in a CC-certified environment, select [2048 bit] for [Device Encryption Level] in "Security Settings".
  Note: The devices must be capable of handling 2048 bit encryption.

If you are replacing the RC Gate, click "Installation Completed" in the section area after this step, and then click [OK] to complete the replacement.

RTB 3: Important Notice about Registering SNMP Devices
RTB 4: Set the RC Gate A2 and devices with the same encryption level when registering

Registering Devices (MFPs/Printers)

Device Registration Flow

Important

- If the SNMP access account of the device has been changed, change the SNMP access account setting of the RC Gate A2 before adding the device. See page 117 "About Access Accounts" for details.

1. Configure [Permit @Remote Task Performance], [Auto Discovery], and [SNMP Access] if necessary.
2. See page 39 "Discovering Devices with [Broadcast]" or page 41 "Discovering Devices with [Network Search]" and search for devices on the network.
3. See page 44 "Device Registration" and register discovered devices.

Discovering Devices with [Broadcast]

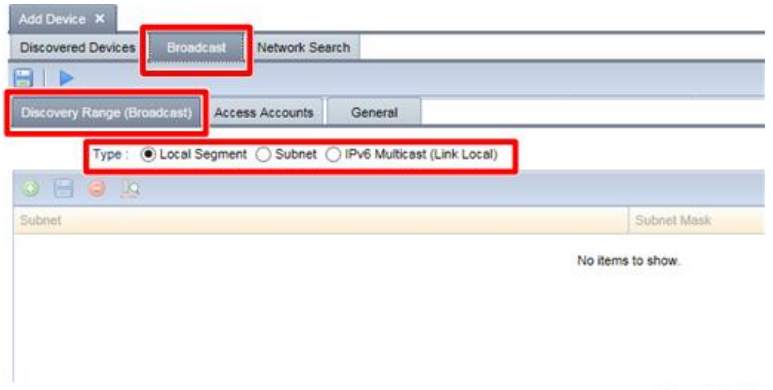
1. Click [Add Device].

   The location of [Add Device] in the section area differs depending on whether installation has been completed or not.

Before completion	After completion
	
d3ara3038	d3ara3039

2. Click the [Broadcast] tab, and then click the [Discovery Range (Broadcast)] tab.

3. **Select the [Type].**



d3ara3040

- When selecting [Local Segment] or [IPv6 Multicast (Link Local)], proceed to step 7.
- When selecting [Subnet], proceed to step 4.

4. **Click (Add) in the list area.**

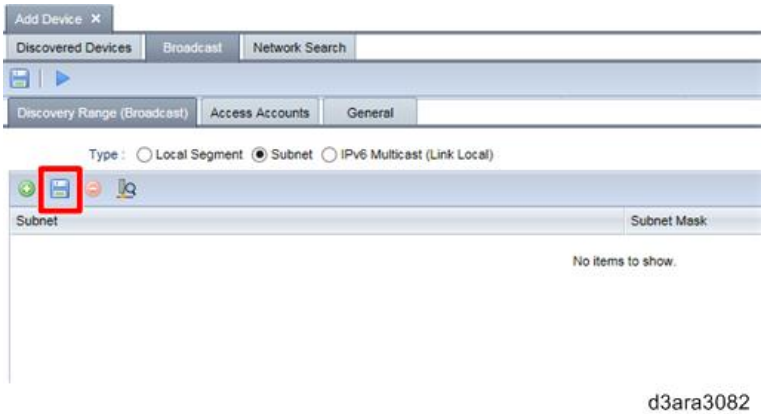
5. **Specify the search conditions.**

Item	Description
Subnet	Enter the subnet address of the broadcast. An IPv4 address can be specified.
Subnet Mask	Enter the subnet mask of the broadcast. An IPv4 address can be specified.

Note

- Click to save the settings as a CSV file.
- Click to import settings saved as a CSV file.

6. **Click the lower (Save) button.**



d3ara3082

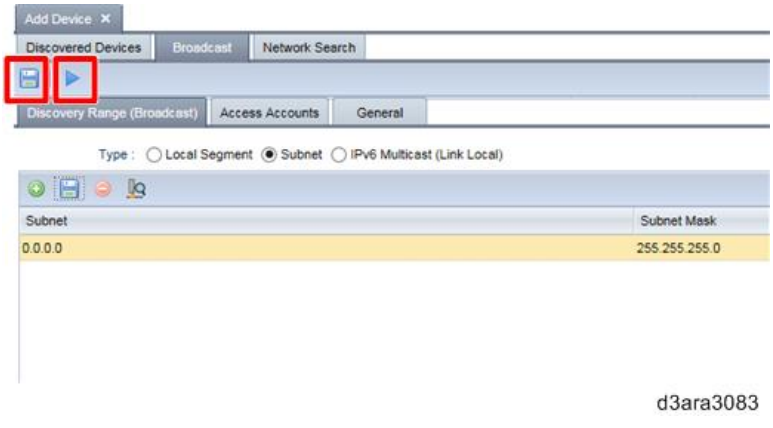
7. **Configure other settings if necessary.**
   - [Access Account] tab

     Set an account used for access to devices at the time of discovery. Change the account to be used from [Not Assigned Accounts] to the [Assigned Account] list by clicking the [▲] [▼] button or by dragging and dropping.
   - [General] tab

     If [Reverse DNS Lookup] is enabled, the machine attempts to determine the host name of the device whose address has been detected. If the attempt fails, only the device address appears.

Item	Description
Reverse DNS Lookup	Select this to enable [Reverse DNS Lookup] to determine device host names.

8. **Click the upper (Save) button, and then click (Immediately perform).**



   Discovery starts. Discovered devices appear in the [Discovered Devices] tab.

9. **See page 44 "Device Registration" and register the devices.**

Discovering Devices with [Network Search]

1. **Click [Add Device].**

   The location of [Add Device] in the section area differs depending on whether installation has been completed or not.

Before completion	After completion
	
d3ara3038	d3ara3039

2. **Click the [Network Search] tab, and then click the [Discovery Range (Network Search)] tab.**

d3ara3041

3. **Click (Add) in the list area.**
4. **Specify the search conditions.**

d3ara3050

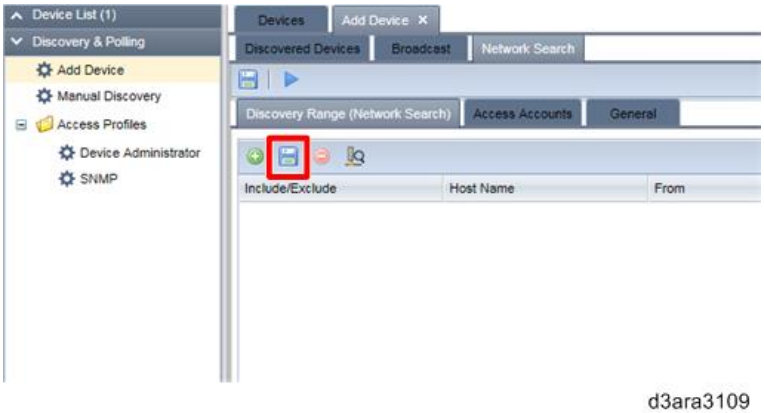
Item name	Description
Include/Exclude	Specify whether to include or exclude a specified range in the network search.

Item name	Description
Range Type	Select [One Host Name], [One IP Address], [Specify IP Range], or [IPv6 Address].
Host Name	Specify this setting only if [Range Type] is set to [One Host Name]. Use 1 to 255 characters.
From	Enter the discovery target IP address or IPv6 address, or the start IP address in the case of a discovery target IP address range.
To	Enter the end IP address of the discovery target IP address range.
Subnet Mask	Enter the subnet mask in the IP address range specified by [From] and [To].

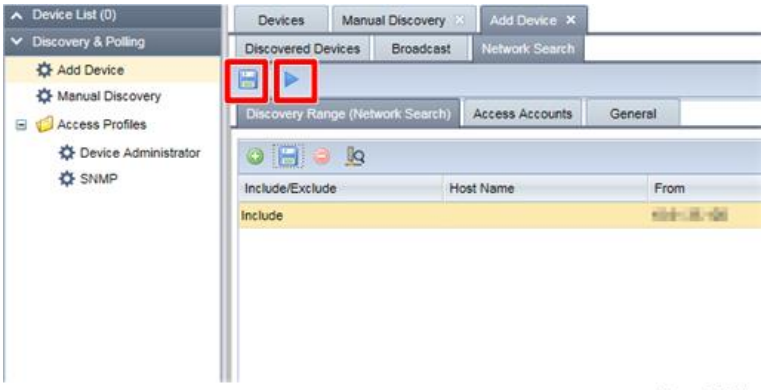
Note

- Click to save the settings as a CSV file.
- Click to import settings saved as a CSV file.

5. **Click the lower (Save) button.**



6. **Click the upper (Save) button, and then click (Immediately perform).**



d3ara3051

Discovery starts. Discovered devices appear in the [Discovered Devices] tab.

7. **See page 44 "Device Registration" and register the devices.**

Device Registration

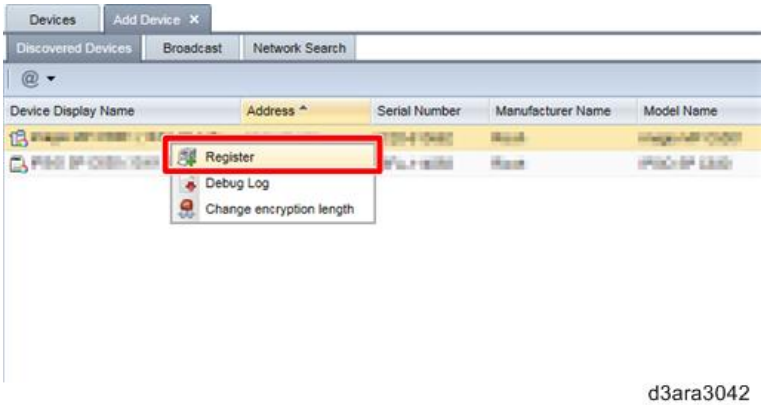
1. **See page 39 "Discovering Devices with [Broadcast]" or page 41 "Discovering Devices with [Network Search]" for details on how to discover the device(s).**

Note

- If a device does not appear in the [Discovered Devices] tab, click (Refresh).
- Discovery may take a long time if the search range is large.

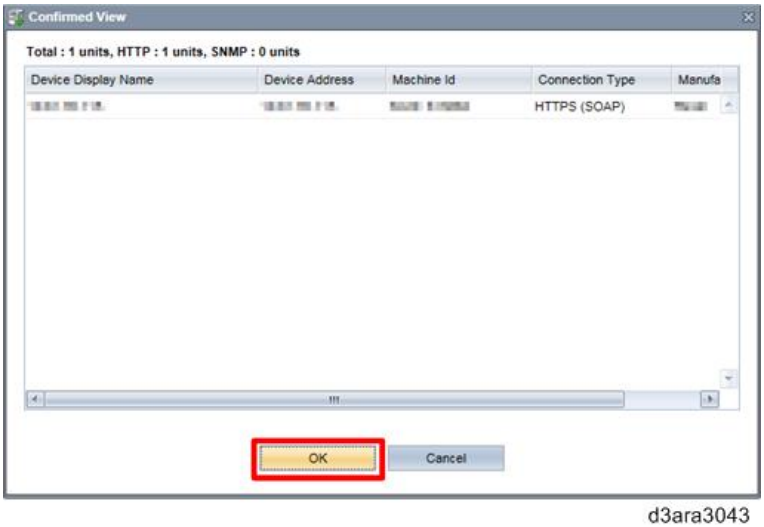
2. **In the [Discovered Devices] tab, right-click on the device you want to register, and then click [Register].**

You can also register by clicking the (@Remote) icon in the list area.



d3ara3042

3. **Check that the device to be registered appears in the [Confirmed View] display that appears, and then click [OK].**



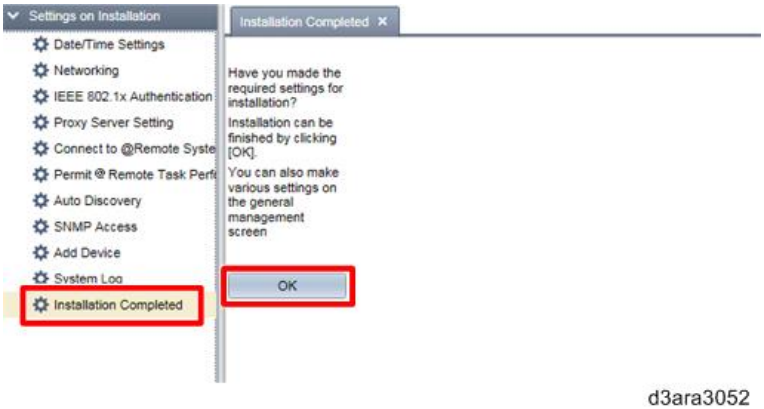
d3ara3043

4. **Click [OK] in the [Registration Result] dialog.**

Note

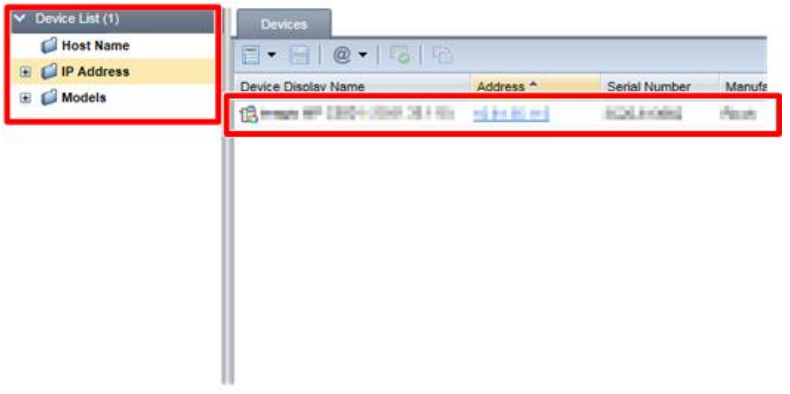
- Registered devices disappear from the list area when you click (Refresh).

5. **When all devices have been registered, click [Installation Completed] in the section area, and then click [OK].**



d3ara3052

6. **After completing installation, check the [Device List] to make sure all registered devices are displayed.**



d3ara3084

⚠CAUTION

- If the Device Administrator account setting of a device has been changed from the default setting, change the account setting on the RC Gate A2 accordingly.
- Inform the customer of the fact that this is required whenever the Device Administrator account is changed.
- See page 117 "About Access Accounts" for details.

Note

- Device information is not updated automatically. The information obtained during device registration or during the last polling is displayed. If you want to check the current status, execute polling (see page 72 "How to Check the Status of Communication with the Imaging Device").

Replacement/Migration

Important

- **When replacing one or more RC Gate BN1/BM1 units, the replacement function works only when the version of RC Gate BN1/BM1 is 3.50 or higher. If the version of RC Gate BN1/BM1 is lower than 3.50, update the firmware to version 3.50 or higher. Otherwise, install RC Gate A2 as a new appliance, without performing the replacement and migration procedures.**
- **When Appliance Replacement must be performed, please avoid doing it on the M/R Date and one day prior to the set M/R Date in order to receive and send closing counter data correctly. For example, if the M/R Date is set as the 20th, appliance replacement should not occur on either June 19 or June 20.**

Note

- You can replace RC Gate A2 (with the storage option) with RC Gate A2 (without the storage) if the number of managed devices are 100 or smaller.

Preparation for Visiting the Customer Site

Before visiting the customer site, contact the @Remote Center and do the following to get a Request No.

1. **Inform the @Remote Center of the serial numbers of the old RC Gate and the new RC Gate.**
2. **Check the number of managed devices.**
3. **Check whether the Accounting Report option is used.**

Items required when replacing the RC Gate

1. A micro-USB cable
2. Request number (for replacement)
3. RC Gate A2
4. RICOH Remote Communication Gate A2 Storage 1000 (SD card) (if the number of managed devices exceeds 100)

Note

- You can replace RC Gate A2 (with the optional SD card) with RC Gate A2 (without the optional SD card) if the number of managed devices are 100 or smaller.

Replacement

1. **Start the web browser of the computer.**

2. **Enter "http://192.168.10.153:8080/index.html" in the address bar.**
3. **The login window of the RC Gate A2 appears on the screen. Check the LED display to make sure that RC Gate A2 has been started up completely. Enter [User Name] and [Password]. Select the display language in [Language], and then click [Login].**

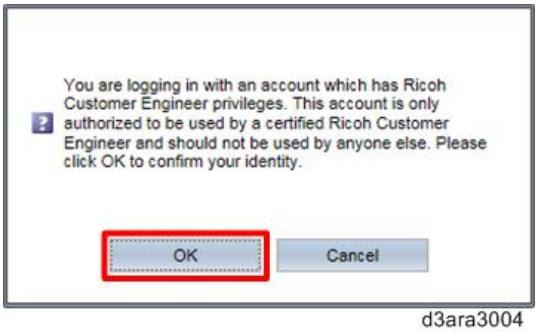
d3ara2006

User Name: RicohAtRemoteOperator

Note

- User Name can not be changed.

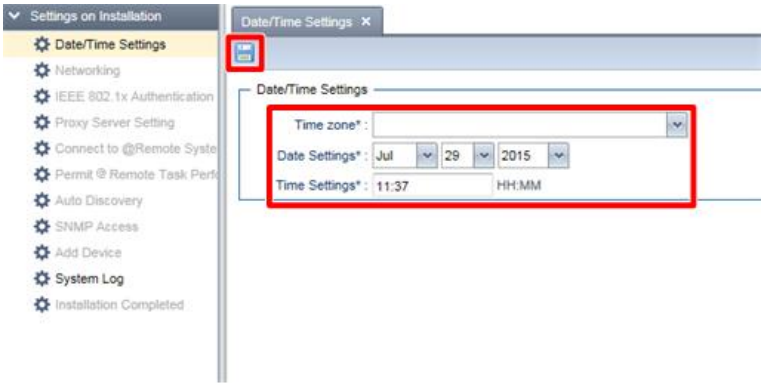
4. **When this confirmation message appears, click [OK].**



d3ara3004

5. **When [Settings on Installation] appears, select the area in which the RC Gate A2 is installed from the [Time zone] pull-down menu. Make sure the date and time are set correctly, and then click (Save).**

   You cannot start configuring the [Networking] settings until you click (Save).

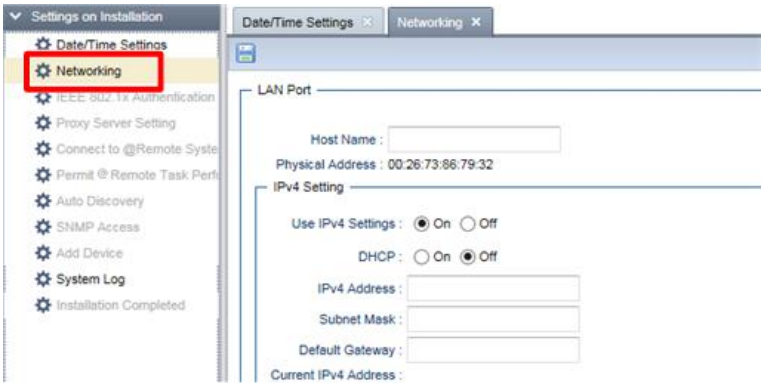


d3ara3005

Note

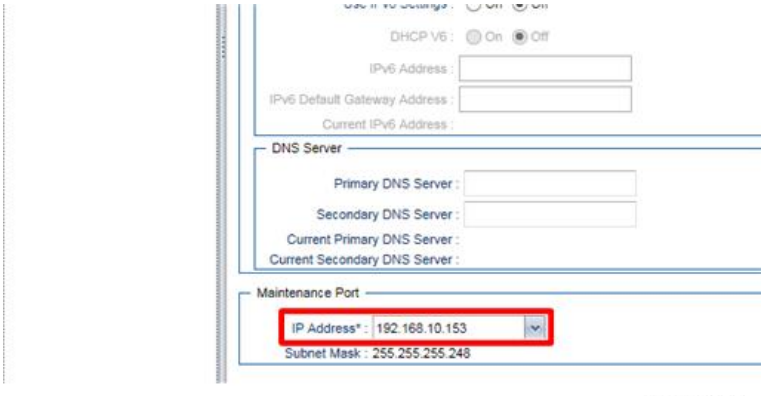
- About Daylight Saving Time
  RC Gate A2 supports Daylight Saving Time (DST) and changes the time displayed on the browser screen and the time at which a task is executed. Whether or not Daylight Saving Time is applied and the implementation period depends on the selected time zone and country or region.
  When the time changes at the beginning or the end of Daylight Saving Time period, tasks are executed as follows:
- Example: When 2:00 becomes 3:00 in local time
  - A task scheduled at 2:00: Will be skipped.
  - A task scheduled at 2:30: Will be skipped.
  - A task scheduled at 3:00: Will be executed at 3:00.
- Example: When 3:00 becomes 2:00 in local time
  - A task scheduled at 2:00: Will be executed again at the second 2:00.
  - A task scheduled at 2:30: Will be executed again at the second 2:30.
  - A task scheduled at 3:00: Will be executed at 3:00.

6. **Click [Networking].**



d3ara3006

7. **Ask the customer whether the IP address of the micro-USB port is being used in the LAN environment of the customer site. If it is being used, change the [IP address] under [Maintenance Port] to an IP address that is not being used.**



d3ara3007

Note

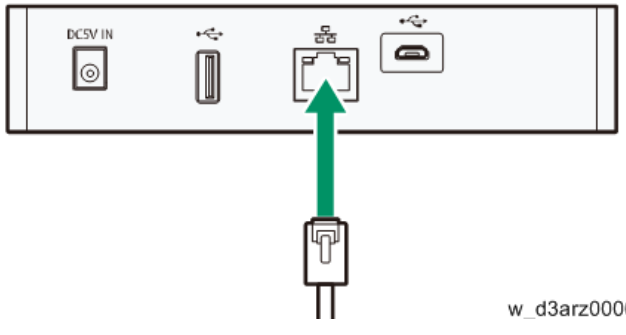
- To avoid an IP address conflict with another device on the customer network, the IP address of the [Maintenance Port] can be changed. The IP address must be "192.168.nnn.153", and any number between 1 and 254 can be selected for "nnn". (Default: 10.)
  Be careful when specifying the address, because the addresses that may conflict with customer devices change depending on the maintenance port address.

Maintenance Port IP Address	IP addresses that may conflict with a device on the customer network
192.168.1.153	192.168.1.152 to 192.168.1.159
192.168.2.153	192.168.2.152 to 192.168.2.159

Maintenance Port IP Address	IP addresses that may conflict with a device on the customer network
:	:
192.168.10.153	192.168.10.152 to 192.168.10.159
:	:
192.168.254.153	192.168.254.152 to 192.168.254.159

- Devices on the customer network with the same network address as the Maintenance Port IP address (192.168.xxx.153) cannot be recognized by the RC Gate A2. Because the Subnet Mask is 255.255.255.248 (prefix length /29), the following IP addresses have the same network address as the Maintenance Port IP address: 192.168.xxx.152 through 192.168.xxx.159.
- The IP address of the computer is assigned by DHCP. The assigned IP addresses are reset after one day. If more than five computers are connected to RC Gate A2 within the reset period (one day), assignable IP addresses will be exhausted and network connection will not work properly. IP addresses can be assigned again after you turn the RC Gate A2 off and on.

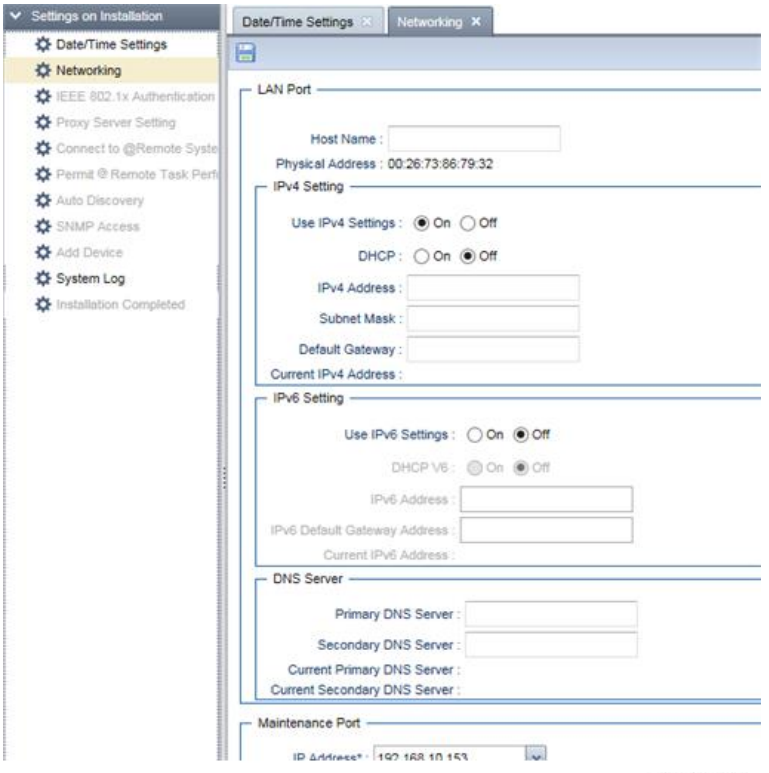
8. **Connect the network cable to the LAN port of RC Gate A2.**



Connect this appliance to the network with the supplied network cable. You can use 10BASE-T, 100BASE-TX or 1000BASE-T network cable instead of the supplied cable. When connecting to the network via a 100BASE-TX or 1000BASE-T network cable, use a Category 5 or higher cable.

9. **Connect the other end of the cable to a hub on the customer's network.**
10. **In [Networking], specify settings for the [LAN Port] group. When using DHCP, select [On].**

When not using DHCP, enter the address directly.



Note

- IPv6 stateless address auto configuration (which means that a router assigns the first part of the address (prefix) to a device) is always enabled. It cannot be disabled.
- After you change the DNS configuration, you must restart the RC Gate A2.

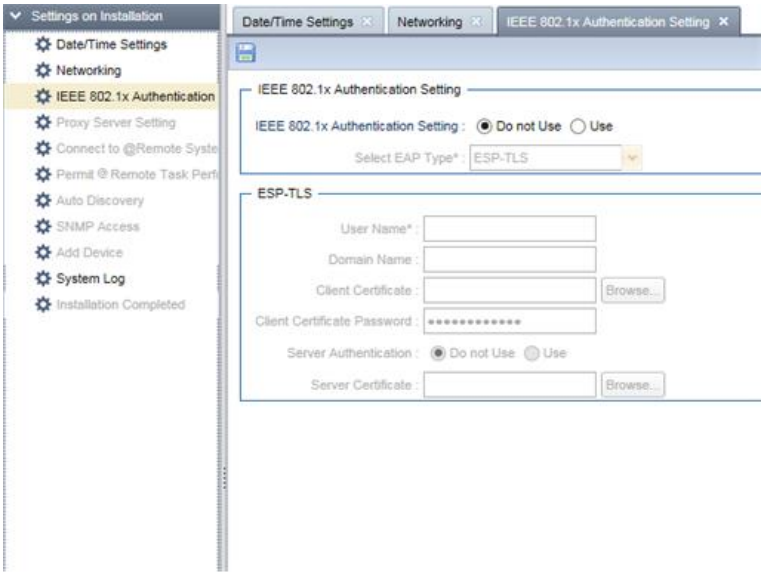
11. Configure the DNS Server settings. (Required)

12. Click (Save).

13. Click [IEEE 802.1x Authentication Setting].

14. If IEEE802.1x Authentication is to be used, select [Use] and configure the required settings.

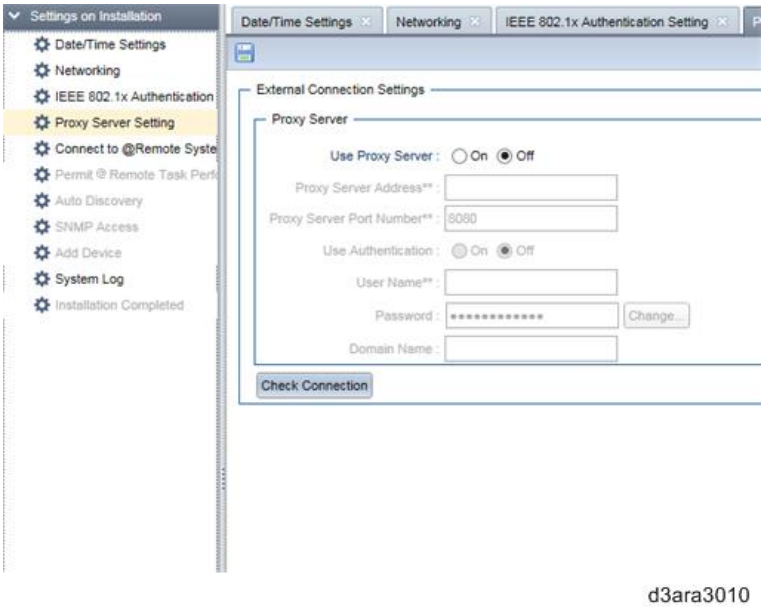
15. Click (Save).



d3ara3009

16. If a proxy server is to be used, click [Proxy Server Setting].

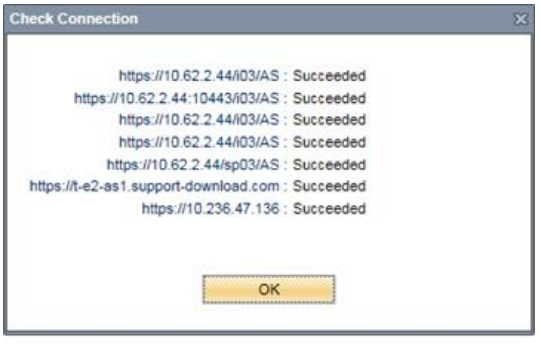
Set "Use Proxy Server" to [On]. Configure other settings as required, and then click (Save).



d3ara3010

Note

- By clicking [Check Connection], you can check whether the RC Gate A2 can connect to the @Remote system servers.



d3ara3011

- When connection fails, see page 75 "How to Check Connection with Related Servers" and take the required action.

17. Click "Connect to @Remote System".

18. Enter the request number and click [Register].

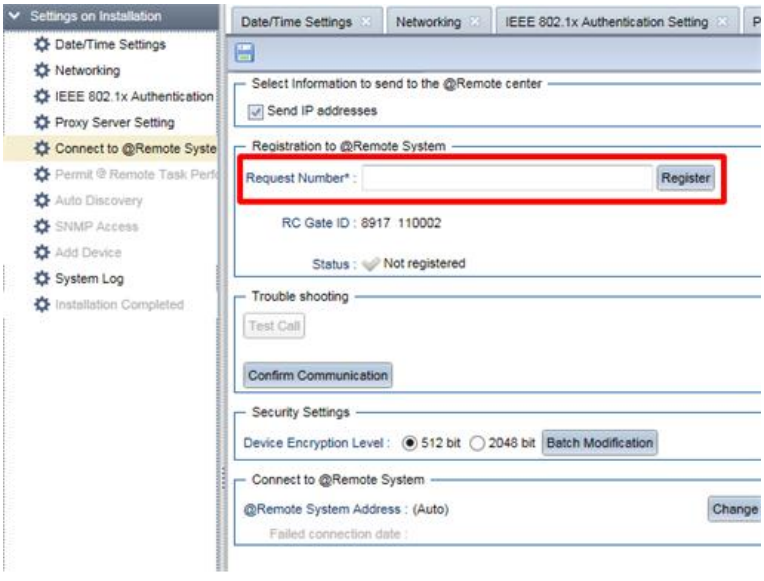
For your interest, this is how the @Remote Center generates the request number. You do not have to do this yourself.

- Use the serial number of the old RC Gate A.
- Put a "#" at the beginning.
- Put 6 spaces in between the 3 digit-prefix and the remaining digits.

Example 1:

When RC Gate XX (V7800000010) is replaced with RC Gate YY (V7800000020), the Request Number will be #V78_____00000010.

Old Appliance S/N (RC Gate XX):	V78_____00000010
New Appliance S/N (RC Gate YY):	V78_____00000020
Request number to be input in RC Gate YY:	#V78_____00000010



19. **"Register is succeeded." appears and "Status" changes to "Registered".**

Note

- Configure "Troubleshooting", "Security Settings", or "Connect to @Remote System" if necessary.
- To use this appliance in a CC-certified environment, select [2048 bit] for [Device Encryption Level] in "Security Settings".
  Note: The devices must be capable of handling 2048 bit encryption.

20. **Click "Installation Completed" in the section area, and then click [OK] to complete installation.**
21. **Check the device list and other settings to see if they have been taken over successfully.**

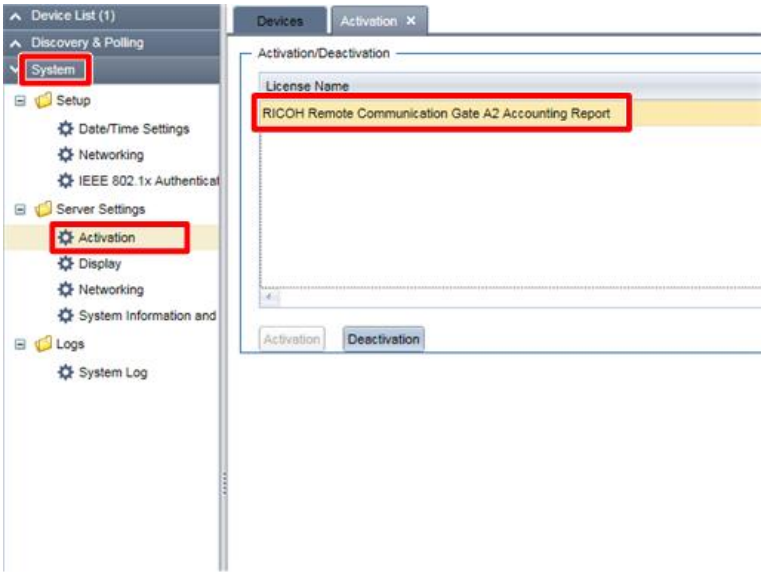
Replacement of the Accounting Report Option

When replacing an RC Gate A2 (with the Accounting Report function activated) with a new RC Gate A2, the RC Gate A2 communicates with the eDC Server, and deactivation of the Accounting Report function of the old RC Gate A2 and activation of the Accounting Report function of the new RC Gate A2 are automatically done.

After replacement is completed, check the activation status of the Accounting Report function.

1. **Click the [System] section.**
2. **Click [Activation] under [Server Settings].**

3. **Check if the activated license is displayed in the [Activation/Deactivation] list.**



d3ara3120

4. **Check if the Accounting Report function is also activated on the @Remote Center side.**

   * If automatic deactivation/activation fails, see page 88 "When an Error Occurs during Activation or Deactivation of Accounting Report Option".

⚠CAUTION

- Save the following information shown in the error message.
  License code, product key, URL, and lock code.

Operation Check

Sending a Test Call from a Device

1. **Press [User Tools/Counter].**
2. **Select [System Settings].**
3. **Select [Administrator Settings].**
4. **Press [Service Test Call]. (This key is added to the Administrator Settings when installation of the RC Gate is completed.)**
5. **Press [Start].**

   If "Service test call successfully completed." appears, communication is established successfully.

Accounting Report Test

You can test the Accounting Report function on a specified device. This test can be performed even if the Accounting Report function is not activated. It can also be performed on devices that are not the target devices of the Accounting Report function.

1. **Select one device in the Device List.**
2. **Click (Accounting Report Collection Test).**

d3ara3069

If the test ends successfully, "Succeeded to retrieve the counter per user" appears.

If the test fails, "Failed to retrieve the counter per user" appears.

Migration

Information of managed devices can be migrated from two or more appliances (RC Gate BN1/BM1/A) to one appliance (RC Gate A2).

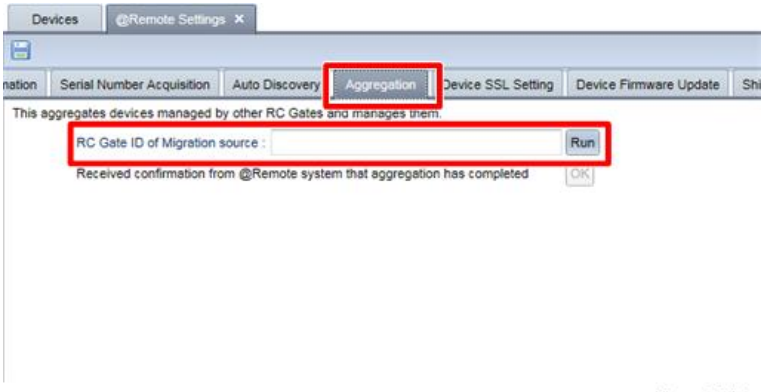
Note

- Only the information of managed devices will be migrated.
- All appliances must be registered at the same site. If there is an appliance that is registered at a different site, preparation on the @Remote Center side takes several days.
- Information cannot be migrated from an appliance on which sending IP addresses to the @Remote Center is disabled.
- Migration from RC Gate A2 to RC Gate A2 is not supported.

1. **From among the migration sources, select one appliance as the main source and execute page 47 "Replacement".**

   The configuration (Auto Discovery range, server settings and other settings) of this appliance will be taken over to the new appliance.
2. **Configure migration in the @Remote Center GUI.**
3. **If the source is a RC Gate BN1/BM1, shut it down. If the source is a RC Gate A, shut it down or disconnect it from the network.**
4. **Click [@Remote].**
5. **Click [@Remote Settings].**

6. **Click the [Aggregation] tab.**
7. **Enter the Request number in the text box, and then click [Run].**



d3ara3014

8. **When communication with the @Remote Center is finished, click [OK] (it is not clickable until communication is finished).**

   Information of managed devices are migrated from the migration sources to the new RC Gate A2, and the IP address of the new RC Gate A2 is registered in the managed devices.

9. **Repeat steps 2 through 8 as many times as the number of migration sources.**

Note

- With RC Gate A2, the maximum number of managed devices is 100 (without the optional memory) or 1000 (with the optional memory). If the remaining space for devices in the RC Gate A2 is smaller than the number of managed devices in the migration source, migration will not be performed. For example, if 50 devices have already been migrated to the RC Gate A2 (without the option) and you try to migrate from a RC Gate BN1 on which 100 devices are managed, migration will be cancelled.

Storage Option

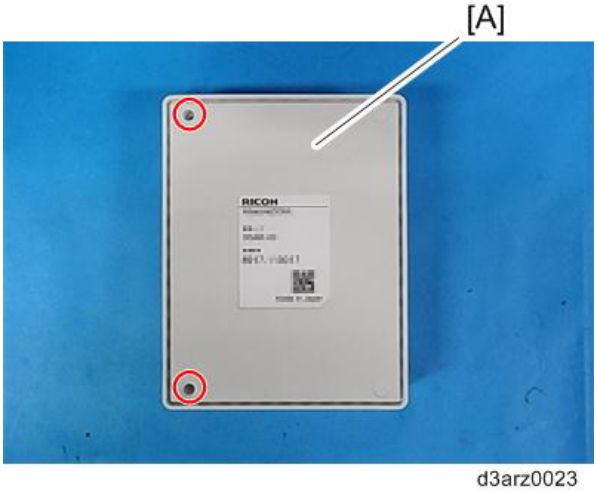
Components Check

RICOH Remote Communication Gate A2 Storage 1000

Description	P/N	Q'ty
OPTION:D3AX-01:WLD:GER	D3AX-0001	1

Storage Option Installation Procedure

1. **Unplug the network cable and the power cord.**
2. **Remove the cover [A]. (x2)**



d3arz0023

Important

- **Remove the cover to which the rating plate is attached. (Opening the other side may cause the power button to be damaged.)**

Note

- The cover is fixed with three hooks. Insert a jeweler's screwdriver to lift it.

d3arz0025

3. **Insert the SD card into the expansion slot [A].**

d3ara0003

4. **Turn on the RC Gate A2.**

   If installation has been completed, it notifies the @Remote Center that the storage option is installed.

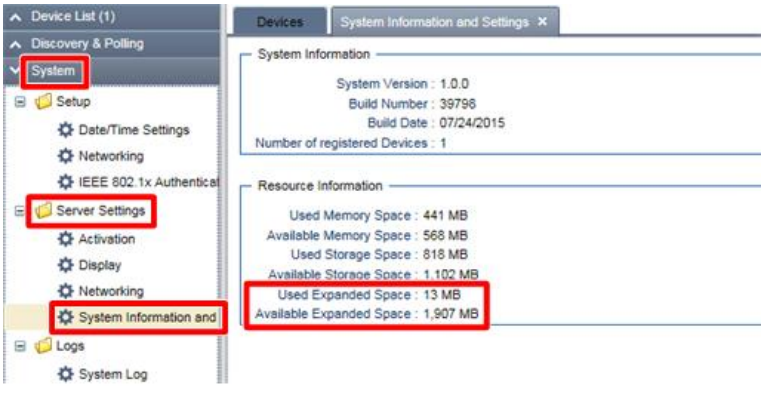
Note

- If there is a file on the storage option when the RC Gate A2 is turned on for the first time after installing the storage option, startup fails and the LEDs indicate "SD card error". See page 79 "LED Display".
- After you install the storage option and start up the RC Gate A2, the RC Gate A2 will not start up properly with the storage option removed.

Operation Check

1. **Log in using the CE account.**
2. **Click the [System] section.**
3. **Click [System Information and Settings] under [Server Settings].**
4. **If "Used Expanded Space" and "Available Expanded Space" are displayed under "Resource Information", the storage option is recognized correctly.**

   If the System Version is 1.0.0, these items will be displayed in English even if a different display language is selected.



d3ara3057

Note

- The size of whichever is smaller between "Available Storage Space" and "Available Expanded Space" is sent to the @Remote Center.

Accounting Report Option

Important

- **The Accounting Report option cannot be used in an IPv6 environment.**

Activate the Accounting Report option. The following conditions must be met before operation.

- The target RC Gate A2 has been registered at the @Remote Center.
- A product key has been purchased by the customer beforehand.
- You have informed the @Remote Center operator of the serial number of the devices on which the Accounting Report option will be used.

The following conditions must be met when using the option.

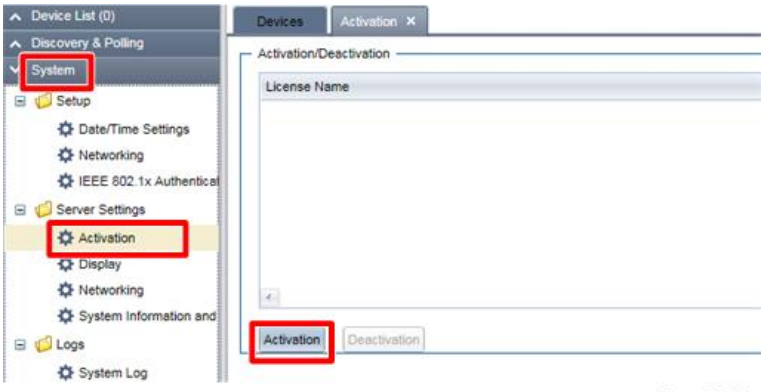
- The Device Administrator account information of each machine and the Device Administrator account information specified on the RC Gate A2 matches.

Note

- When replacing an RC Gate A that has the User Code Counter Capturing Option, activate the Accounting Report option in the same way as when installing a new RC Gate A2.
- When replacing an RC Gate A2 that has the Accounting Report option, activation information is automatically taken over. Therefore, the Accounting Report function can be used without re-activation.
- When doing the Replacement/Migration procedure, to migrate multiple appliances to a new RC Gate A2, the appliance in which the Accounting Report function is activated must be the one that is replaced first, before doing the migration of other appliances. Otherwise, the activation status is not reflected in the new RC Gate A2. This is because Accounting Report activation/licensing information is not copied over to the new appliance during the migration phase (only the device lists will be migrated).

1. **Click the [System] section.**
2. **Click [Activation] under [Server Settings].**

3. **Click [Activation].**



d3ara3045

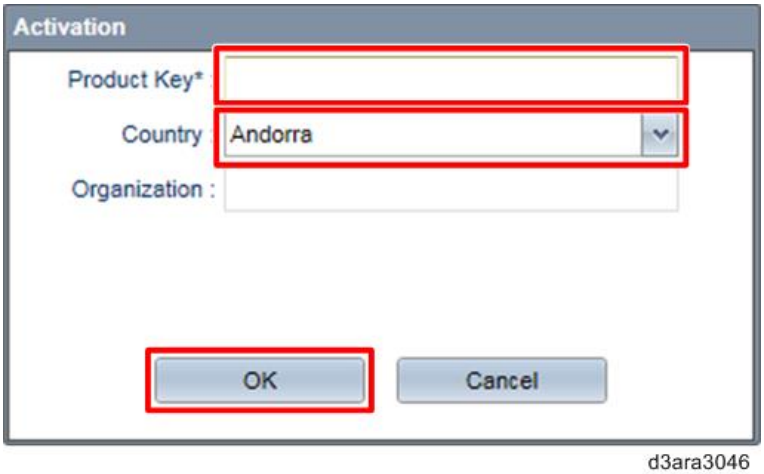
4. **Enter the product key.**

   Use one that has been purchased by the customer.

5. **Select an option from the "Country" pull-down menu.**

   Select where the RC Gate A2 is used. Activation will be done even if you do not select any option.

6. **Click [OK].**



d3ara3046

7. **Click [OK].**

d3ara3054

8. **Notify the Center operator that the activation of the Accounting Report option is done.**

Configuration for a CC-Certified Environment

To use this appliance in a CC-certified environment, configure it as follows.

Setting	Value
System] - [Setup] - [Date/Time Settings] - [Time zone]	Current zone
[System] - [Setup] - [Date/Time Settings] - [Date Settings]	Current Date
[System] - [Setup] - [Date/Time Settings] - [Time Settings]	Current time
[System] - [Server Settings] - [Networking] - [SSL] - [Use SSL]*1	[On]
[@Remote] - [@Remote Settings] - [Save Call/Counter History] - [S/MIME Setting]*1	[On]
[@Remote] - [@Remote Settings] - [Device SSL Setting] - [Use SSL]*1	[On]
[@Remote] - [@Remote Settings] - [Connect to @Remote System] - [Security Settings] - [Device Encryption Level]	2048 bit
[System] - [Server Settings] - [User Accounts] - [Access Accounts] - [Login password minimum length]*2	8 characters or more
[System] - [Server Settings] - [Networking] - [SSL] - [Disable HTTP]	Check the button
[@Remote] - [@Remote Settings] - [Permit @Remote Task Performance] - [Update System Firmware]*2	[Do not permit]

*1 These settings must be specified after the initial setting.

*2 These settings must be specified using a user account.

RTB 2
SSL3.0 setting must be added to the above table

Shutdown

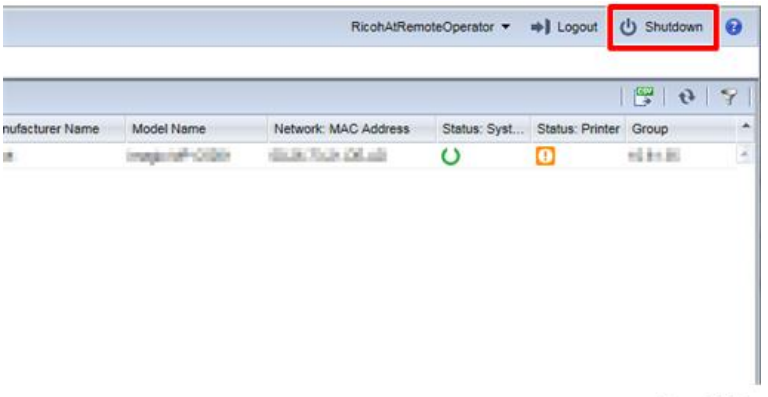
There are two ways to shut down the RC Gate A2.

Important

- If you unplug the power cord before the RC Gate A2 is shut down completely, the storage media may get damaged. If this happens, the latest 1 hour of log data may be lost. Always shut down the RC Gate A2 before unplugging the power cord. Make sure all LEDs are unlit when unplugging the power cord.

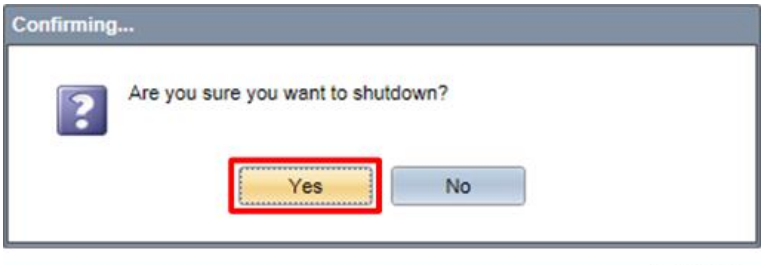
Shutdown from the browser display

1. In the header area, click [Shutdown].



d3ara3085

2. When the confirmation message appears, click [Yes].



d3ara3086

3. Wait until all LEDs are off, then disconnect the power cord.

Shutdown by pressing the Power button

1. Hold down the Power button for 4 seconds (until the red LED starts flashing).
2. Wait until all LEDs are off, then disconnect the power cord.

RTB 5: Information added

3. Maintenance of @Remote-Connected Devices

Maintenance of @Remote-Connected Devices

Maintenance Precautions

- If you do maintenance on a device that is connected to @Remote, make sure that you follow the procedures in this section before starting and after finishing.
- If you start work on an @Remote-connected device without turning off the @Remote function, service calls during maintenance will be sent to the @Remote Center and the jam alert count will increase.

Preparation before Starting Maintenance

Set SP5-816-002 (Remote Service: CE Call) to "0: Start of the service". The @Remote Center will be notified of the start time of maintenance and the @Remote function will be turned off.

When You Have Finished Maintenance

Set SP5-816-002 (Remote Service: CE Call) to "1: End of the service". The @Remote Center will be notified of the ending time of maintenance and the @Remote function will be turned on.

- Do not forget to do this after you have finished maintenance.
- If the value of SP5-816-002 is kept at "0", it will be changed to "1" after 4 hours. If maintenance is taking longer than 4 hours, set SP5-816-002 to "0: Start of the service" again.

4. Troubleshooting

Restoring Connection With the @Remote Center

When the @Remote Center cannot receive device information, connection must be restored using the procedure below.

How to Check and Restore Connection

1. Check the cable connection of the device.

1. **Check if the device is connected to a hub with a network cable.**
2. **Check if the hub and the router are turned on.**

2. Check the device configuration.

Check if the device is configured correctly as follows.

Item	SP No.	Value
I/F Setting	SP5-816-001	1 (CSS remote service on) 2 (@Remote service on)
Function Flag	SP5-816-003	1 (Enabled)
Regist: Status	SP5-816-201	0: Neither the @Remote device nor Embedded RC Gate is set. 1: The Embedded RC Gate is being set. 2: The Embedded RC Gate is set. 3: The External RC Gate is set. 4: The @Remote module has not started. An error has occurred.
RCG IP Address	SP5-821-002 (IPv4) SP5-821-005 (IPv6)	Check if the IP address of RC Gate is set.

3. Check if the device can connect to the RC Gate A2.

1. **Press the [User Tools/Counter] key.**
2. **Press [System Settings].**

3. **Press [Interface Settings].**
4. **Press [Ping Command].**
5. **Press [Change].**
6. **Enter the IP address of the RC Gate A2, and then press [#].**
7. **Press [Ping].**

   Check the result on the device's screen.

4. Check the conditions of the RC Gate A2.

1. **Check the status of the LED indicators. See page 79 "LED Display".**
2. **Check if the RC Gate A2 is connected to a hub with a network cable.**
3. **Check if the hub and the router are turned on.**

5. Check the settings of the RC Gate A2.

Ask the customer if the following settings have been changed after they were saved on the RC Gate A2.

- IP address for the RC Gate A2 / Subnet mask / Gateway address / proxy server address / port number / proxy ID and proxy password* (* if the proxy server requires an ID and a password)

If any of the settings above has been changed, change the settings on the RC Gate A2.

6. Check the communication between the RC Gate A2 and the device.

1. **Check if the device appears in the [Device List].**
2. **See page 72 "How to Check the Status of Communication with the Imaging Device" and check if the RC Gate A2 is communicating with the device properly.**

   If the RC Gate A2 is not communicating properly, proceed to step 3. If the RC Gate A2 is communicating properly, proceed to step 4.
3. **If the RC Gate A2 is not communicating with the device properly, check the following.**
   - Check if the IP address of the device which is displayed in the RC Gate A2 Monitor and the actual IP address configured on the device match. If they do not match, update the information. See page 94 "When the IP Address of a Device Stored on the RC Gate Does Not Change Automatically After the IP Address of the Device Changes" for procedure.
   - See page 77 "A LAN-Connected Device Is Discovered as an SNMP-Connected Device" and check if the ID2 code and the certificate are configured correctly.
4. **If the RC Gate A2 is communicating with the device properly, check the connection between the RC Gate A2 and the servers.**
   1. Click the [System] section.
   2. Click [Server Settings].

3. Click [Networking].
4. Click [Check Connection].

   If there is a connection failure, see page 75 "How to Check Connection with Related Servers".

7. Make a Service Test Call from the device.

Make a Service Test Call to confirm the connection between device and @Remote Center. See page 56 "Sending a Test Call from a Device" for procedure.

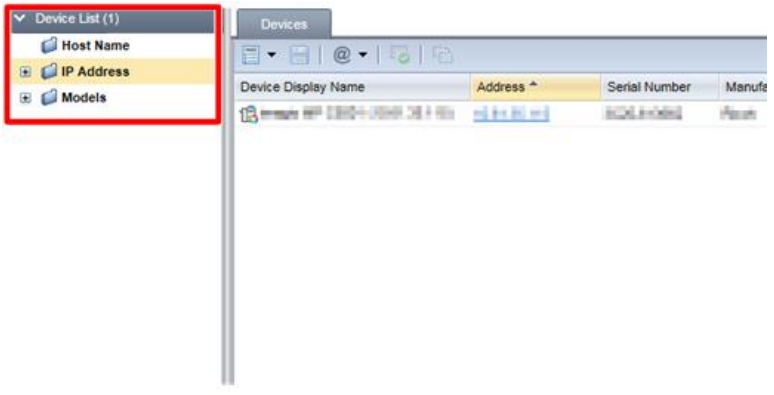
If the call is made successfully, restoration is completed.

If the call fails, the RC Gate A2 is assumed to be malfunctioning.

Contact the @Remote Center and replace the RC Gate A2.

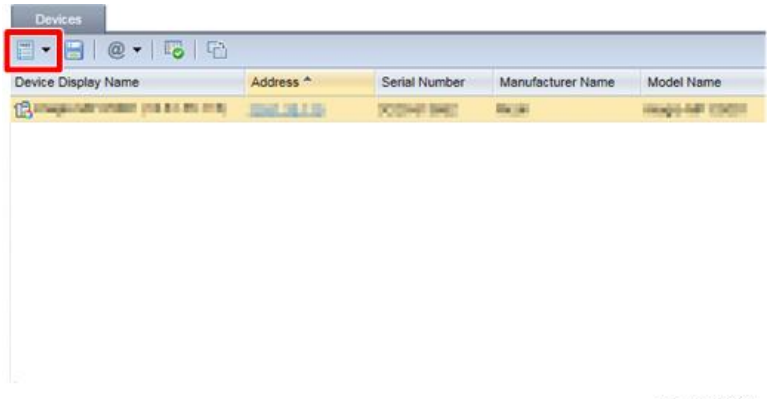
How to Check the Status of Communication with the Imaging Device

1. Log in as a CE.
2. In the [Device List] section, click a target group to display the corresponding device list.



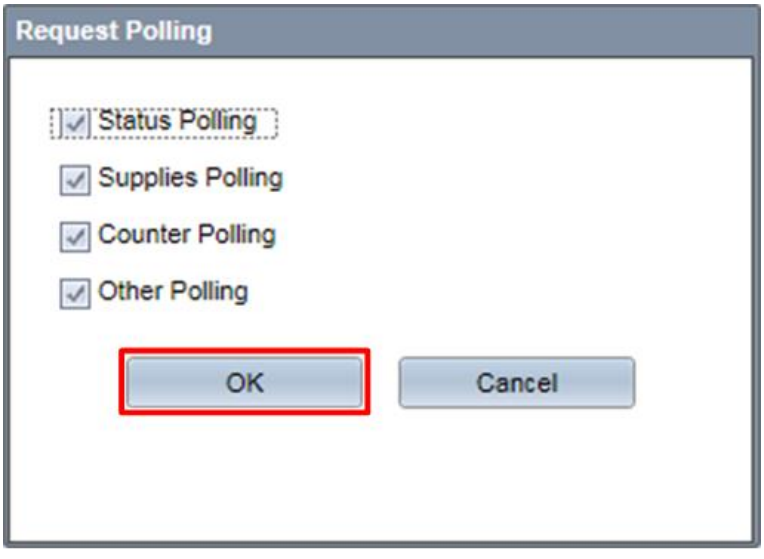
d3ara3087

3. Select a target device in the list area. Multiple devices can be selected.
4. Click (Menu) and select [Request Polling].



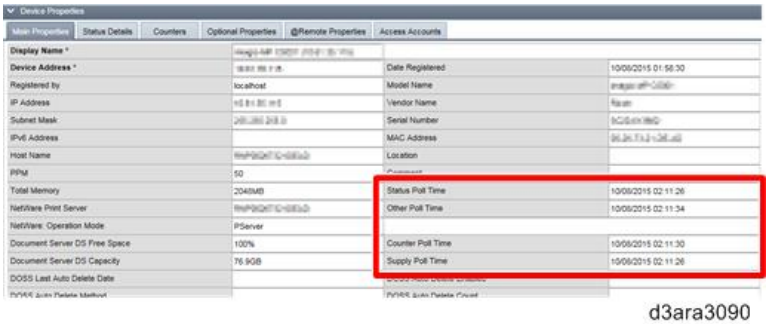
d3ara3088

5. When a dialog appears, click [OK].



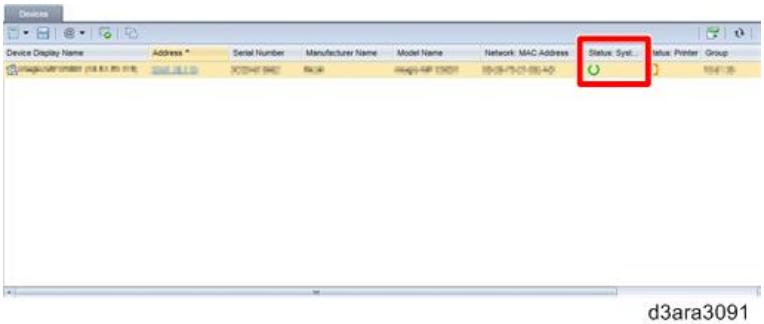
d3ara3089

6. Click (Refresh) in the upper part of the window, and then select the device. Check if the various Poll Time displays in the lower part of the window have been updated.



d3ara3090

7. Check the [Status: System] column of the device shows no problem.



d3ara3091

If the icon is displayed, check and restore connection with the device.

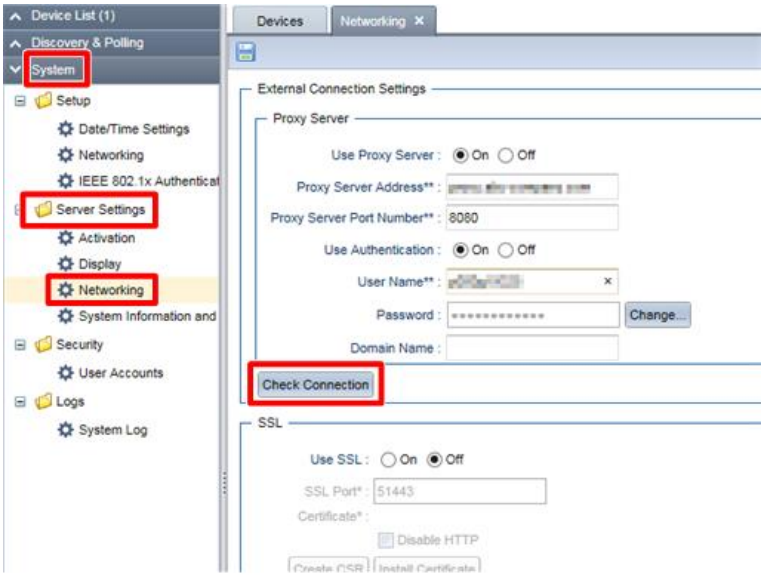
Note

- If all Poll Time displays except "Status Poll Time" are not updated, communication with the device is failing or the access account settings of the device and RC Gate A2 do not match.

How to Check Connection with Related Servers

You can check whether the RC Gate A2 can connect to the related servers.

1. **Start RC Gate A2 Monitor and log in as a CE.**
2. **Click the [System] section.**
3. **Click [Networking] under [Server Settings].**
4. **Click [Check Connection] in [External Connection Settings].**



d3ara3092

The check results are displayed.

d3ara3011

5. **Click [OK] to finish.**

Do the following if connection fails.

- Make sure that the network settings (IP address, subnet mask, gateway, DNS) are correct.

- Check the proxy server settings.
- If URL filtering is implemented on the customer network, ask the customer to allow communication with the displayed URLs.

Destination server	IPv4 address	IPv6 address
NRS Gateway (Center Server)	https://210.173.216.59/i02/AS	https://[2001:df0:467:a104:28d3:80d6:0:1021]/i02/AS
URL for sending Auto Discovery results	https://210.173.216.59/Auto/AS	https://[2001:df0:467:a104:28d3:80d6:0:1021]/Auto/AS
Rescue URL (for Device Certificate acquisition)	https://210.173.216.60/Rescue/AS	https://[2001:df0:467:a104:28d3:80d6:0:1023]/Rescue/AS
URL for sending Accounting Report data (eDC)	https://e2-as1.support-download.com	https://e2-as1.support-download.com
Global Server (SERES)	https://p-rfu-ds2.support.ricoh.com	https://p-rfu-ds2.support.ricoh.com
spGateway URL(for log acquisition)	https://210.173.216.61/sp02/AS	https://[2001:df0:467:a104:28d3:80d6:0:1025]/sp02/AS

A LAN-Connected Device Is Discovered as an SNMP-Connected Device

There are cases where the "Connection Type" of a discovered LAN-connected device is "SNMP" even though the device supports @Remote.

The "Connection Type" becomes "SNMP" in the following cases:

1. The ID2 code is not set in the device correctly.
2. There is a problem with the common certificate on the device (for example, it has already been registered with @Remote).

Action

1. Check the ID2 code setting.

   Execute SP5-990-002 to print the SP Mode Data List and check if the ID2 code (SP5-811-003) is set correctly.

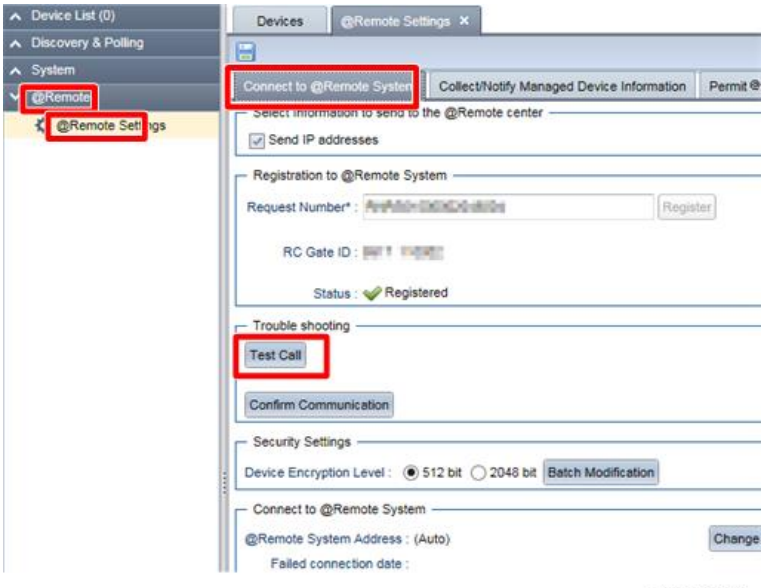
   - If the characters do not match, proceed to "2. ID2 code registration".
   - If the characters match, proceed to "3. Certificate configuration".

2. ID2 code registration

   Inform the @Remote Center operator of the "serial number of the RC Gate A2", "serial number of the device shown on the rating plate", "device IP address", and "device MAC address".

   Do the following as instructed by the @Remote Center operator.

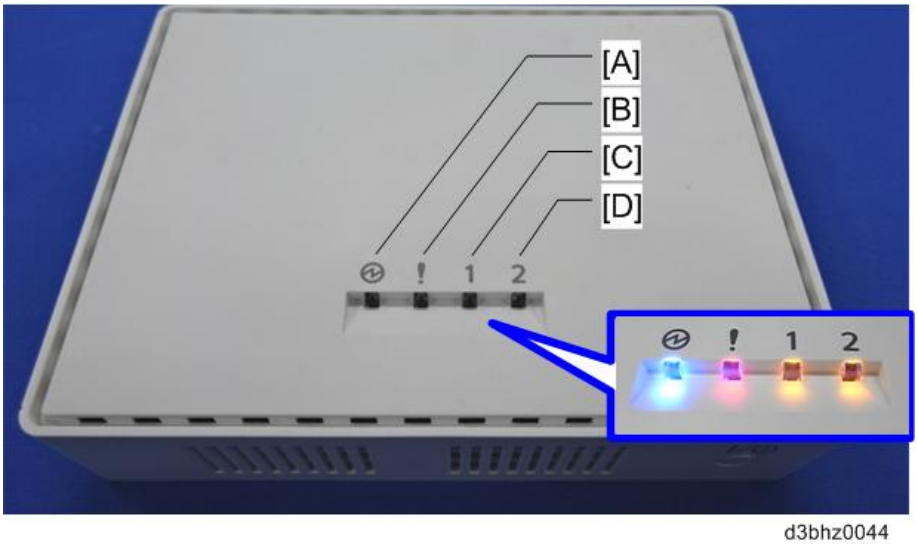
   Click [@Remote] > [@Remote Settings] > [Connect to @Remote System] > [Test Call].



3. Certificate configuration
    1. Check the encryption strength of the certificate [SP5-816-102 (1: 512 bits, 2: 2048 bits)].
    2. Initialize the certificate [SP5-870-003].
    3. Set an appropriate encryption strength for the certificate [512-bit: SP5-870-001, 2048-bit: SP5-870-004].
    4. Execute device discovery again.

LED Display

The RC Gate A2 has four LED lamps. This section explains the location of lamps and the LED patterns.

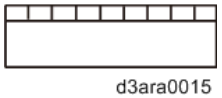
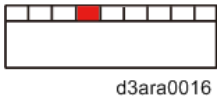


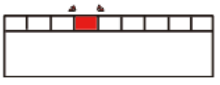
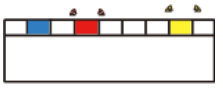
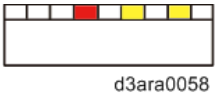
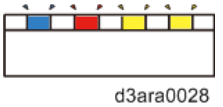
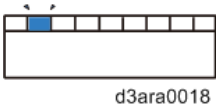
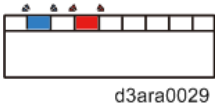
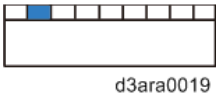
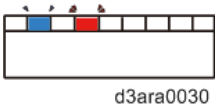
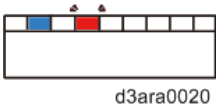
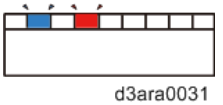
d3bhz0044

	LED name	LED indication	Color
[A]	LED(P)	Power	Blue
[B]	LED(E)	Alert	Red
[C]	LED(1)	Status 1	Yellow
[D]	LED(2)	Status 2	Yellow

: Flashes at one-second intervals.

: Flashes at 0.2-second intervals.

LED Pattern	Status	LED Pattern	Status
 d3ara0015	Power off (Standby)	 d3ara0021	The cable is disconnected or broken.
 d3ara0016	Power has just been turned on.	 d3ara0022	No usable IP address has been assigned.

LED Pattern	Status	LED Pattern	Status
 d3ara0064	SD card error: The inserted SD card is not valid. (Detected a file on the SD card when turned on for the first time after the insertion of the SD card.)	 d3ara0024	IEEE 802.1X authentication server error.
 d3ara0058	Starting up with the DIP switch turned on: Restoring the factory-default settings.	 d3ara0027	Recovering from an error.
 d3ara0017	Starting up the application.	 d3ara0028	Updating the system firmware.
 d3ara0018	Registration with the @Remote Center has not been completed.	 d3ara0029	System error persists even after restarting the RC Gate A2 the specified number of times.
 d3ara0019	Registration with the @Remote Center System has been completed and communication is established.	 d3ara0030	Restarting system
 d3ara0020	A communication error has occurred.	 d3ara0031	Shutting down

RTB 9: New pattern added

Error Codes

SC Codes

SC No.	Description
002	Insufficient Memory
200	Insufficient SD card capacity error
500	System Critical Authentication error
600	System Critical Communication error
700	System Critical Database error
901	System Critical Internal error

Please follow the recovery procedure below for all the above SCs.

1. Shut down the RC Gate A2 (see page 66 "Shutdown"), and then turn it on again.
   Go to the next step if this does not solve the problem (SC).
2. Execute page 47 "Replacement".

Other Errors

Check the error code and the solutions described below, and then check or correct settings.

* If "-" is shown in the "Solution" column, execute the following procedure.

1. Turn the appliance off and on.
2. Initialize the appliance.
3. Replace the appliance.

If changing the settings and replacing the appliance do not solve the problem, acquire the log and make an inquiry.

Error code	Description	Solution
107	You do not have the privileges to perform this operation.	1. Check the Access Account used for access to the device. 2. Check the Web Services account. 3. Check the SNMPv1/v2 community name. 4. Check the SNMPv3 account. 5. Check the privileges of the device administrator.
202	Communication timeout has occurred.	Check the network environment.
203	SSL communication is unavailable.	Check if the certificate is correctly configured.
300	An authentication error for the external system has occurred.	1. Check if the certificate is correctly configured. 2. Check if the license information is correct.
301	Unable to access external system.	Check the network environment.
302	Failed to send email. Verify email server settings and retry.	1. Check the network environment. 2. Check the settings of the mail server.
303	SMTP server authentication has failed.	1. Check the network environment. 2. Check the settings of the mail server.
304	Proxy authentication has failed.	Check if the authentication information for the proxy server is configured correctly.
305	Proxy connection has failed.	Check the proxy settings.
306	Failed to connect with the RICOH Software Server.	1. Check the network environment. 2. Check the network settings.
307	Unable to communicate with the RICOH Software Server.	Check if the appliance can communicate with the eDC server.
308	Communication with the RICOH Software Server has been interrupted.	Check if the appliance can communicate with the eDC server.

Error code	Description	Solution
313	SSL communication is unavailable.	Check if the certificate is correctly configured.
350	Other external system connection error.	Check the network settings.
400	Entered parameters are invalid.	Check if the specified information is correct.
401	The file format is invalid.	-
402	The file version is invalid.	-
403	The character code of the file is invalid.	-
404	Interrupted by user operation.	Wait a while and try again.
409	The file name already exists.	Specify a different file name.
410	There is a profile name conflict.	Check if the profile name is unique.
411	There is a name conflict.	Specify a different name.
500	Database authentication has failed.	-
501	Failed to access the database.	-
502	Failed to save data on the database.	-
503	Failed to read data	-
504	Failed to save the data.	-
550	Other data I/O error	-
601	Canceled because of system suspension.	-
604	The product key is invalid.	Check the entered product key.
650	Other system error.	-
700	Failed to save data	-

Error code	Description	Solution
701	Failed to save data	-
702	An unexpected error has occurred.	-
703	An unexpected error has occurred.	-
704	An unexpected error has occurred.	-
707	Running Tasks:Perform the process again later.	Wait a while and try again.
708	The DM Server cannot be reached. The task will execute when the service becomes available.	-
750	Other unexpected error.	-
801	Outside of regular office hours.	Try again during business hours.
802	Failed to obtain device information.	1. Wait a while and try again. 2. Check the network settings.
803	Failed to send message.	Wait a while and try again.
804	A hardware related error has occurred.	-
805	A database related error has occurred.	-
806	An error on the Center server side that does not have an error code has occurred.	-
807	An error on the appliance side that does not have an error code has occurred.	-
808	Bad file	-

Error code	Description	Solution
809	Cannot find the appliance in @Remote Center System.	Check the registration status at the @Remote Center. If there is a difference between the device lists of the @Remote Center and the appliance, initialize the appliance and then restore data from the Center.
810	The managed device does not exist in @Remote Center System.	Check the registration status at the @Remote Center. If there is a difference between the device lists of the @Remote Center and the appliance, initialize the appliance and then restore data from the Center.
811	There is no such data found in the database.	-
813	In operation.	Wait a while and try again.
814	The appliance or device has already been registered.	Check if the device or appliance has already been registered in the @Remote Center.
815	Cannot register device.	Check the Request Number and make a call to the Center.
816	This is a device that is already registered. Or Cannot register RC Gate with a device.	Ask the Center whether the device is registered.
817	Oversized data entry.	Check the specification of the entered information. Make sure it does not exceed the maximum size.
818	Parameter error.	1. Check if there is any incorrect or missing information. 2. Check the function flag of the device to see if it is not already "Enabled".
819	A property list item that does not exist has been specified.	-

Error code	Description	Solution
820	In the property list settings, an out of range or oversized value has been specified.	-
821	A property list item that cannot be set has been specified.	-
822	There was a connection system error.	Check the network settings.
823	The size of the restore file is larger than the size of the free space in the system.	Wait a while and try again.
824	The result has expired.	Wait a while and try again.
825	Email settings error.	1. Check if the mail server is configured. 2. Check if the administrator Email address is specified on the appliance.
826	The targeted schedule for cancelling does not exist.	Check the connection between the appliance and the device.
827	User cancellation.	Check the connection between the appliance and the device.
828	Cannot access targeted device.	1. Check the network settings. 2. Check the Access Account used for access to the device.
829	FTP login authentication failure	Check the connection between the appliance and the device.
830	FTP disconnected.	1. Check the connection between the appliance and the device. 2. Wait a while and try again.
831	A reply did not come back from the printing devices within a specified period of time.	1. Check the connection between the appliance and the device. 2. Wait a while and try again.

Error code	Description	Solution
834	The operation has been cancelled.	-
835	There was an operation timeout.	-
836	Timeout.	-
841	The connector id is not correct.	-
842	The device id in this notification and in the installation plan information differs.	Check the Request Number.
843	The format of the connector id invalid.	-
844	Received request number incorrect.	Check if the entered Request Number is correct.
845	A device is already registered with the same IP address.	Check the registration status at the @Remote Center. Initialize the appliance and install it again.
848	Communication test failed.	1. Check the network environment. 2. Check the network settings.
849	Exchange is not supported by the service site.	-
852	Corresponding data does not exist.	-
853	A CSS device has been specified as managed device.	CSS devices are not supported.
899	There was an unclassified error.	-
951	Internal network error	Check the network settings.
954	Function is not permitted.	Check the "Permit @Remote Task Performance" settings.
955	INTERNAL_PARSE_ERROR	-
1001	INTERNAL INVALID STATE	-
9801	Http Connection Error	Check if the certificate is correctly configured.

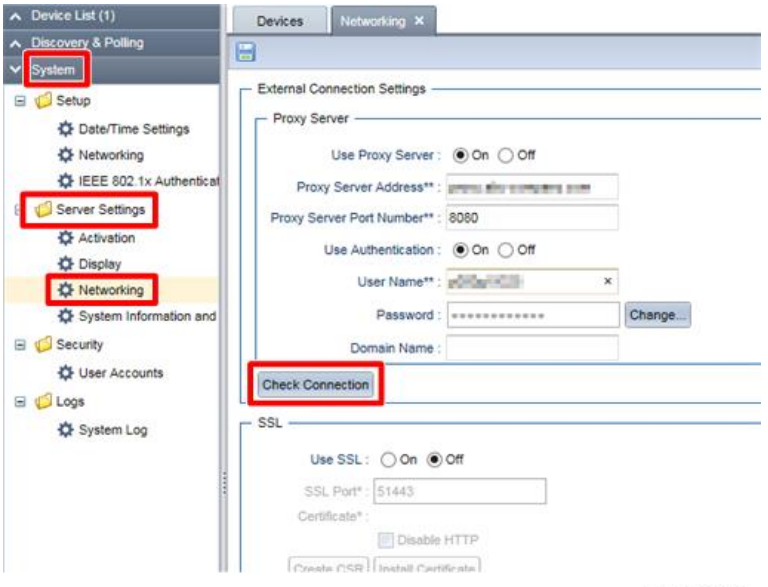
When an Error Occurs during Activation or Deactivation of Accounting Report Option

⚠CAUTION

- Save the following information shown in the error message.
  License code, product key, URL, and lock code.
- If you have closed the error message window before saving the information, check the system log immediately (because the contents of the system log are automatically deleted with time).
  Download the system log and search for the required information. Do not change the log collection level from the default setting (Warning level) because changing it may cause the required information to be not recorded.

If activation fails

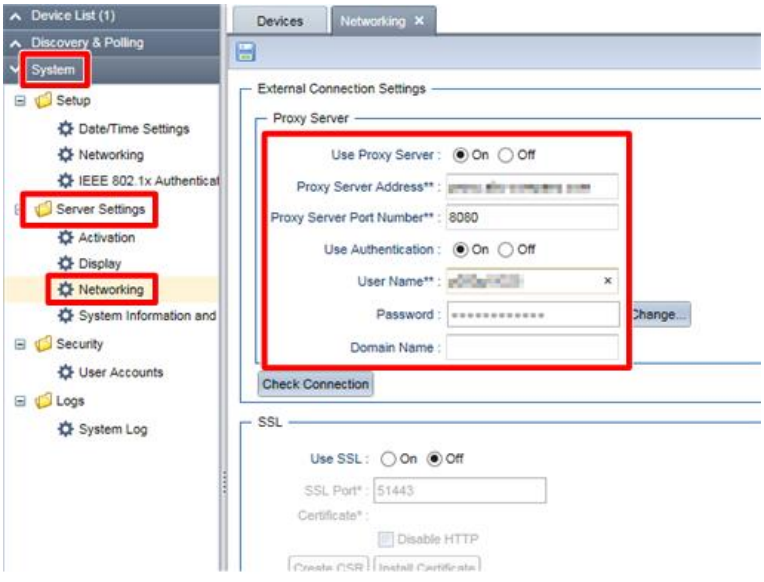
1. **Check the error code, and then check the following points.**
2. **Check if you entered the product key correctly.**
3. **Click [Check Connection] in the [Networking] screen and see if the RC Gate A2 can connect to the eDC server (see page 75 "How to Check Connection with Related Servers").**



d3ara3092

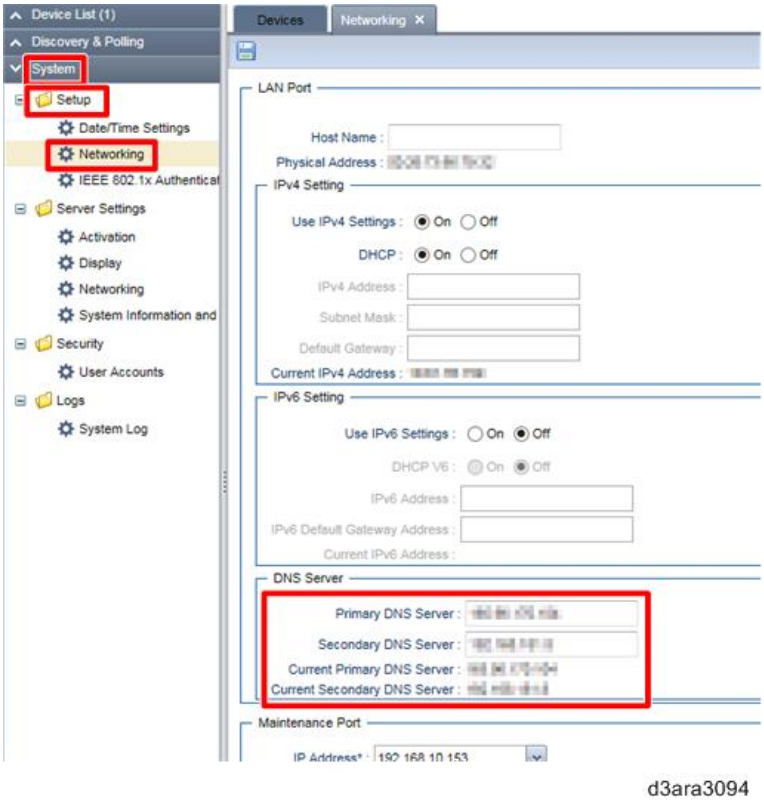
4. **Check if the IP addresses of the proxy server and the DNS server are correct.**

   [Proxy Server]: Click [System], and then click [Networking] under [Server Settings].



d3ara3093

[DNS Server]: Click [System], and then click [Networking] under [Setup].

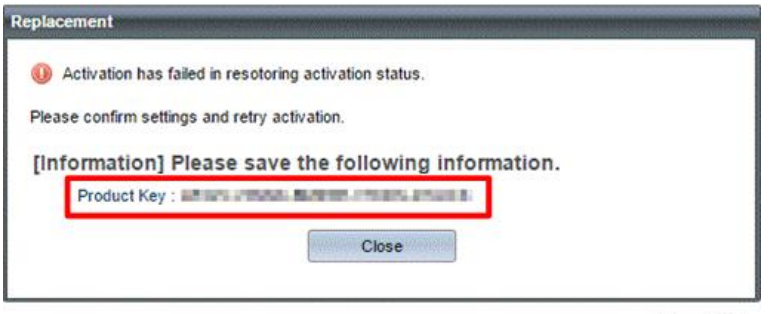


d3ara3094

5. **If URL filtering implemented on the customer network prohibits connection to the eDC server, ask the customer to allow such connection.**

If automatic activation fails (when replacing the appliance)

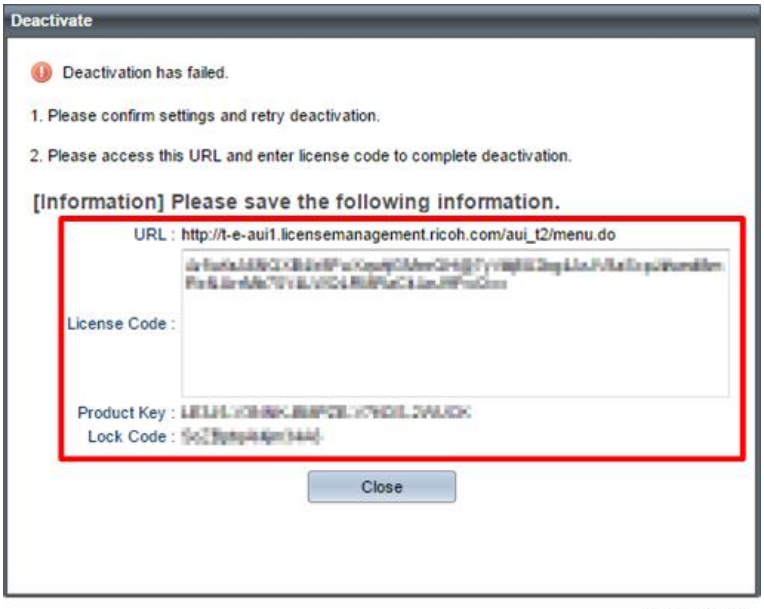
Perform activation using the product key displayed on the dialog (see page 62 "Accounting Report Option").



d3ara3095

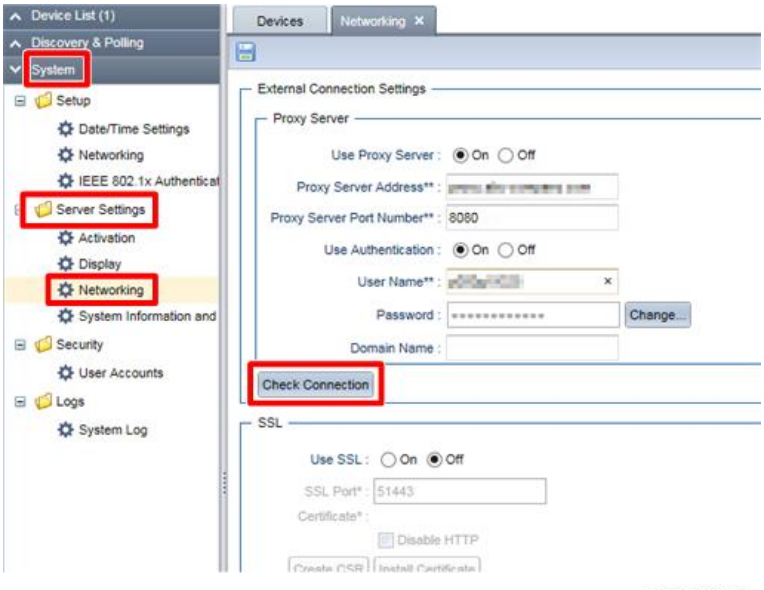
If deactivation or automatic deactivation (when replacing the appliance) fails

1. **Copy the following information shown in the error message, and save it on your computer.**
   - URL
   - License code
   - Product key
   - Lock code



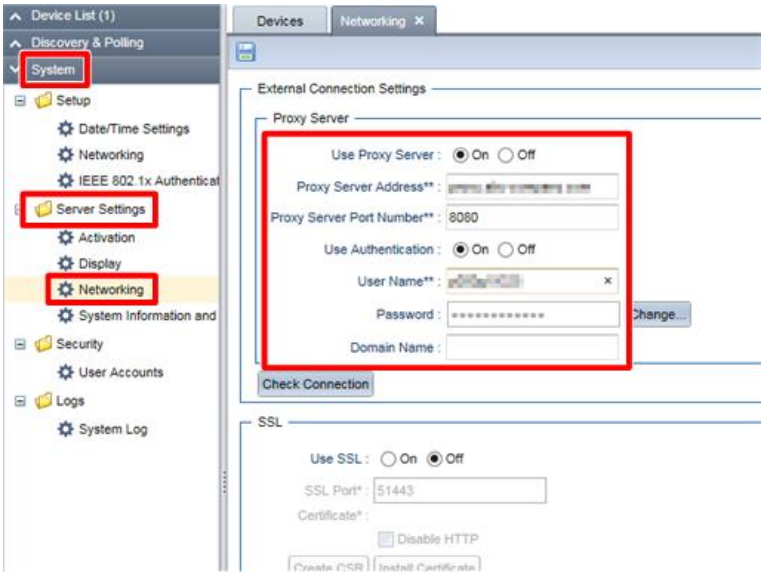
d3ara3032

2. Click [Check Connection] in the [Networking] screen and see if the RC Gate A2 can connect to the eDC server (see **page 75 "How to Check Connection with Related Servers"**).

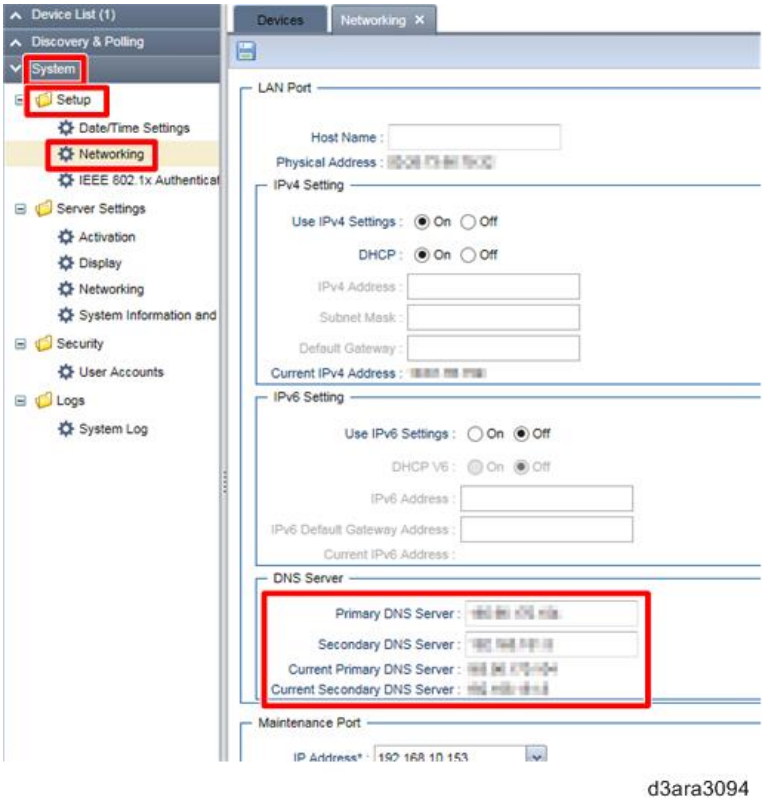


d3ara3092

3. **Check if the IP addresses of the proxy server and the DNS server are correct.**



d3ara3093



d3ara3094

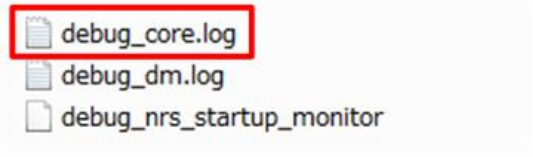
4. **Access the URL shown in the error message, and then enter the other items shown in the error message to delete the activation information on the eDC server.**

   If deactivation failed during appliance replacement, perform activation using the product key displayed on the dialog (see page 62 "Accounting Report Option").

How to find the aforementioned information in the log file

1. **Download the log file and save it on your computer (see page 138 "How to Download the Log File of the RC Gate A2").**
2. **Open the file named "debug_core.log" and search for the following string.**

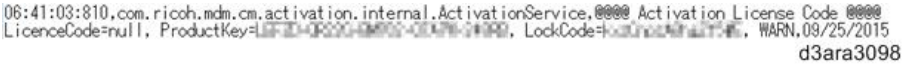
   `@@@@ Activation License Code @@@@`



d3ara3097

   If it is not found, search the newest file among those that have numbers indicating the date after "debug_core.log".

3. **Copy the license code/product key/lock code found in the log file and save them.**



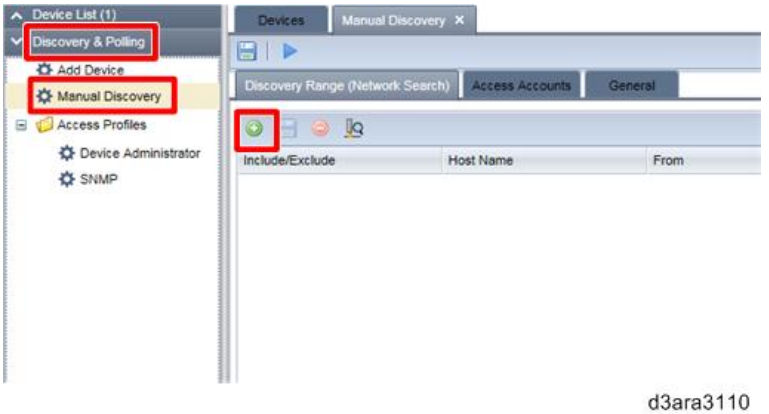
d3ara3098

When the IP Address of a Device Stored on the RC Gate Does Not Change Automatically After the IP Address of the Device Changes

The RC Gate A2 changes the IP addresses of devices stored on itself automatically if the actual IP addresses change.

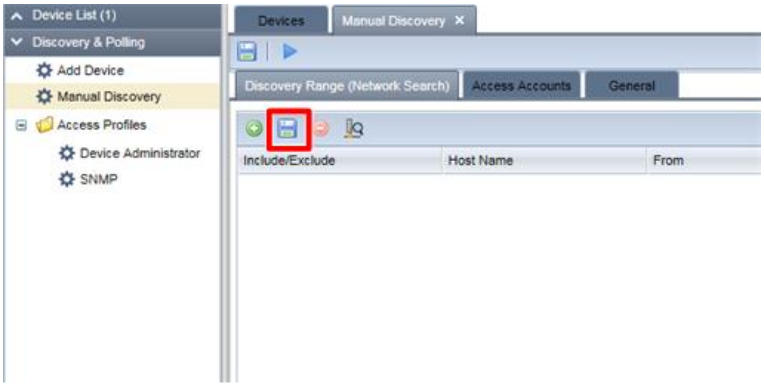
If they do not change automatically for some reason (customer network, device status etc.), or both the IP addresses of RC Gate A2 and the devices have been changed at once, do the following procedure manually, to change the IP addresses stored on the RC Gate A2.

1. **Log in as a CE.**
2. **Click [Discovery & Polling] in the section area.**
3. **Click [Manual Discovery] in the section tree.**
4. **Click (Add) in the list area.**



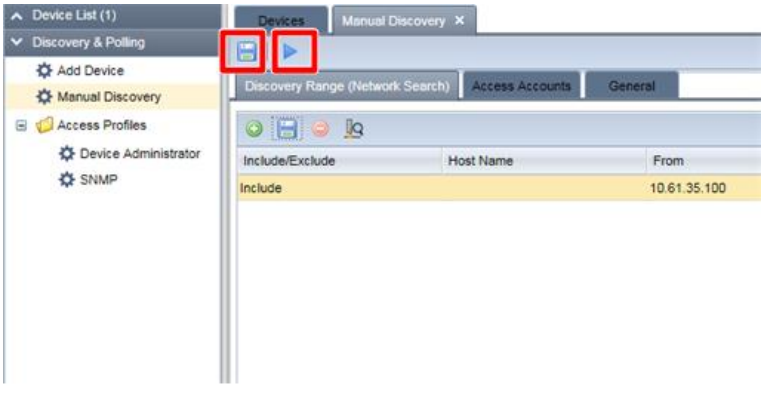
5. **Enter the search conditions such as IP address ranges.**

6. Click the lower (Save) button.



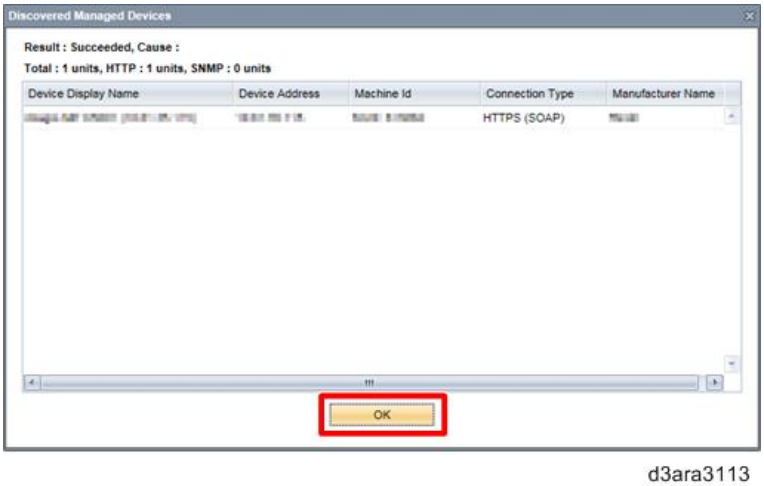
d3ara3111

7. Click the upper (Save) button, and then click (Immediately perform).



d3ara3112

8. Check the results in the "Discovered Managed Devices" dialog, and then click [OK].



d3ara3113

When Replacing the Controller Board of a Device connected to an RC Gate A2

When replacing the controller board of an @Remote-managed device:

After the controller board of the device has been replaced, you must change the settings of the device following the procedure below.

1. **Reconfiguring the device serial number**

   This is not required if the NVRAM is taken over from the previous controller board.

2. **Initializing the certificate area: SP5-870-003**

   This may or may not apply, depending on the machine type.

3. **Set the appropriate encryption strength for the certificate: [512-bit: SP5-870-001, 2048-bit: SP5-870-004]**

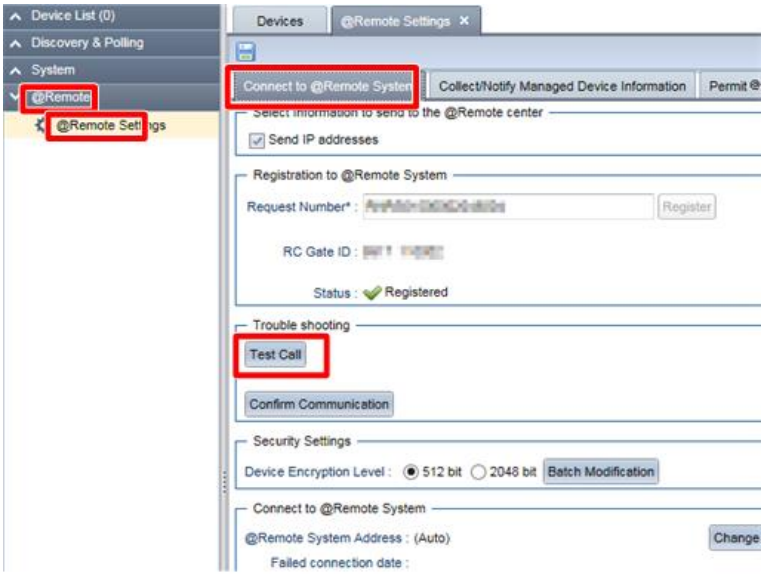
   For steps 2 and 3: Because the certificate is stored on the flash memory on the controller board, these steps are required even if the NVRAM is taken over from the previous controller board.

4. **If it is impossible to take over the NVRAM from the previous controller board, request the @Remote Center operator to reconfigure the ID2 code, in accordance with the following procedure.**

How to reconfigure the ID2 code

1. **Inform the @Remote Center operator of the "serial number of the RC Gate", "serial number of the device shown on the rating plate", "device IP address", and "device MAC address".**

2. **Do the following as instructed by the @Remote Center operator. Click [@Remote] > [@Remote Settings] > [Connect to @Remote System] > [Test Call].**



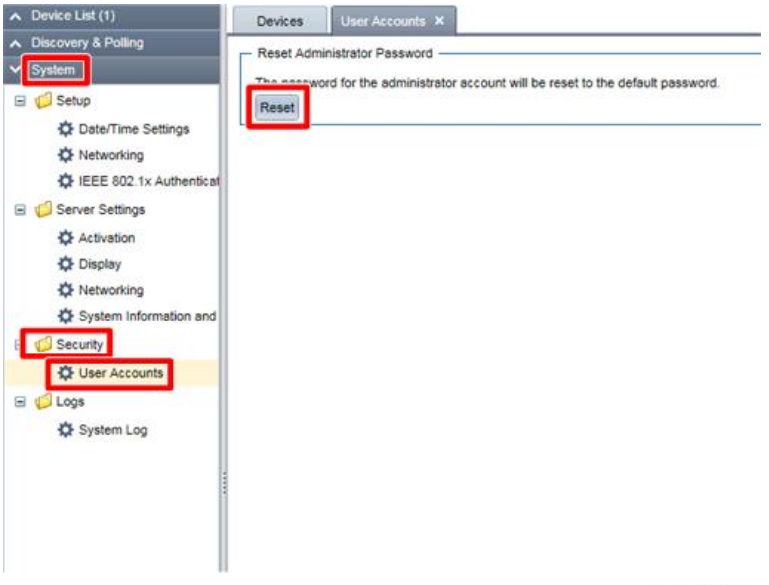
If the Administrator Forgot the Administrator Password

Resetting the Administrator Password

If the administrator forgot the administrator password, a CE can log in and reset the administrator password.

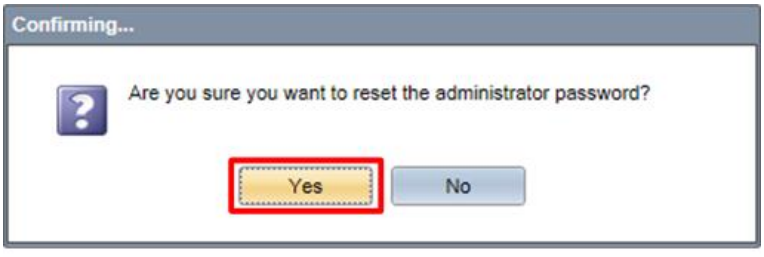
If login by a CE is prohibited (see page 116 "About Access Permission") and the administrator forgot the password, the password cannot be reset. Reset the RC Gate A2 to the factory-default settings or replace it with a new one (see page 132 "Resetting to the Factory Default Settings").

1. **Login as a CE.**
2. **Click the [System] section.**
3. **Click [Security] > [User Accounts].**
4. **Click [Reset] under [Reset Administrator Password].**



d3ara3099

5. When a confirmation message appears, click [Yes].



d3ara3100

6. A dialog appears to indicate that the password was reset successfully. Click [OK] to close the dialog.

d3ara3101

Other Problems

Connection with Devices or the Computer Fails

In [SSL/TLS Settings], you can select the protocols to be used during communication between devices and the RC Gate A2, and between your PC and the RC Gate A2.

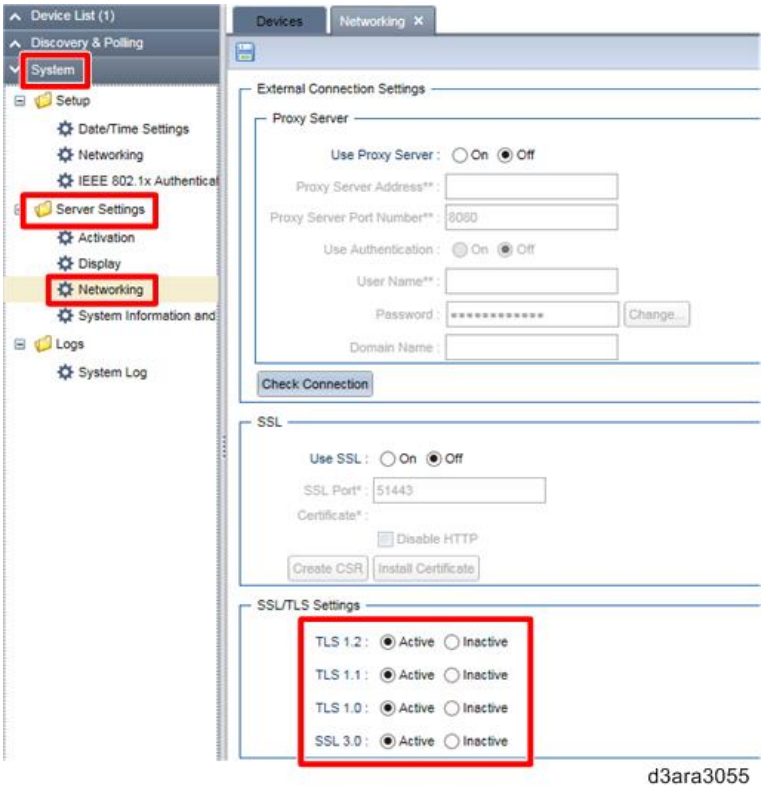
- TLS1.2
- TLS1.1
- TLS1.0
- SSL3.0

When specifying usable protocols in the configuration screens of your browser and the RC Gate A2, there must be at least one protocol that is selected in both of them.

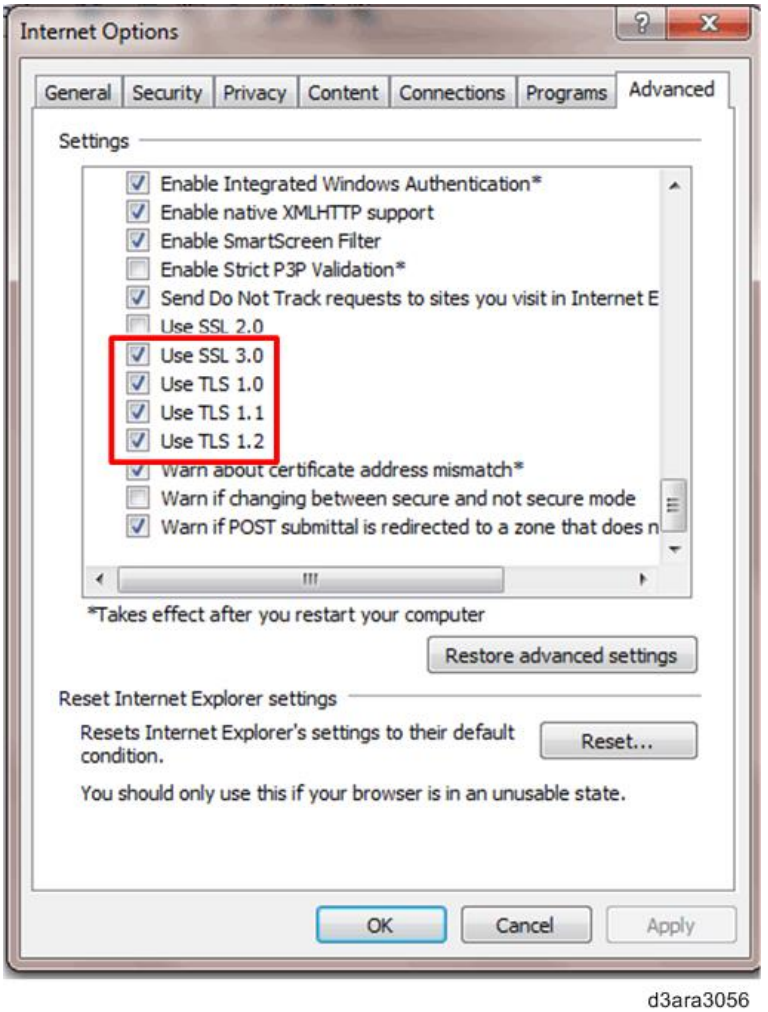
Setting up the RC Gate A2

1. **Log in as a CE.**
2. **Click the [System] section.**
3. **Click [Server Settings] > [Networking].**

4. Enable or disable protocols under [SSL/TLS Settings].



Browser settings (example: Internet Explorer)


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Enable Integrated Windows Authentication*
Enable native XMLHTTP support
Enable SmartScreen Filter
Enable Strict P3P Validation*
Send Do Not Track requests to sites you visit in Internet E
Use SSL 2.0
Use SSL 3.0
Use TLS 1.0
Use TLS 1.1
Use TLS 1.2
Warn about certificate address mismatch*
Warn if changing between secure and not secure mode
Warn if POST submittal is redirected to a zone that does n
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

d3ara3056

If the Login Screen of RC Gate Monitor Does Not Appear

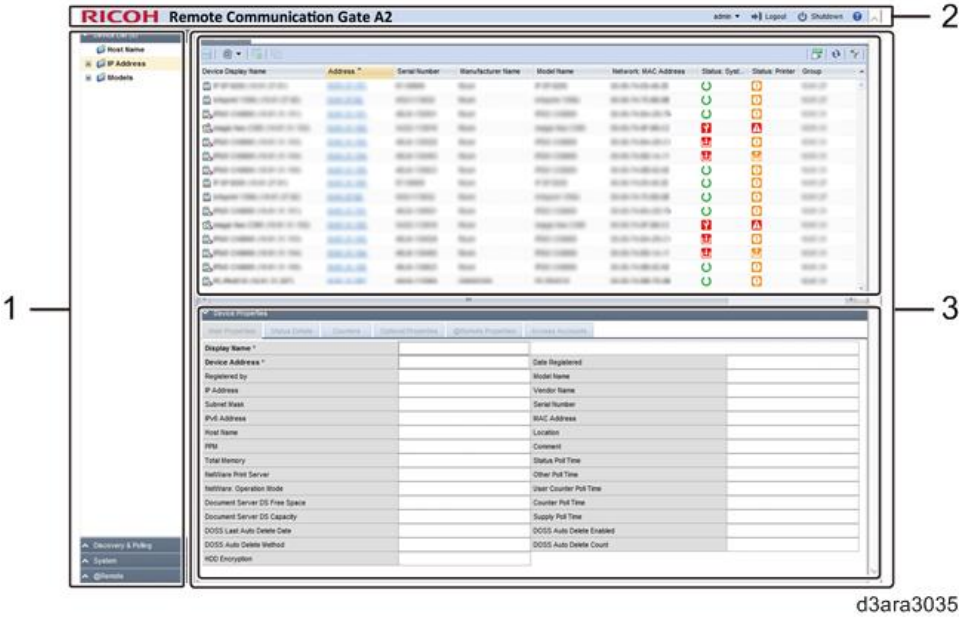
Status	Solution
The message "This page can't be displayed" is displayed.	1. Check the cable connection between the RC Gate and the computer. 2. Check if the entered URL starts with "http:". 3. Check if a ping reaches the maintenance port of the RC Gate (default: 192.168.10.153). 4. See if the encryption strength settings of the RC Gate and the browser match (see page 100 "Connection with Devices or the Computer Fails"). 5. Replace the cable between the RC Gate and the computer.
A message appears, instructing you to enable Cookies on the browser.	1. Check if Cookies are enabled in the browser settings. 2. Delete the temporary internet files, Cookies, and browsing history, and then restart the computer and the RC Gate.
The screen for dial-up connection appears.	Check if Local Area Connection is enabled.
The message "There is a problem with this website's security certificate." is displayed.	Click "Continue to this website".

5. Features

How to Use the RC Gate Monitor Screen

Main Screen

The standard screen configuration of the RC Gate A2 Monitor is explained below.



1. Section area

   Items in each section are displayed in this area.

   When a section is clicked, details of each item are displayed in a tree structure.

2. Header area

   - admin/RicohAtRemoteOperator (login user name)

     You can change the RC Gate A2 Monitor login password. For details about the password setting method, see page 115 "About the Login Password".

   - Logout

     Log out from the RC Gate A2 Monitor.

   - Shutdown

     Shut down and put the RC Gate A2 in standby mode. For details about shutdown, see page 66 "Shutdown".

- 

  Connect to the Ricoh website. You can also download "Setup Guide" and "Operating Instructions" from the Ricoh website.

  For information on functions that are not explained in this service manual, see "Operating Instructions".

3. Tab area

   The upper part is the list area (*1) and the bottom part is the properties area (*2).

   The control screen that corresponds to the selected tree item in the section area is displayed and uses the tabs to switch between multiple control screens. To close multiple tabs at once, right-click on the tab and select [Close All but Current] or [Close All].

   ***1 List area (The upper part)**

   A list of devices, tasks and other items is displayed above the tab area. Various icons are located on the tool bar in the list area and can be used for the following operations:

   - Import and export information such as the information in a list
   - Switch to an arbitrary view
   - Sort and classify lists
   - Access Web Image Monitor.

     Click the IP address of the target device. The device management tool displayed may differ depending on the target device.

   ***2 Properties area (The bottom part)**

   Detailed information about a device or task selected in the list area is displayed below the tab area, and can be used for editing and configuring the information.

   Click the name bar in the property area to open or close the selected area. Drag the name bar to change the size (height) of the area.

Status Icons

Status Icons

When you select a device from the device list, information about the device obtained through discovery/polling is displayed in the properties area.

Note

- Device information is not updated automatically. The information obtained during device registration or during the last polling is displayed. If you want to check the current status, execute polling (see page 72 "How to Check the Status of Communication with the Imaging Device").

Printer Status Icons

To display detailed information, place the mouse cursor on the status icon.

Icon	Description	Function				
		System	Copy	Printer	Fax	Scanner
	No response	Yes	Yes	Yes	Yes	Yes
	Service call	Yes	Yes	-	Yes	Yes
	Replace/supply	Yes	-	-	-	-
	Toner/ink exhausted	Yes	Yes	Yes	Yes	-
	Paper jam	Yes	Yes	Yes	Yes	-
	No paper	Yes	Yes	Yes	Yes	-
	Paper jam in ADF	Yes	Yes	-	Yes	Yes
	Performing maintenance	Yes	-	-	Yes	-
	Fax transmission error	Yes	-	-	Yes	-
	Open cover	Yes	Yes	Yes	Yes	Yes

Icon	Description	Function				
		System	Copy	Printer	Fax	Scanner
	Miscellaneous error	Yes	Yes	Yes	Yes	Yes
	Access violation has been detected	Yes	-	-	-	-
	Ready	Yes	Yes	Yes	Yes	Yes
	Offline	-	-	Yes	-	-
	Warming up	-	Yes	Yes	Yes	-
	Busy	-	Yes	Yes	Yes	Yes
	Toner/ink cartridge almost empty	-	Yes	Yes	Yes	-
	Paper almost empty	-	-	Yes	-	-
	Caution	-	Yes	Yes	Yes	Yes
	Energy saver mode	-	Yes	Yes	Yes	Yes

Paper Tray Icons

You can check the paper tray type. Also, you can check the orientation, size, type and remaining quantity of paper loaded in each paper tray.

 : Indicates two orientations of the loaded paper

On devices using rolled paper, an icon that indicates the remaining paper amount is displayed on the right-hand side.

 : No paper

 : 0 to 20 %

 : 20 to 40 %

 : 40 to 60 %

 : 60 to 80 %

 : 80 to 100 %

Toner/Ink Icons

You can check the colors of toner/ink and the remaining quantity of each toner/ink. "Unknown" may be displayed for some devices or monochrome MFPs if the remaining quantity of toner or ink cannot be detected.

The level of remaining toner or ink is indicated as shown below. The color of the indicator is the same as that of the applicable toner. Black is used as an example below:

 : Toner/ink is empty

 : Toner/ink cartridge is almost empty

 : 0 to 20 %

 : 20 to 40 %

 : 40 to 60 %

 : 60 to 80 %

 : 80 to 100 %

Output Tray Icons

You can check the output tray type and the status of each tray.

The output tray status is indicated by the icons as shown below:

 : Output tray is full

 : There is some paper in the output tray

 : Miscellaneous error

Nothing appears: Normal status

Displaying Device Properties

1. **In the [Device List] section, click a target group to display the corresponding device list.**
2. **Select a target device in the list area.**

   The information about the selected device is displayed in the [Device Properties].

Note

- Device information is not updated automatically. The information obtained during device registration or during the last polling is displayed. If you want to check the current status, execute polling (see page 72 "How to Check the Status of Communication with the Imaging Device").

Tab Configuration of Device Properties

Main Properties

You can check general information such as display name, model name, and IP address, along with date registered, serial number and MAC address.

- Display Name

  The name of the device is displayed. You can change the display name to the one you want.

- Device Address

  The address for the RC Gate to access the device is displayed.

- Date Registered

  The registration date is displayed. This date/time indicates when discovery was made or when the device was manually added.

- Registered by

  This is displayed as "localhost".

- Model Name
- IP Address
- Vendor Name
- Subnet Mask
- Serial Number
- IPv6 Address
- MAC Address
- Host Name
- Location

  The location configured on the device is displayed.

- PPM
- Comment

  The comment configured on the device is displayed.

- Total Memory
- Status Poll Time
- NetWare Print Server
- Other Poll Time
- NetWare: Operation Mode
- User Counter Poll Time
- Document Server DS Free Space

- Document Server DS Capacity
- Counter Poll Time
- Supply Poll Time
- DOSS Last Auto Delete Date
- DOSS Auto Delete Enabled
- DOSS Auto Delete Method
- DOSS Auto Delete Count
- HDD Encryption

Note

- On a RICOH MFP or printer, the settings configured in Web Image Monitor are displayed as "WIM Location" and "WIM Comment".

Status Details

You can check the device status by switching the [Printer Status], [Paper Tray], [Toner/Ink], and [Output Tray] tabs.

Counters

You can check counter information such as the number of pages printed in color/monochrome or number of transmitted pages.

- Total

  A total of the counters for the copier, printer, and fax functions
- Copy Color: Black, Full, Twin, Mono

  Counters for the copier function
- Printer Color: Black, Full, Twin, Mono

  Counters for the printer function
- Economy Color Counter
- Fax Color: Black, Mono

  Counters for the fax function
- A3/DLT
- A2
- Duplex
- Send: Color, Mono

  A total of the counters for the scanner transmission and fax transmission functions
- Fax Send
- Scanner Send: Color, Mono

  The counters for the scanner transmission function

- Total: Mono, Color
- Coverage Color: Pages, Percentage
- Coverage B&W: Pages, Percentage
- Color 1, 2, 3
- Active
- Idle
- Preheat
- Sleep
- OffMode

Optional Properties

You can check the individual information of optional properties by switching the [Custom Properties], [Installed Applications], [Firmware and Platform], and [Functions] tabs.

- Custom Properties

  Users can configure custom properties. For details about configuring custom properties, see "Setting custom properties".

- Installed Application

  You can check Application, Version, and Product ID.

- Firmware and Platform

  The user can check each device's version.

- Functions

  You can check the functions and printer language provided for the device.

  Functions: You can check the functions provided for the device, such as manual paper feed, duplex printing, and card printing functions.

  Printer Language: You can check the printer language provided for the device.

@Remote Properties

Part of the device information that the @Remote Center manages appears.

- Machine ID
- Connection Type
- Cutoff Date
- Service Depot
- Service Depot Phone No
- Supply Order From
- Supply Order Phone No
- Encryption Length

Access Accounts

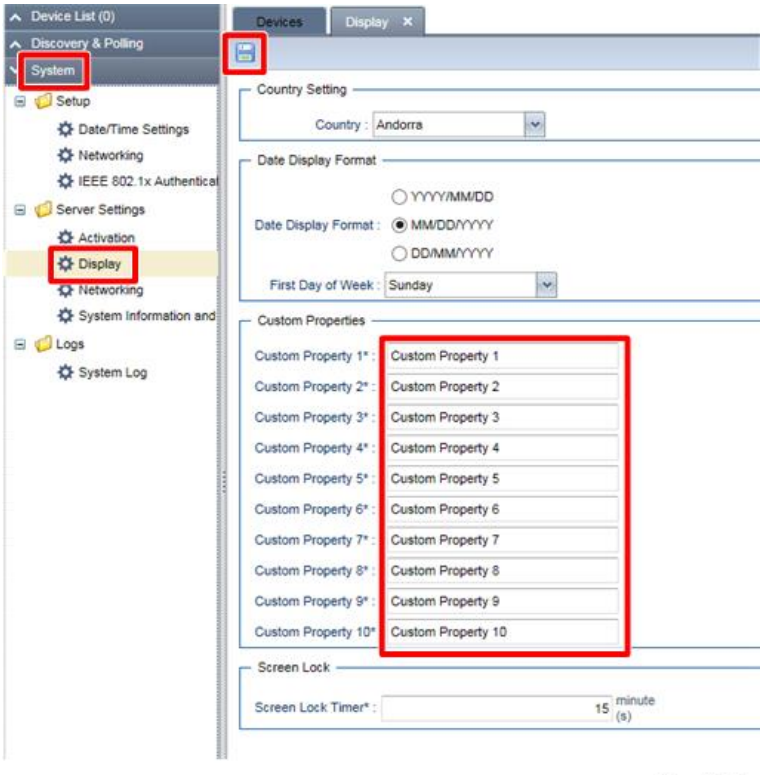
You can check access account profiles used for access to devices. Also, you can change the access account profile for each device.

Setting Custom Properties

Custom properties are used for adding arbitrary information to devices.

Information such as an administration number or an asset number can be set for each device.

1. **In the section area, click [System].**
2. **In the [Server Settings] category in the section tree, click [Display].**
3. **Enter the item name to be used for the custom property. You can use up to 255 alphanumeric characters for a name. You can create up to 10 custom properties. However, you cannot create multiple custom properties with the same name.**
4. **Click (Save).**



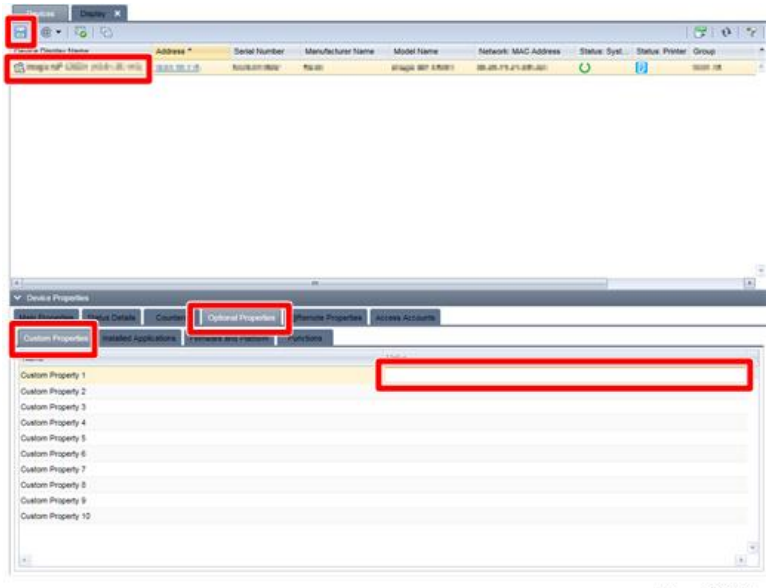
d3ara3080

5. **Select a target device from the device list.**
6. **In the properties area, click the [Optional Properties] tab, and then click the [Custom Properties] tab.**

7. **Double-click the [Value] row, and enter the unique information.**

   Use 0 to 255 characters.

8. **Click (Save) when the setting is configured.**



d3ara3081

Note

- Custom properties are not saved on the devices. They are saved on the RC Gate A2.

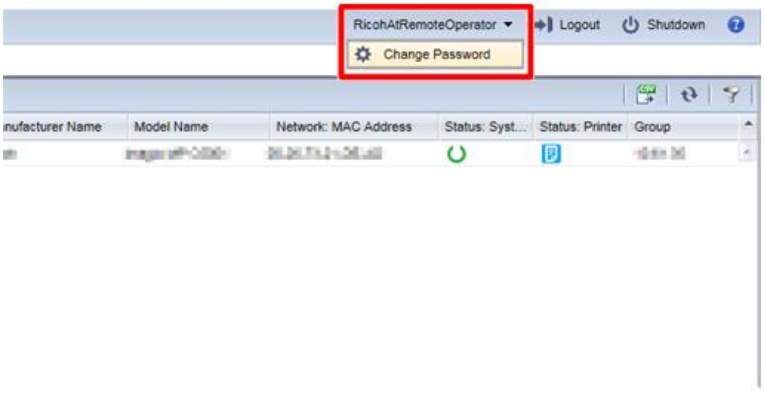
About Accounts, Passwords, and Access Permission

About the Login Password

The CE password and the administrator password can be changed by first logging in with the current password.

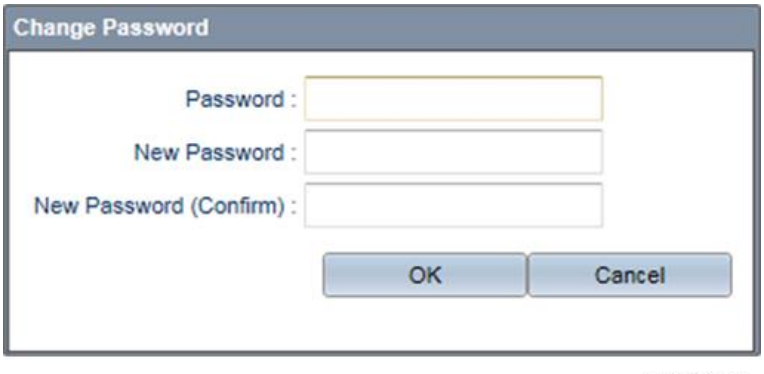
This procedure shows how to change the CE password.

1. **In the header area, click the login user name and [Change Password].**



d3ara3071

2. **In the [Password], enter a password.**
3. **In the [New Password], enter a new password.**
4. **In [New Password (Confirm)], enter the new password again to prevent mistyping.**
5. **Click [OK].**



d3ara3072

When changing the password

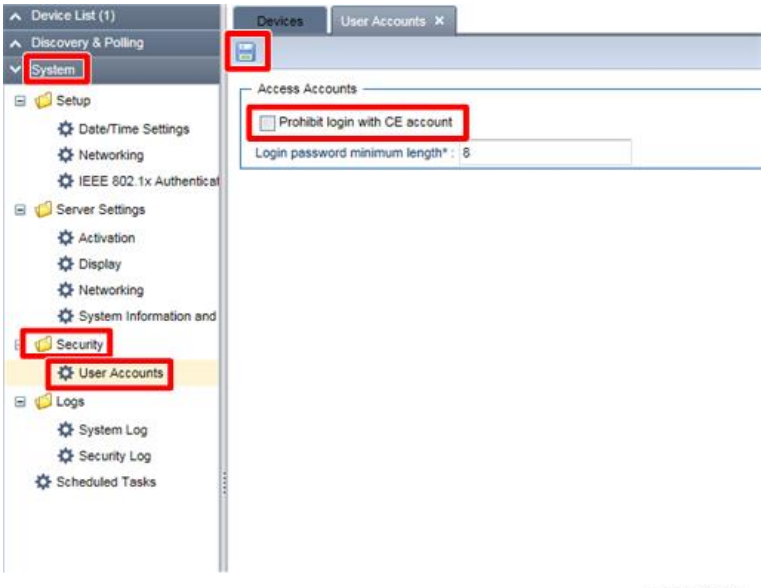
- Use 8 to 128 characters.
- You can use the following ASCII characters for the password: (Space)"(double quotations)! % &'(/)+,- . :$; <=>?[ ]^_` { | } ~0 1 2 3 4 5 6 7 8 9 #a b c d e f g h i j k l m n o p q r s t u v w x y z @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *
- Avoid using well known words or phrases, or repeated characters that can easily be guessed.
- Do not leave passwords written where they can be seen.
- New passwords become valid at the next login.
- If you forget the CE password, the RC Gate must be replaced.

If the administrator forgets the administrator password

The CE can reset the administrator password. See page 98 "Resetting the Administrator Password".

However, if CE login is prohibited (see page 116 "About Access Permission"), you cannot log in and therefore cannot reset the administrator password. In this case, you must reset the RC Gate A2 to the factory-default settings (see page 132 "Resetting to the Factory Default Settings") or replace it with a new one (see page 47 "Replacement/Migration").

About Access Permission



d3ara3102

If the customer selects [Prohibit login with CE account] in [Access Accounts], which is displayed when you log in as an administrator and click [User Accounts] under [Security], and clicks , login with the CE account is disabled. You cannot log in to the RC Gate A2 for maintenance or repair until the customer cancels it. When CE login is necessary, ask the customer to allow access.

About Access Accounts

When the RC Gate A2 communicates with an imaging device, an access account information corresponding to the communication type is required. If the access profile is not properly configured, the following problems will occur.

SNMP:

- Devices will not be discovered. (Add Device/Auto Discovery)

Device Administrator:

- The Accounting Report function will fail.
- Remote Firmware Update will fail.
- Polling will fail.
- Remote registration will fail.

Configuration overview

1. **Configure an access profile that includes the required account/password information by creating a new profile or editing an existing profile.**
2. **Select an access profile configured above when discovering devices (SNMP) or completing device registration (Device Administrator).**

How to configure the Access profiles

1. **Click [Discovery & Polling] > [Access Profiles] > [Device Administrator] or [SNMP].**
   When configuring the SNMP access profile before installation completion: Click [SNMP Access] under [Settings on Installation].

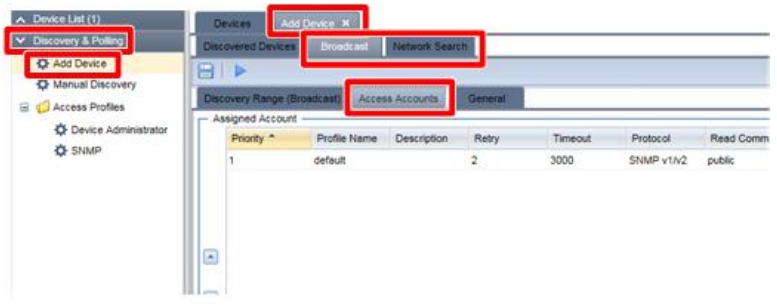
[Discovery & Polling]	[Settings on Installation]
	
d3ara3103	d3ara3105

2. **To create a new profile: Click , and then enter the required information under [Details].**
   To edit an existing profile: Click an existing profile, and then edit the information under [Details].
3. **Click .**

How to select an access profile configured above when discovering devices (SNMP) or completing device registration (Device Administrator)

SNMP

1. On the [Add Device] screen, click the [Broadcast] or [Network Search] tab > [Access Accounts] tab, and then select an account configured above.

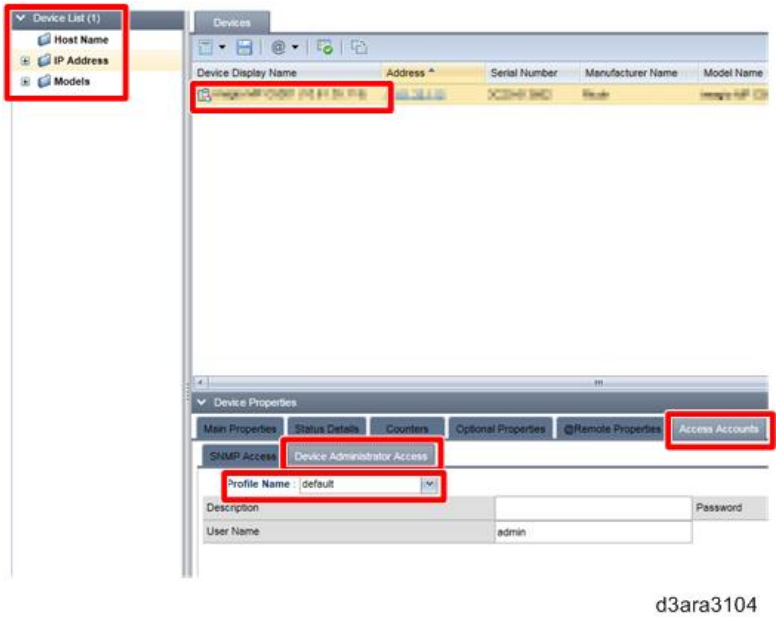


d3ara3108

2. Click .

Device Administrator

1. In the [Device List] section, click a target group to display the corresponding device list.
2. Select a target device in the list area.
3. Click [Access Accounts] > [Device Administrator Access] in the properties area.
4. Select a profile from the "Profile Name:" pull-down menu.



d3ara3104

5. Click .

Note

- If there are more than one Device Administrator accounts, first select the one that is used on the largest number of devices as the default settings, and then select the accounts for the other devices one by one.

About Device Discovery

There are several ways to search for devices. Choose the right one according to what you want to do.

Function	Description
Auto Discovery	Periodically collects MIB information of monitored/managed devices within the specified address ranges (see page 120 "What Is Auto Discovery?").
Manual Discovery	Searches devices to update the information about devices already registered when their IP addresses have been changed (see page 94 "When the IP Address of a Device Stored on the RC Gate Does Not Change Automatically After the IP Address of the Device Changes").
Add Device	Searches for devices and allows you to select which devices to register at the @Remote Center (see page 39 "Registering Devices (MFPs/Printers)").

What Is Auto Discovery?

With the Auto Discovery function, the RC Gate A2 periodically collects MIB information of monitored/managed devices within the specified address ranges.

- Network search

  When network search is selected, the RC Gate A2 attempts to access each address in the specified range using SNMP. It does not use ICMP.

- Broadcast

  Sends SNMP broadcast packets to all devices within the local network or a specified network range.

Note

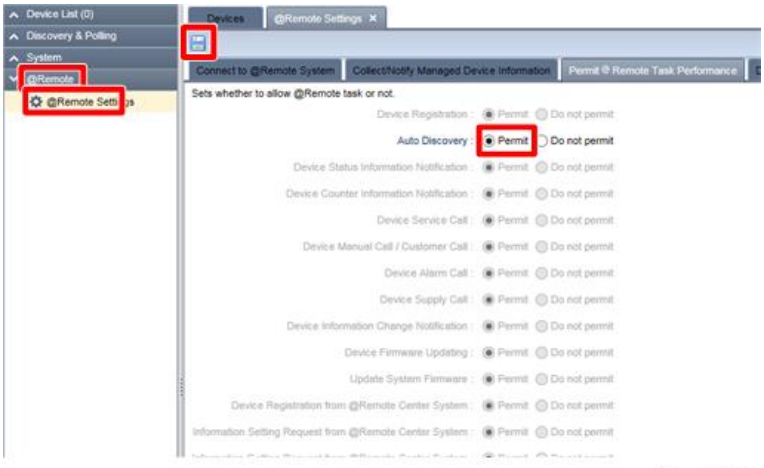
- Devices compliant with Printer MIB v2 (RFC 3805), Printer MIB (RFC 1759), MIB-II (RFC1213), Host Resource MIB (RFC 2790) can be discovered.
- Each target device wakes up from energy saver mode when it is discovered.

How to Configure Auto Discovery

Auto Discovery Using Network Search

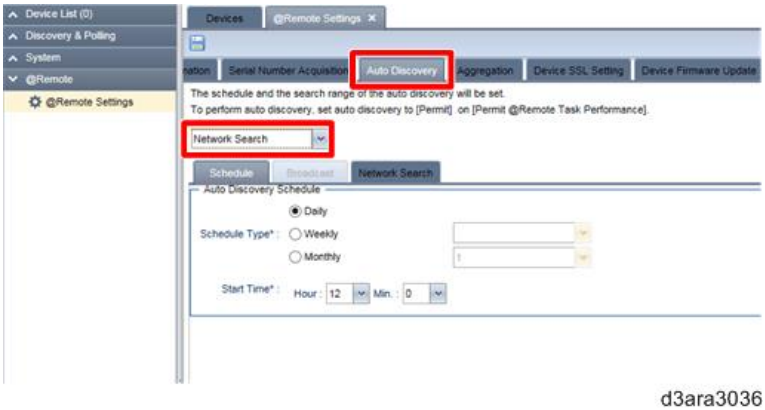
1. **Log in as a CE.**
2. **Click [@Remote].**

3. Click [@Remote Settings].
4. Click the [Permit @Remote Task Performance] tab.
5. Select [Permit] for Auto Discovery.
6. Click (Save).



d3ara3073

7. Click the [Auto Discovery] tab.
8. Select [Network Search] from the pull-down menu.



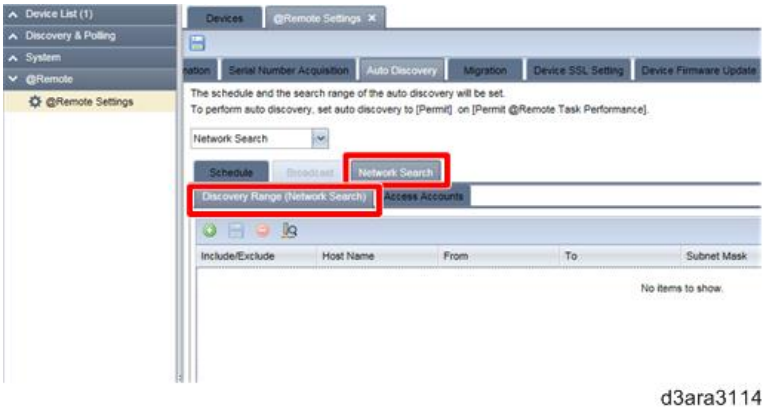
d3ara3036

9. In the [Schedule] tab, configure the discovery schedule.

Item	Description
Schedule Type	Schedule type can be selected from: • Daily • Weekly • Monthly

Item	Description
Start Time	Configure the start time. Hour: 0 to 23 Min. : 0 to 59

10. Click the [Network Search] tab, and then click the [Discovery Range (Network Search)] tab.



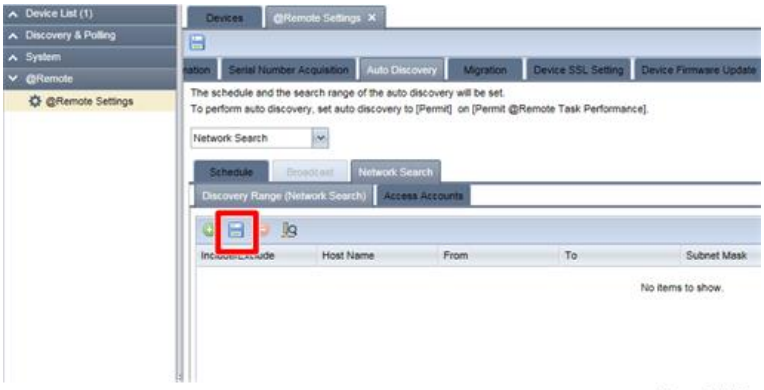
11. Click (Add) in the list area.

12. Specify the search conditions.

The following can be specified.

- Include/Exclude
- Type (Host Name/IP Address/Specify IP Range/IPv6 Address)
- Host Name
- From
- To
- Subnet Mask
- Range Name
- Comment

13. Click the lower (Save) button.

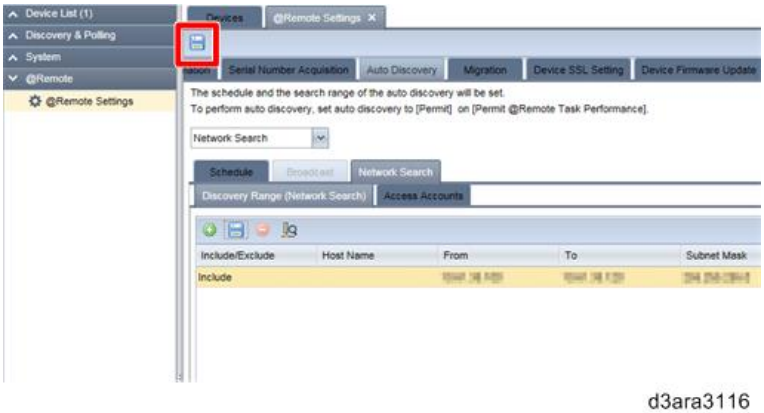


d3ara3115

Note

- Click to save the settings as a CSV file.
- Click to import settings saved as a CSV file.

14. If required, click the [Access Accounts] tab and select an access account suitable for communicating with the devices that can be detected.
15. Click the upper (Save) button.



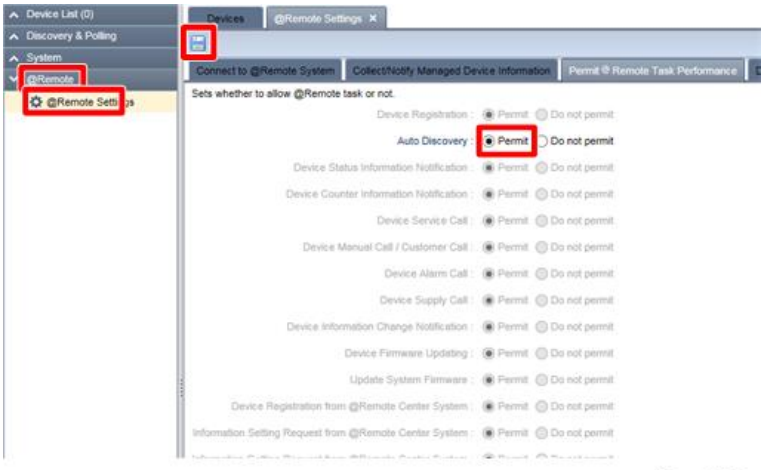
d3ara3116

Auto Discovery will be done according to the configured schedule.

Auto Discovery Using Broadcast

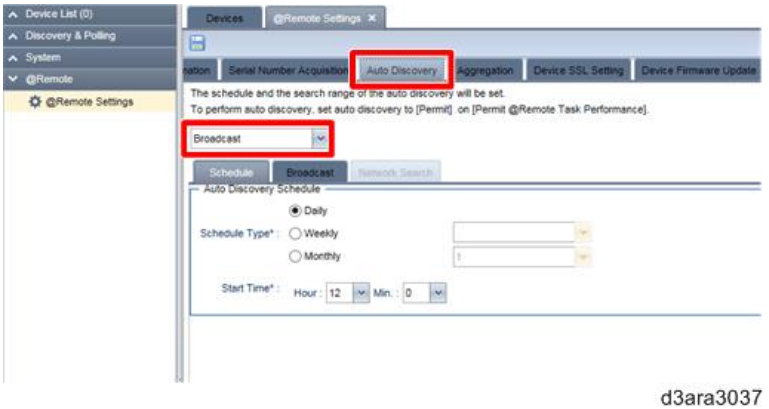
1. Log in as a CE.
2. Click [@Remote].
3. Click [@Remote Settings].
4. Click the [Permit @Remote Task Performance] tab.

5. Select [Permit] for Auto Discovery.
6. Click (Save).



d3ara3073

7. Click the [Auto Discovery] tab.
8. Select [Broadcast] from the pull-down menu.



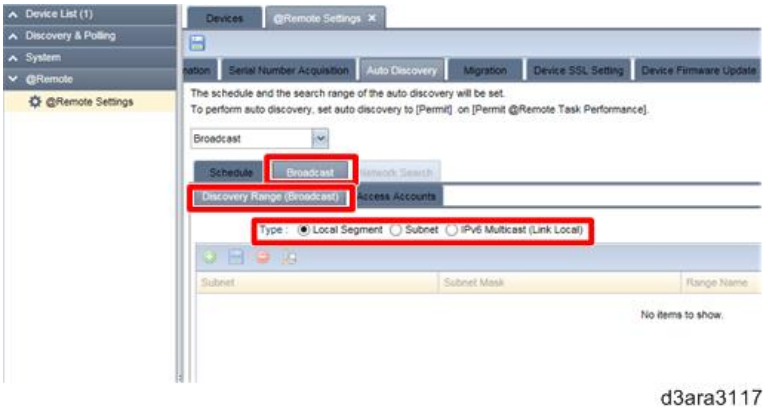
d3ara3037

9. In the [Schedule] tab, configure the discovery schedule.

Item	Description
Schedule Type	Schedule type can be selected from: • Daily • Weekly • Monthly

Item	Description
Start Time	Configure the start time. Hour: 0 to 23 Min. : 0 to 59

10. **Click the [Broadcast] tab, and then click the [Discovery Range (Broadcast)] tab.**
11. **Select the [Type].**



d3ara3117

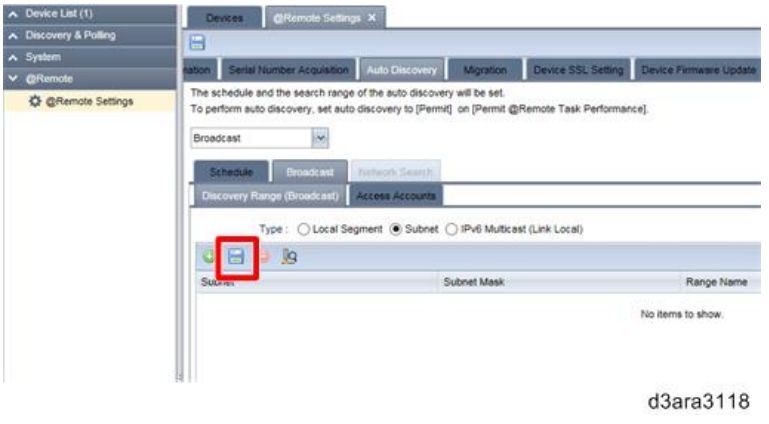
- When selecting [Local Segment] or [IPv6 Multicast (Link Local)], proceed to step 15.
- When selecting [Subnet], proceed to step 12.

12. **Click (Add) in the list area.**
13. **Specify the search conditions.**

    The following can be specified.

    - Subnet
    - Subnet Mask
    - Range Name
    - Comment

14. **Click the lower (Save) button.**

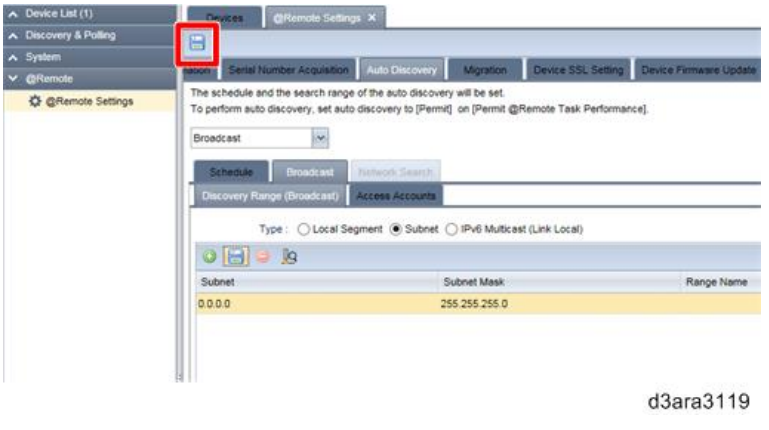


Note

- Click to save the settings as a CSV file.
- Click to import settings saved as a CSV file.

15. **If required, click the [Access Accounts] tab and select an access account suitable for communicating with the devices that can be detected.**

16. **Click the upper (Save) button.**



Auto Discovery will be done according to the configured schedule.

Using a CSV File

CSV files are used to import/export RC Gate A2 data.

Device lists can be exported to a CSV file ( ), and the data in the CSV file can be edited and then loaded to a CSV file ( ).

This procedure is explained using the CSV file for broadcasting the discovery range.

The variables are indicated by "X".

Typical description of a CSV file

# Format Version: 6.1.1.X			
# Generated at: XX/XX/XXXX XX:XX:XX			
# Function Name: Broadcast Discovery Range			
Subnet	Subnet Mask	Range Name	Description
X.X.X.X	X.X.X.X	XXXX	XXXX

d3ara3068

Note

- UTF-8 is used as the character code for CSV files. However, GB18030 is used as the character code when the language is Chinese.
- When data includes commas (,) or double quotations ("), enclose the entire data with double quotations. When using double quotation marks to enclose data that includes double quotation marks, place additional quotation marks outside the double quotation marks in the data. (e.g., a, "b", c => "a, ""b"", c")

Broadcast

The broadcast CSV file can be read and written in the following screens:

- [Broadcast] in [Add Device] in [Discovery & Polling].
- [Broadcast] in [Auto Discovery] in [@Remote Settings] in [@Remote].

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: 6.1.1.X
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Broadcast Discovery Range
4	"**(Row name)**"
5	"**(Value that corresponds to the row name)**"

The "Row name" and row number in line four, and their corresponding values in line five and subsequent lines are as follows:

Row number	Row name	Value of line five and subsequent lines
A	Subnet	Enter a subnet address. An IPv4 address can be used.
B	Subnet Mask	Enter a subnet mask.

Row number	Row name	Value of line five and subsequent lines
C	Range Name	Enter a discovery range name. Use up to 61 alphanumeric characters.
D	Description	Enter a discovery range description. Use up to 61 alphanumeric characters.

Rows C and D appear only if you write data using the broadcast setting in [Auto Discovery] in [@Remote Settings]. However, you can also have CSV files including rows C and D read into the broadcast setting in [Add Device]. Also, you can have CSV files written from the broadcast setting in [Add Device] read using broadcast setting in [Auto Discovery].

Note

- Do not change the information in lines one through three, because this information is used for identification.

Network Search

The network search CSV file can be read and written in the following screens.

- [Network Search] in [Add Device] in [Discovery & Polling].
- [Manual Discovery] in [Discovery & Polling].
- [Network Search] in [Auto Discovery] in [@Remote Settings] in [@Remote].

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: 6.1.1.X
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Network Search Discovery Range
4	"**(Row name)**"
5	"**(Value that corresponds to the row name)**"

The "Row name" and row number in line four, and their corresponding values in line five and subsequent lines are as follows:

Row number	Row name	Value of line five and subsequent lines
A	Range Type	Specify the search criteria from "One Host Name", "One IP Address", "Specify IP Range", and "IPv6 Address".

Row number	Row name	Value of line five and subsequent lines
B	IP Start/IP Address/ Host Name	Enter the discovery target host name, IP address, and IPv6 address, or the start IP address of the discovery target IP address range.
C	IP End	Enter the end IP address of the discovery target IP address range.
D	Subnet Mask	Enter a subnet mask.
E	0=Include/ 1=Exclude	Specify whether to include or exclude network search as a search range. The data is included in the network search if you enter "0" and excluded if you enter "1".
F	Range Name	Enter a discovery range name. Use up to 61 alphanumeric characters.
G	Description	Enter a discovery range description. Use 0 to 61 alphanumeric characters.

Rows F and G appear only when writing data using the broadcast setting in [Auto Discovery] in [@Remote Settings]. However, you can also have CSV files including Rows F and G read into the broadcast setting in [Add Device] or [Network Search] in [Manual Discovery]. Also, you can have CSV files written from the broadcast setting in [Add Device] or [Network Search] in [Manual Discovery] read using broadcast setting in [Auto Discovery].

Note

- Do not change the information in lines one through three, because this information is used for identification.

About the Accounting Report Option

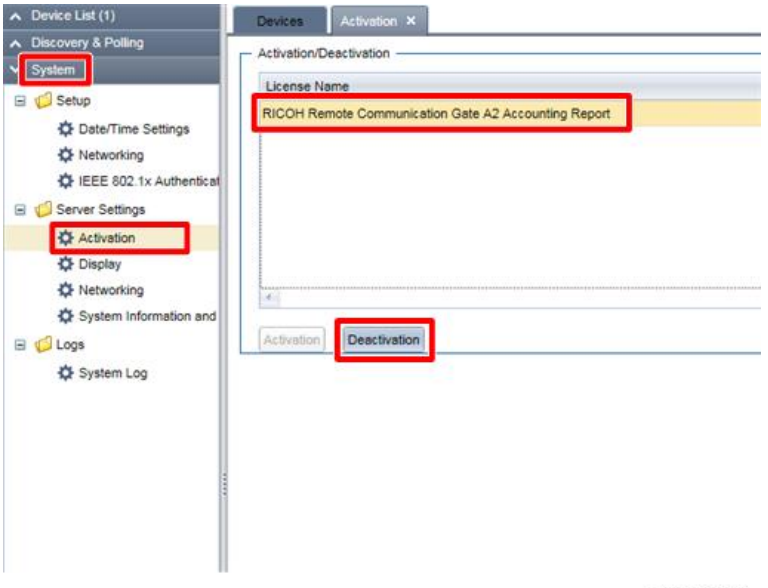
This option is required for collecting the counter of each user and sending it to the Gateway. For the sake of license management, activation is required when installing it. Deactivation is required when removing it.

About the Device Administrator Account

To use the Accounting Report option, the Device Administrator account settings on the RC Gate A2 and each device must match. For details, see page 117 "About Access Accounts".

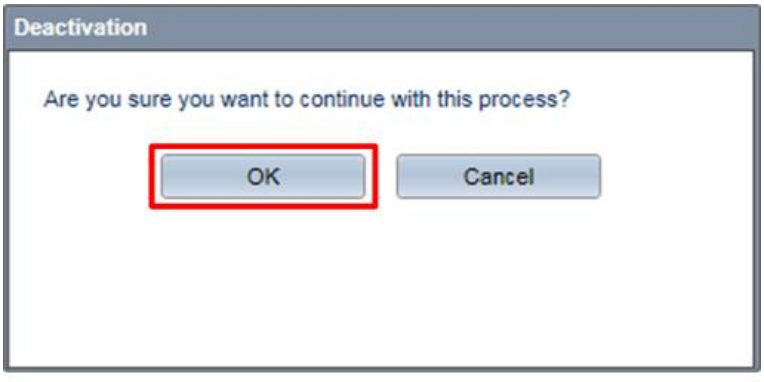
Activation/Deactivation

1. For the activation procedure, see page 62 "Accounting Report Option".
2. Deactivation procedure
    1. **Click the [System] section.**
    2. **Click [Activation] under [Server Settings].**
    3. **Select the target license and click [Deactivation].**



d3ara3074

4. Click [OK].



d3ara3075

5. Click [OK].

d3ara3076

Resetting to the Factory Default Settings

You can erase all data, including settings/counter/system log, and reset the RC Gate A2 to the factory default settings by changing the settings of the DIP switches.

Note

- The pictures above show the setting of the DIP switches during normal operation.

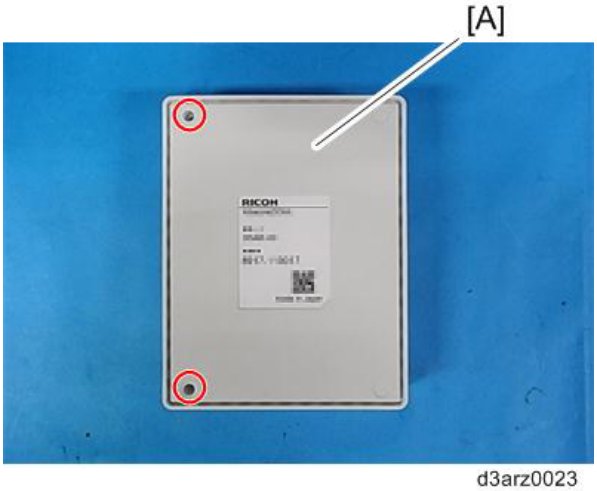
This function starts automatically when the RC Gate A2 is turned on with the DIP switch setting changed. One it starts, you cannot retrieve the erased data.

DIP switch setting	SW1	SW2	SW3	SW4	SW5	SW6
For normal operation	OFF	OFF	OFF	OFF	OFF	OFF
For initialization	OFF	OFF	OFF	ON	ON	OFF

Procedure

1. **Unplug the network cable and the power cord.**

2. **Remove the cover [A] (x2).**



d3arz0023

Important

- **Remove the cover to which the rating plate is attached. (Opening the other side may cause the power button to be damaged.)**

Note

- The cover is fixed with three hooks. Insert a jeweler's screwdriver to lift it.

d3arz0025

3. **Set the DIP switches according to the "For initialization" row in the table above.**
4. **Connect the power cord.**

   The RC Gate A2 turns on and data will be erased. When completed, the LED indicators will be as follows ("Before shipment" status):

LED name	Color	Status
LED(P)	Blue	Lit
LED(E)	Red	Lit
LED(S1)	Yellow	Unlit
LED(S2)	Yellow	Unlit

5. **Disconnect the power cord to turn off the RC Gate A2.**
6. **Set the DIP switches according to the "For normal operation" row in the table above.**
7. **Attach the cover.**

About the Tact Switch

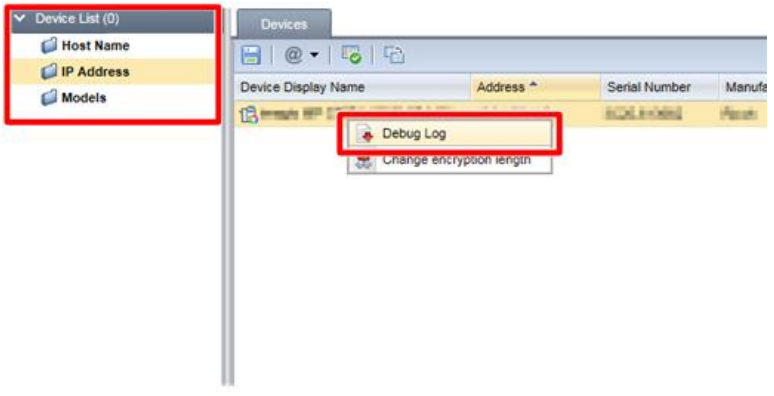
There is no CE operation that requires the use of tact switch [A].

If you happen to press the tact switch while the power is on and the cover is open, any operation will be stopped and the RC Gate A2 will be rebooted in the same way as when the power cord is disconnected and connected again.

d3bhz0025

How to Download the Device Log

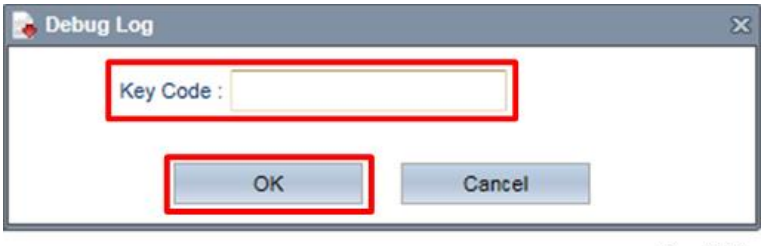
1. **Log in as a CE.**
2. **In the [Device List] section, click a target group to display the corresponding device list.**
3. **Select a target device in the list area, right-click on it, and select [Debug Log] from the displayed menu.**



d3ara3077

4. **Enter each of the key codes in the following list, and then click [OK] after each one.**

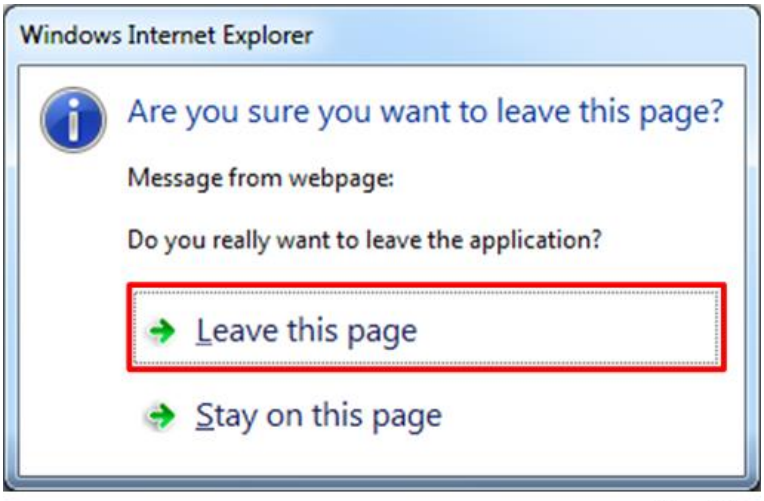
   In other words: Input 'ps', then click OK, then input 'syslog', then click OK, then input '2222', etc. This will obtain all of the logs.



d3ara3078

Key codes									
ps	syslog	2222	8181	8186	8187	7777	2000	2022	8255

When a dialog appears asking "Are you sure you want to leave this page?", click "Leave this Page".

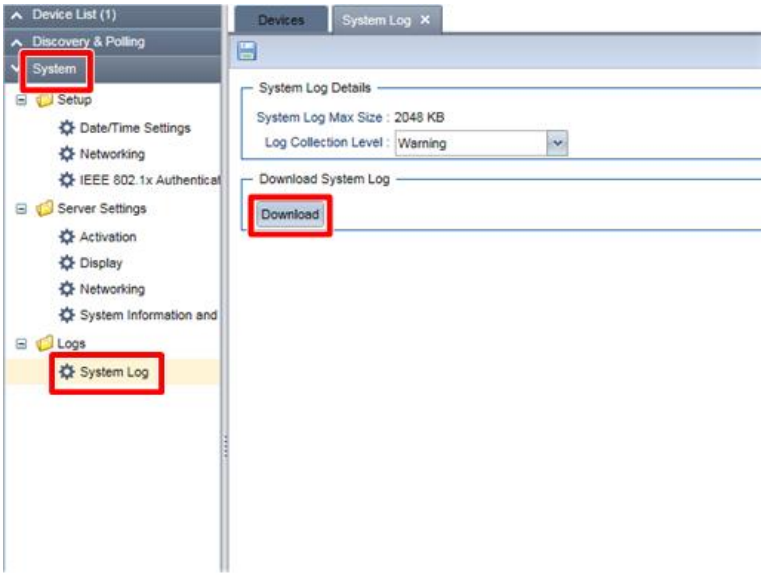


d3ara3079

5. Specify a folder to save the log and download it.

How to Download the Log File of the RC Gate A2

1. Log in as a CE.
2. Click the [System] section.
3. Click [Logs] > [System Log].
4. Click [Download] and save the log where you want to.



Do not change the log collection level unless you are instructed to do so.

How to Update the Firmware

The firmware of the RC Gate A2 is updated remotely from the @Remote Center. Request the @Remote Center operator for a Remote Firmware Update.

MEMO