



imageCLASS

LBP335x

User's Guide

Contents

Introduction	2
Using User's Guide	3
Screen Layout of User's Guide	4
Viewing User's Guide	7
Manuals and Their Contents	9
Environmental Information, Regulations, and Standards	10
Disclaimers	11
 About the Machine	 16
Parts and Their Functions	18
Front Side	19
Back Side	21
Interior	23
Multi-Purpose Tray	24
Paper Drawer	25
Control Panel	26
Turning ON the Machine	29
Turning OFF the Machine	30
Loading Paper	31
Paper Loading Operations	32
Basic Paper Loading Method	33
Loading Envelopes	41
Loading Postcards	45
Loading Preprinted Paper	48
Specifying Paper Size and Type	51
Specifying Paper Size and Type in the Paper Drawer	52
Specifying Paper Size and Type in the Multi-purpose Tray	54
Registering Frequently Used Paper Size and Type for the Multi-purpose Tray	57
Registering Free Size Paper (Custom Size Paper)	59
Automatically Selecting the Appropriate Paper Source for a Specific Function	60
Main Unit Maintenance	61
Regular Cleaning	63
Cleaning the Exterior	64
Replacing the Toner Cartridge	65
Relocating the Machine	68
Replacement Parts	70
Checking the Remaining Amount of Consumables	72
Clearing Paper Jams	73
Paper Jams inside the Machine or in the Back Side	76
Paper Jams in a Paper Source	80
Paper Jams at the Duplex Transport Guide	83
Options	85

Optional Equipment	86
Paper Feeder PF-C	87
Hardware Specifications	88
Main Unit	89
Available Paper	91
Paper Feeder PF-C	98

Setting Up 100

Preparations Required Before Use	101
Preventing Unauthorized Access	102
Setting up Using the Setup Guide	104
Setting the Date/Time	105
Setting up the Network Environment	106
Selecting the Network Connection Method	108
Connecting to a Wired LAN	110
Connecting to a Wireless LAN	112
Setting Up the Connection Using WPS Push Button Mode	114
Setting Up the Connection Using WPS PIN Code Mode	115
Setting Up Connection by Selecting a Wireless Router	116
Setting Up a Connection by Specifying Detailed Settings	117
Checking the SSID and Network Key	118
Setting an IP Address	119
Setting an IPv4 Address	120
Setting an IPv6 Address	122
Setting the IPv4 Address of the Sub Line	124
Adapting to the Network Environment	125
Making Ethernet Settings	126
Setting the Wait Time When Connecting to a Network	127
Making DNS Settings	128
Monitoring and Controlling the Machine with SNMP	132
Setting Static Routing	136
Other Network Settings	138
Configuring System Data Communication	140
Installing Drivers	142
Configuring E-Mail Print Settings	143

Basic Operations 147

Using the Control Panel	149
Basic Screens	150
Items Displayed on the <Home> Screen	152
Basic Operation	154
Entering Characters	157
Logging into the Machine	159
Customizing the Display	160
Customizing the <Home> Screen	161
Switching the Displayed Language	162

Setting Sounds	163
Entering Sleep Mode	164
Printing	168
Printing From a Computer	170
Canceling Printing	173
Checking the Printing Status and History	175
Printing from an External Network (IPP Printing)	176
Advanced Functions for Printing	179
Printing Documents that are Forced to be Held in the Machine	180
Printing Held Documents Automatically When Logging In	182
Print Screen	183
Printing Out Secured Documents	185
Various Printing Methods	187
Directly Printing Files without Opening Them	188
Printing Using a Virtual Printer	190
Printing From Memory Media (Media Print)	192
Printing Received E-mail (E-Mail Print)	193
Printing Using the Microsoft Cloud Service (Universal Print)	194
Configuring the Universal Print User Settings	198
Using Memory Media Such as USB Memory	201
Using Memory Media	202
Linking with Mobile Devices	208
Connecting with Mobile Devices	209
Connecting Directly	210
Utilizing the Machine through Applications	214
Using AirPrint	217
Printing with AirPrint	221
If AirPrint Cannot Be Used	225
Printing with Default Print Service (Android)	226
Managing the Machine	229
Applying a Security Policy to the Machine	231
Using a Password to Protect the Security Policy Settings	232
Configuring the Security Policy Settings	234
Security Policy Setting Items	236
Managing Users	241
Configuring the Personal Authentication Management Settings	243
Registering User Information in the Local Device	246
Importing/Exporting User Data	251
Adding and Editing User Information in a CSV File	254
Associating IPP Printing Information with Users	259

Registering Server Information	262
Configuring the Authentication Functions	270
Using Personal Authentication to Manage Printing via a Computer	274
Using Other Convenient Personal Authentication Management Functions	275
Setting the Department ID Management	276
Changing the System Manager ID and PIN	277
Configuring the Department ID Management Settings	279
Using Department IDs to Manage Printing via Computer	282
Setting an Authentication/Password Policy	283
Configuring the Network Security Settings	286
Restricting Communication by Using Firewalls	288
Specifying IP Addresses in Firewall Settings	289
Specifying MAC Addresses in Firewall Settings	292
Configuring the Firewall in IP Addresses of the Sub Line	295
Configuring the Firewall in MAC Addresses of the Sub Line	298
Setting a Proxy	301
Configuring the Key and Certificate for TLS	303
Generating the Key and Certificate for Network Communication	307
Configuring the IPSec Settings	310
Configuring the IEEE 802.1X Authentication Settings	317
Restricting the Machine's Functions	320
Restricting Printing from a Computer	321
Restricting the Use of Memory Media	325
Restricting Use of the Control Panel	326
Managing the Machine from a Computer (Remote UI)	327
Starting the Remote UI	329
Checking the Status and Logs	334
Turning OFF/Restarting the Machine	336
Registering a Key and Certificate for Network Communication	337
Configuring the Expiration Check Method for Received Certificates	340
Generating a Key and Certificate Signing Request (CSR)	343
Retrieving/Updating a Certificate from an SCEP Server	346
Managing the Logs	352
Importing/Exporting the Setting Data	357
Importing/Exporting All Settings	359
Updating the Firmware	363
Updating the Firmware (Distribution)	365
Setting Scheduled Updates	368
Displaying Messages from the Administrator	370
Setting the Website for Purchasing Consumables	371
Installing System Options	373
Managing Storage Device Data	375
Initializing Settings	376
Checking the Number of Pages for Print	378
Printing Reports and Lists	379

Paper Type Management Settings	380
--------------------------------------	-----

Settings/Registration 386

Settings/Registration Table	387
Preferences	389
Display Settings	390
Timer/Energy Settings	391
Network	393
External Interface	412
Accessibility	413
Volume Settings	414
Adjustment/Maintenance	415
Adjust Image Quality	416
Maintenance	418
Function Settings	419
Common	420
Printer	422
Custom Settings	423
UFR II	425
PCL	426
PS	428
Imaging	429
PDF	430
XPS	431
Utility	432
Send	433
Receive	434
Access Files	435
Print	437
Management Settings	438
User Management	439
Device Management	440
License/Other	441
Data Management	442
Security Settings	443
Output Report	444
<Preferences>	445
<Display Settings>	446
<Timer/Energy Settings>	448
<Network>	452
<External Interface>	465
<Accessibility>	467
<Volume Settings>	468
<Adjustment/Maintenance>	469
<Adjust Image Quality>	470
<Maintenance>	474
<Function Settings>	475

<Common>	476
<Printer>	479
<Send>	481
<Receive>	482
<Access Files>	483
<Print>	484
<Management Settings>	485
<User Management>	486
<Device Management>	487
<License/Other>	489
<Data Management>	491
<Security Settings>	493
<Output Report>	495

Adjusting Print Quality 499

Adjusting the Print Position	500
Adjusting the Standard Density	503
Adjusting Density for Specific Paper	504

Troubleshooting 506

If the Machine Does Not Operate	507
Cannot Print	509
Problems with Printing Results	510
Problems with the Network	521
Problems with Security	525
Other Problems	526
A Message or a Number Starting with "#" (an Error Code) Is Displayed	530
A Message Saying to Contact Your Dealer or Service Representative Is Displayed	531
Countermeasures for Each Message	532
Countermeasures for Each Error Code	550
When a Problem Cannot Be Solved	558

Implementing Security Measures 560

Various Security Functions	561
----------------------------------	-----

Appendix 565

Feature Highlights	566
Productivity	567
Image Quality	568
Manageability	569
Building a Dual Network Environment	570
Reliability	573
Office Compatibility	574

MEAP	575
Installing MEAP Applications	577
Managing MEAP Applications	580
Managing MEAP Application Licenses	585
Changing Login Services	588
Basic Windows Operations	592
System Specifications	598
Printer Functions	599
Management Functions	602
System Environment	607
Network Environment	608
System Options	610

Introduction

- Introduction 2**
- Using User's Guide 3**
 - Screen Layout of User's Guide 4
 - Viewing User's Guide 7
- Manuals and Their Contents 9**
- Environmental Information, Regulations, and Standards 10**
- Disclaimers 11**

Introduction

E9SJ-000

This chapter describes the instructions on how to use the User's Guide, disclaimers, copyright information, and other important information for customers. Read this chapter as necessary.

■ Manuals for the Machine

This section describes the different manuals you can refer to for information on how to use the User's Guide (this manual) and the machine's functions and operating procedures.



▶ **Using User's Guide(P. 3)**

▶ **Manuals and Their Contents(P. 9)**

■ Disclaimers and Copyright

See this section for disclaimers and copyright information.

▶ **Disclaimers(P. 11)**

Using User's Guide

E9SJ-001

The User's Guide is a manual that can be viewed on your computer or smartphone, etc. This section describes the screen layout of the User's Guide and how to view the User's Guide. It also describes how to make settings for the display of the User's Guide.

■ Screen Layout of User's Guide

This section explains the User's Guide screen layout and how to use the buttons on the screen. ▶ **Screen Layout of User's Guide(P. 4)**

■ Viewing User's Guide

This section describes what you should be familiar to when viewing the User's Guide, including the meanings of the marks used in the User's Guide and how the keys on the control panel and buttons on the computer screen are represented in the User's Guide. ▶ **Viewing User's Guide(P. 7)**

■ Setting the Display of the User's Guide

You can change the character size used in the User's Guide, and switch the screen layout to one that is appropriate to the device on which the User's Guide is displayed.

NOTE

- If you are unable to view the manual in PDF format, download Adobe Acrobat Reader from the Adobe Systems website (<https://get.adobe.com/reader/>).

How to find the topic you are looking for

Search the contents

- You can find the page you are looking for by selecting the topic from the Contents on the left side of the screen.

Search by keyword

- Perform a search by entering a keyword, such as "envelope" or "toner cartridge," and the pages containing the keyword are displayed. You can find the page you are looking for from those results. You can also enter phrases such as "connecting to a network." The keyword search also supports the AND Boolean to search for multiple keywords. For the details of the search screen and how to operate the screen, see ▶ **Search(P. 5)** .

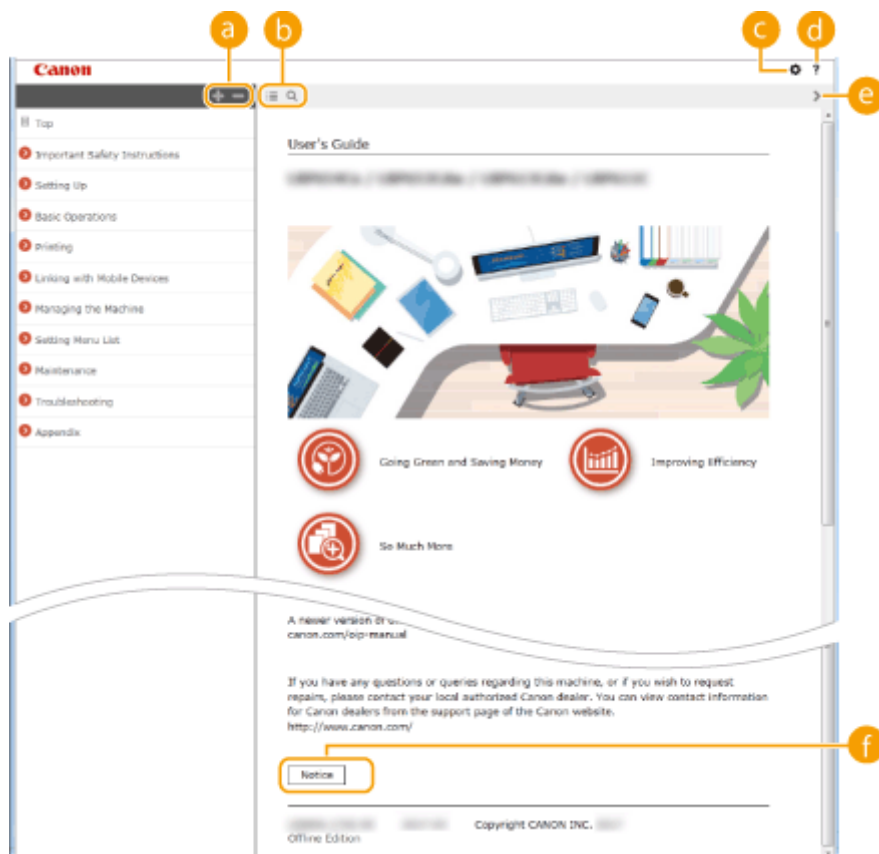
Screen Layout of User's Guide

E9SJ-002

The User's Guide is divided into different screens, and the content of each screen varies.

Top Page

Appears when the User's Guide starts.



Click to display all items underneath chapters. Click to return to the original list.



Click to switch between the table of contents and the search display. When the table of contents is displayed, each click on switches between hiding and showing the display. When the search display is shown, each click on switches between hiding and showing the display.



Click to specify settings such as text size, layout, and display method for the User's Guide.



Click to display information on how to view the User's Guide, how to perform a search, and other information.



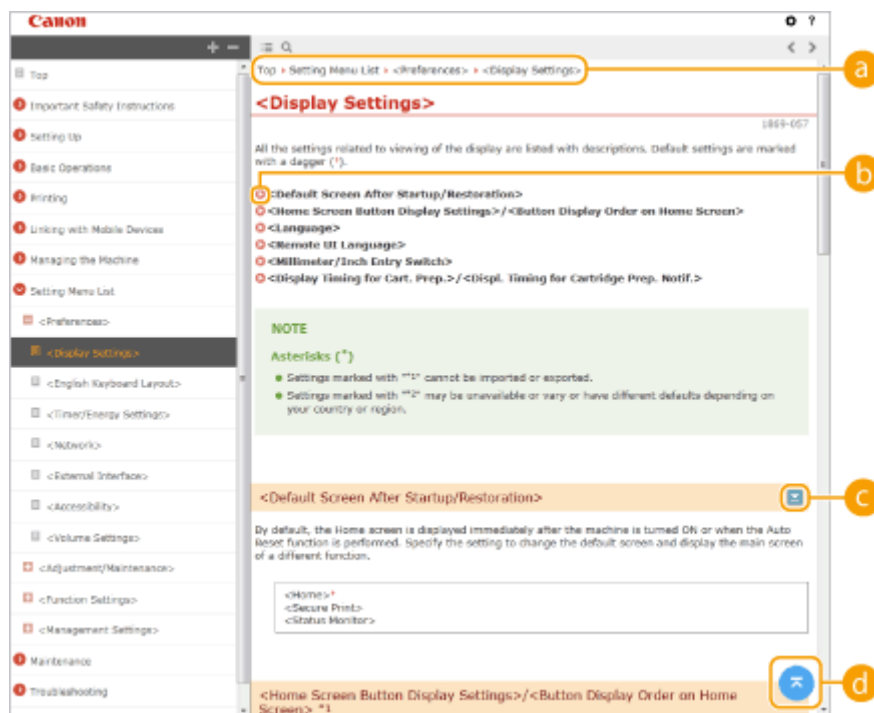
Click to display the previous or following topic.

f [Notice]

Click to view important information you should know when using the machine.

Topic Page

Contains information about how to configure and use the machine.



a Navigation

See what chapter topic you are currently viewing.



Click to go to the corresponding page. To return to the previous page, click "Back" on your Web browser.



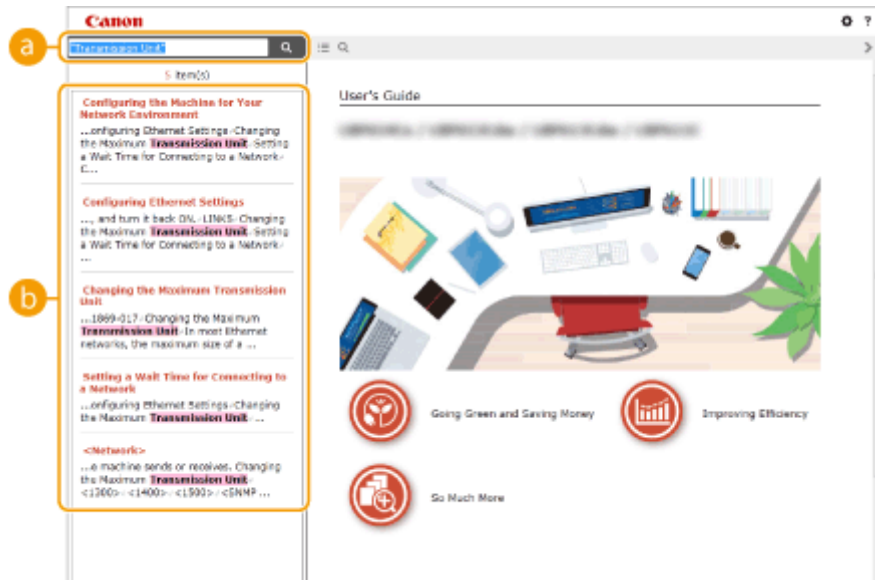
Click  to display the hidden detailed descriptions. Click  to close the detailed descriptions.



Click to return to the page top.

Search

Click  to display the search screen. Contains a text box to perform a search by keyword and find the page you are looking for.



a [Enter keyword(s) here]

Enter a keyword or keywords and click  to display the search results. You can search for pages containing all the keywords by separating the keywords by a space (blank). Also you can only search for pages containing an exact phrase by enclosing the keywords in double quotation marks.

b Search result

Displays the search results of the pages that contain the specified keywords. From the results, locate the page you are looking for and click the topic title of the page.

NOTE

- The keywords appear in bold in the pages displayed as search results.

Viewing User's Guide

E9SJ-003

This section describes the marks, buttons, screens, and other items used in the User's Guide. The warnings and cautions are also given in the "Important Safety Instructions" included with the machine. See also these instructions.

Marks

Cautions regarding safety, restrictions and cautions regarding the handling of the machine, useful tips, and other information are indicated using the marks below.



WARNING

Indicates a warning concerning operations that may lead to death or serious personal injury if not performed correctly. To ensure that you use the machine safely, always observe these warnings.



CAUTION

Indicates a precaution for preventing the risk of personal injury or property damage other than a product fault due to improper use of the machine. To ensure that you use the machine safely, always observe these cautions.



Indicates an operation that must not be performed. Read these items carefully, and make sure not to perform the described operations.



IMPORTANT

Indicates important operational requirements and restrictions that should always be observed when using this machine. Always observe these important items to avoid malfunctions, faults or property damage due to improper machine operation.

NOTE

Indicates a clarification of an operation, or contains additional explanations for a procedure.

TIPS

Indicates useful functions or tips for using the machine.

Keys and buttons

Keys on the control panel and buttons on the computer screen are indicated as follows.

Type	Example
Keys on the control panel	 
Settings displayed on the control panel	<Function Settings> <Cancel?>
Buttons and other text interfaces displayed on the computer display	[Preferences] [OK]



▲, ▼, and  on the control panel are used to select the target item in settings, but their description is omitted in the User's Guide. The operation for selecting <XXXXX> using ▲ or ▼ and pressing  is represented as shown below in the User's Guide.

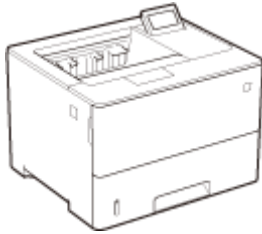
- 1 Select <XXXXX>.

Screen

Depending on the operating system you are using, the appearance of the displays used in this manual may slightly differ from the actual displays. Also, the appearance of the printer driver and software may differ depending on their version.

Illustrations

Illustrations used in the User's Guide are from "imageCLASS LBP335x" unless otherwise specifically noted.



Manuals and Their Contents

E9SJ-005

The following manuals are included with the machine. Refer to them as necessary.

Important Safety Instructions	 	The content described in this manual is for the prevention of damage to property and injury to users of the machine and others.
Setup Guide	 	This manual, viewable using a Web browser, outlines the initial settings on the machine required when the machine is turned on for the first time; and describes how to install the software and driver. It can be viewed from the online manual Website.
User's Guide (This Manual)		This manual describes all the functions of the machine in a manual that is viewed using a Web browser. You can browse information by category or enter a keyword to search for pages on a specific topic.  Using User's Guide(P. 3)
Setting the Machine (PS/PCL/UFR II Printer)		This manual, viewable using a Web browser, describes how to use the PS/PCL/UFR II printer. It can be viewed from the online manual Web site.

Environmental Information, Regulations, and Standards

E9SJ-006

■ IPv6Ready Logo



The protocol stack included in this product has obtained the IPv6 Ready Logo Phase-2 established by the IPv6 Forum.

■ E-Waste rules

- E-Waste rules for India -



<https://in.canon/en/consumer/web/e-waste>

■ When disposing of used toner cartridges

- To protect the environment and make more effective use of resources, Canon promotes the recovery and recycling of used toner cartridges. Please cooperate in the recovery of toner cartridges (resource reuse). For details on resource reuse, see the Canon website:

global.canon/ctc

When disposing of toner cartridges, pack them in their original packaging to prevent toner dispersal and dispose of the cartridges in accordance with your local government instructions.

Disclaimers

E9SJ-007

■ Disclaimers

- The information in this document is subject to change without notice.
- CANON INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MANUAL, EITHER EXPRESS OR IMPLIED, EXCEPT AS STIPULATED HEREIN, INCLUDING WITHOUT LIMITATION THEREOF WARRANTIES AS TO MARKETABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OF USE, OR NON-INFRINGEMENT OF PATENT RIGHTS. CANON INC. SHALL NOT BE LIABLE FOR ANY DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY NATURE, NOR FOR LOSSES OR EXPENSES RESULTING FROM THE USE OF THIS MANUAL.
- If you are unable to view the manual in PDF format, download Adobe Acrobat Reader from the Adobe Systems website (<https://get.adobe.com/reader/>).

■ Trademarks

"MEAP" is a trademark of CANON Inc., referring to an application platform for Canon multifunction and single function printers.

Mopria®, the Mopria® Logo and the Mopria® Alliance logo are registered trademarks and service marks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.

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

This product contains the Universal Font Scaling Technology or UFST® under license from Monotype Imaging, Inc. UFST® is a trademark of Monotype Imaging, Inc. registered in the United States Patent and Trademark Office and may be registered in certain jurisdictions.

UFST: Copyright © 1989 - 1996, 1997, 2003, 2004, 2008, 2014 all rights reserved, by Monotype Imaging Inc.

Apple, Bonjour, iPad, iPhone, iPod touch, Mac, macOS, OS X, and Safari are trademarks of Apple Inc.

Google Chrome, Chrome OS, Chromebook, Google Workspace, and Android are trademarks of Google LLC.

QR Code is a trademark of DENSO WAVE INCORPORATED.

Portions of this software are copyright © 2007 The FreeType Project(www.freetype.org).

All rights reserved.



Java is a registered trademark of Oracle and /or its affiliates.



Adobe, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Copyright © 2007 -08 Adobe Systems Incorporated. All rights reserved.

Protected by U.S. Patents 5,737,599; 5,781,785; 5,819,301; 5,929,866; 5,943,063; 6,073,148; 6,515,763; 6,639,593; 6,754,382; 7,046,403; 7,213,269; 7,242,415; Patents pending in the U.S. and other countries.

All instances of the name PostScript in the text are references to the PostScript language as defined by Adobe Systems Incorporated unless otherwise stated. The name PostScript also is used as a product trademark for Adobe Systems' implementation of the PostScript language interpreter.

Except as otherwise stated, any reference to a "PostScript printing device," "PostScript display device," or similar item refers to a printing device, display device or item (respectively) that contains PostScript technology created or licensed by Adobe Systems Incorporated and not to devices or items that purport to be merely compatible with the PostScript language.

Adobe, the Adobe logo, PostScript, the PostScript logo, and PostScript 3 are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Linux is a registered trademark of Linus Torvalds. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are the property of their respective owners.



The PDF logo is a trademark or registered trademark of Adobe Systems Incorporated in the United States and other countries.

Copyright © 2008 Adobe Systems Incorporated. All rights reserved.

Protected by U.S. Patents 6,185,684; 6,205,549; 7,213,269; 7,272,628; 7,278,168; Patents pending in the U.S. and other countries.

All instances of the name PostScript in the text are references to the PostScript language as defined by Adobe Systems Incorporated unless otherwise stated. The name PostScript also is used as a product trademark for Adobe Systems' implementation of the PostScript language interpreter.

Except as otherwise stated, any reference to a "PostScript printing device," "PostScript display device," or similar item refers to a printing device, display device or item (respectively) that contains PostScript technology created or licensed by Adobe Systems Incorporated and not to devices or items that purport to be merely compatible with the PostScript language.

Adobe, the Adobe logo, Adobe LiveCycle® Policy Server, PostScript, the PostScript Logo, and PostScript 3 are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Trellix is a trademark or registered trademark of Musarubra US LLC or its affiliates in the US and other countries. Other names and brands may be claimed as the property of others.

Copyright © 2023 Musarubra US LLC

All brand names and product names appearing on this document are registered trademarks or trademarks of their respective owners.

Microsoft, Excel, Microsoft 365, Microsoft Edge, Microsoft Entra, Windows, Windows Mobile, Windows Phone, Windows Server are trademarks of the Microsoft group of companies.

■ Third-Party Software

For details about third-party software included in the manual, click the following icon:



For details about third-party software in the machine, see "Third-Party Software" at the online manual site.

<https://oip.manual.canon/>

■ Copyright

Unauthorized reproduction of the contents of this document in whole or in part is prohibited.

V_251107

About the Machine

About the Machine	16
Parts and Their Functions	18
Front Side	19
Back Side	21
Interior	23
Multi-Purpose Tray	24
Paper Drawer	25
Control Panel	26
Turning ON the Machine	29
Turning OFF the Machine	30
Loading Paper	31
Paper Loading Operations	32
Basic Paper Loading Method	33
Loading Envelopes	41
Loading Postcards	45
Loading Preprinted Paper	48
Specifying Paper Size and Type	51
Specifying Paper Size and Type in the Paper Drawer	52
Specifying Paper Size and Type in the Multi-purpose Tray	54
Registering Frequently Used Paper Size and Type for the Multi-purpose Tray	57
Registering Free Size Paper (Custom Size Paper)	59
Automatically Selecting the Appropriate Paper Source for a Specific Function	60
Main Unit Maintenance	61
Regular Cleaning	63
Cleaning the Exterior	64
Replacing the Toner Cartridge	65
Relocating the Machine	68
Replacement Parts	70
Checking the Remaining Amount of Consumables	72
Clearing Paper Jams	73
Paper Jams inside the Machine or in the Back Side	76
Paper Jams in a Paper Source	80
Paper Jams at the Duplex Transport Guide	83
Options	85
Optional Equipment	86

Paper Feeder PF-C 87

Hardware Specifications 88

 Main Unit 89

 Available Paper 91

 Paper Feeder PF-C 98

About the Machine

E9SJ-008

This chapter provides essential information for using the machine, such as parts and paper loading methods. You can also refer to this section for information on topics such as maintenance procedures for the main unit, dealing with paper jams, and the machine specifications.

■ Parts and Their Functions

This section describes the exterior and interior parts of the machine and their functions.



▶ Parts and Their Functions(P. 18)

■ Turning ON the Machine

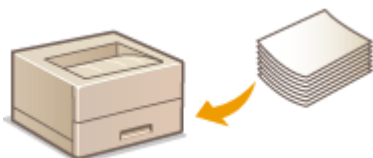
This section describes how to turn the machine ON or OFF.



▶ Turning ON the Machine(P. 29)

■ Loading Paper

This section describes how to load the paper into the paper drawer and multi-purpose tray.



▶ Loading Paper(P. 31)

■ Main Unit Maintenance

This section describes the maintenance and management of the machine, such as regular cleaning and the replacement of consumables.



▶ **Main Unit Maintenance(P. 61)**

■ **Clearing Paper Jams**

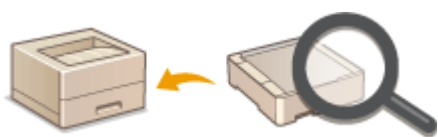
This section describes how to deal with paper jams that occur during machine use.



▶ **Clearing Paper Jams(P. 73)**

■ **Options**

See this section to check the optional equipment to use the machine more efficiently.



▶ **Options(P. 85)**

■ **Machine Specifications**

See this section for the specifications for the main unit and optional equipment units.

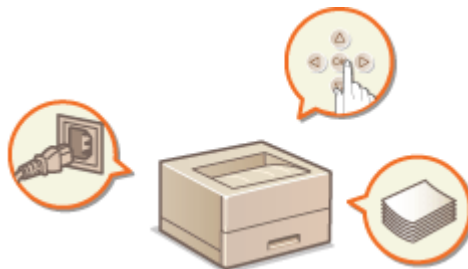


▶ **Hardware Specifications(P. 88)**

Parts and Their Functions

E9SJ-009

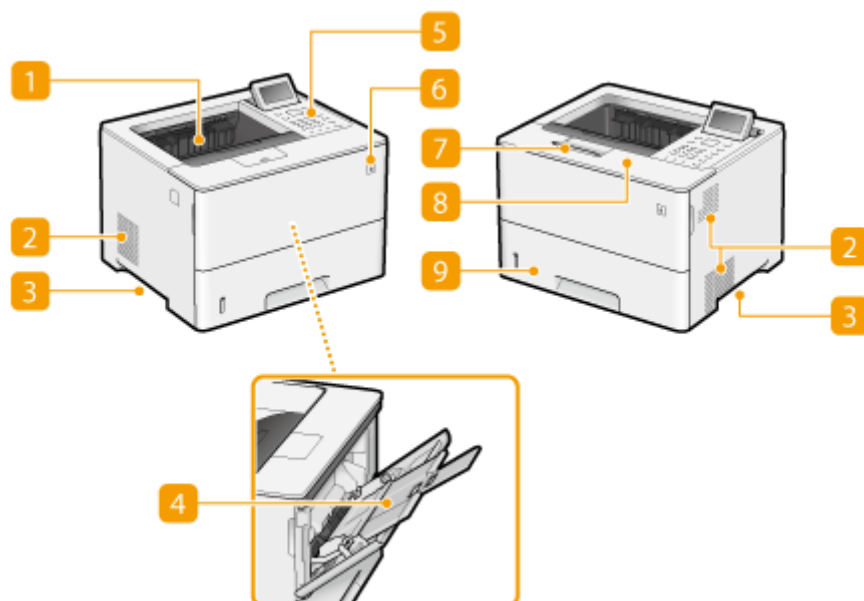
This section describes the parts of the machine (front side, back side, and interior) and how they function. This section also describes the names and usage of the keys on the control panel. Read this section for tips on how to use the machine properly.



- ▶ **Front Side(P. 19)**
- ▶ **Back Side(P. 21)**
- ▶ **Interior(P. 23)**
- ▶ **Multi-Purpose Tray(P. 24)**
- ▶ **Paper Drawer(P. 25)**
- ▶ **Control Panel(P. 26)**

Front Side

E9SJ-00A



1 Output tray

Printed paper is output to the output tray.

2 Ventilation slot

Air from inside the machine is vented out to cool down the inside of the machine. Note that placing objects in front of the ventilation slots prevents ventilation.

3 Lift handles

Hold the lift handles when carrying the machine. ▶ **Relocating the Machine(P. 68)**

4 Multi-purpose tray

Load the paper into the multi-purpose tray when you want to temporarily use a type of paper different from that which is loaded in the paper drawer.

▶ **Multi-Purpose Tray(P. 24)**

▶ **Basic Paper Loading Method(P. 33)**

5 Control Panel

The control panel consists of numeric keys, a display, status indicators, etc. You can perform all the operations and specify settings from the control panel.

▶ **Control Panel(P. 26)**

▶ **Basic Screens(P. 150)**

6 Power switch

Press the power switch to turn ON and turn OFF the machine.

▶ **Turning ON the Machine(P. 29)**

▶ **Turning OFF the Machine(P. 30)**

7 Paper stopper

Open the paper stopper to prevent paper in the output tray from falling.

8 Front cover

Open the front cover when replacing toner cartridges or removing jammed paper from inside the machine.

▶ **Replacing the Toner Cartridge(P. 65)**

▶ **Interior(P. 23)**

9 Paper drawer

Load the type of paper you frequently use into the paper drawer.

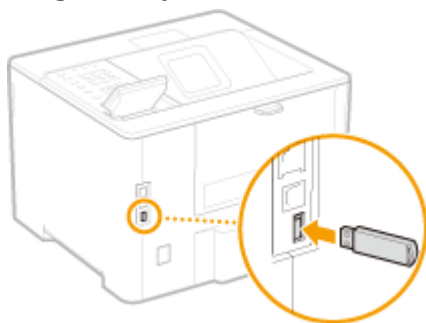
▶ **Paper Drawer(P. 25)**

▶ **Basic Paper Loading Method(P. 33)**

Connecting a USB Memory Device

You can connect a USB memory device to the USB port located on the back side of the machine, and directly print data from the USB memory device.

▶ **Using Memory Media(P. 202)**



! IMPORTANT

- Make sure that the USB memory device is oriented properly when connecting it to the machine. If it is not connected properly, it may cause the USB memory device or machine to malfunction.
- Make sure to follow the proper procedure when removing the USB memory device. ▶ **Inserting/Removing Memory Media(P. 202)** Failure to do so may cause the USB memory device or machine to malfunction.
- You can use a USB memory device with a FAT32 (up to 32 GB) or exFAT (up to 2 TB) file system.

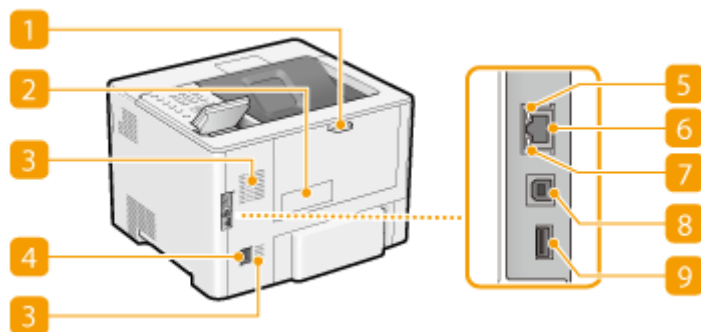
NOTE

Unsupported devices and usages

- Memory media with security functions
- Memory media that does not meet the USB specification
- Memory card readers connected via USB
- Connecting memory media via an extension cable
- Connecting memory media via a USB hub

Back Side

E9SJ-00C



1 Rear cover

Open the rear cover when clearing paper jams. ▶ **Paper Jams inside the Machine or in the Back Side(P. 76)**

2 Rating label

The label shows the serial number, which is needed when making inquiries about the machine. ▶ **When a Problem Cannot Be Solved(P. 558)**

3 Ventilation slot

Air from inside the machine is vented out to cool down the inside of the machine. Note that placing objects in front of the ventilation slots prevents ventilation. ▶ **Relocating the Machine(P. 68)**

4 Power socket

Connect the power cord.

5 ACT indicator

The ACT indicator blinks while data is being sent or received.

6 LAN port

Connect a LAN cable when connecting the machine to a wired LAN router, etc. ▶ **Setting up the Network Environment(P. 106)**

7 LNK indicator

The LNK indicator blinks green when the machine is properly connected to a network.

8 USB port (for computer connection)

Connect a USB cable when connecting the machine and a computer.

NOTE:

- The USB port (for computer connection) supports USB 2.0.

9 USB port (for USB device connection)

Connect a USB device that is used with MEAP applications. Also, connect a USB memory device when exporting or importing the settings of the machine. ▶<**Data Management**>(P. 491)

! IMPORTANT:

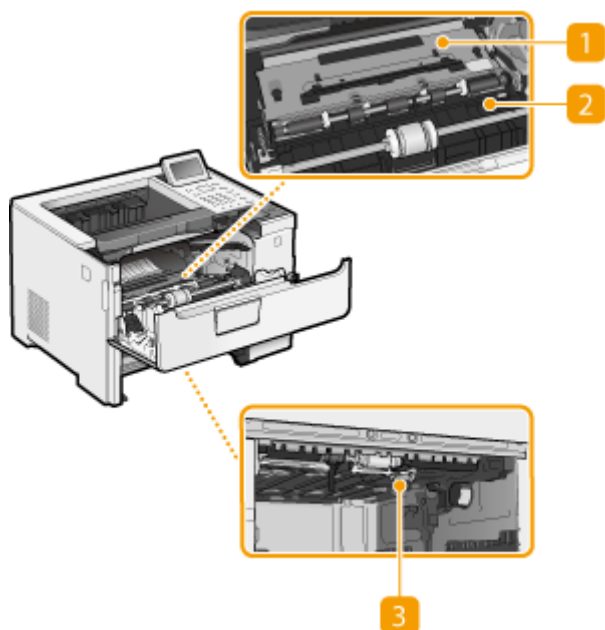
- The machine can supply a maximum power of 5 V 500 mA. Connecting a device that requires more power may damage the machine.

NOTE:

- The USB port (for USB device connection) supports USB 2.0.

Interior

E9SJ-00E



1 Transport guide (at the back)

If there is a paper jam inside the machine, raise the transport guide toward the front of the machine to remove the jammed paper. ▶ **Paper Jams inside the Machine or in the Back Side(P. 76)**

2 Transport guide (at the front)

If there is a paper jam inside the machine, raise the transport guide toward the back of the machine to remove the jammed paper. ▶ **Paper Jams inside the Machine or in the Back Side(P. 76)**

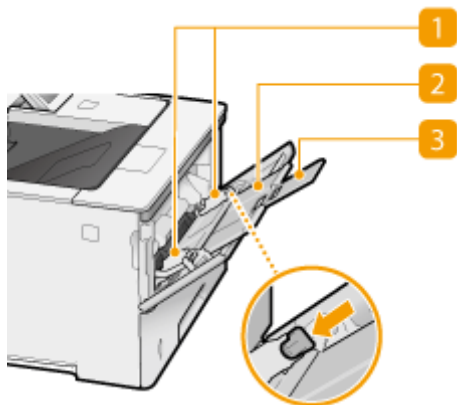
3 Duplex transport guide

If paper has jammed during 2-sided printing, lower the duplex transport guide to remove the jammed paper. ▶ **Paper Jams inside the Machine or in the Back Side(P. 76)**

Multi-Purpose Tray

E9SJ-00F

Use the multi-purpose tray when you want to print on a type of paper that is not loaded in the paper drawer, such as labels or envelopes.



1 Paper guides

Adjust the paper guides to exactly the width of the loaded paper to ensure that paper is fed straight into the machine. Press the lock release lever that is marked with arrow in the illustration to release the lock and slide the paper guides.

2 Paper tray

Pull out the paper tray when loading paper.

3 Tray extension

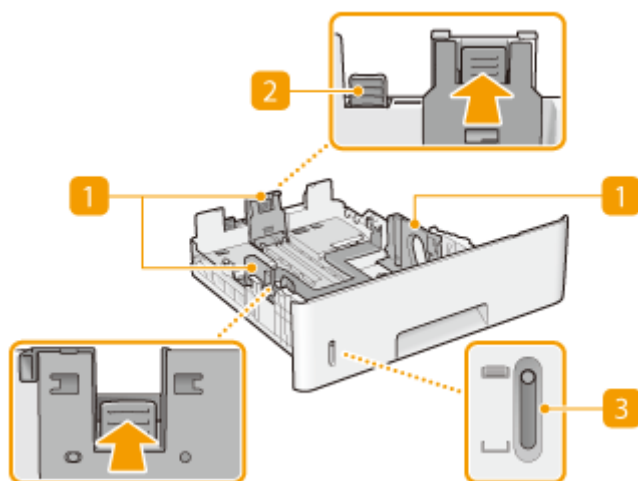
Open the tray extension when loading large paper.

LINKS

- ▶ **Loading Paper in the Multi-Purpose Tray(P. 38)**
- ▶ **Loading Envelopes in the Multi-Purpose Tray(P. 43)**
- ▶ **Loading Postcards in the Multi-Purpose Tray(P. 45)**

Paper Drawer

E9SJ-00H



1 Paper guides

Adjust the paper guides to exactly the size of the loaded paper to ensure that paper is fed straight into the machine. Press the lock release levers that are marked with arrows in the illustrations to release the locks and slide the paper guides.

2 Lock release lever (for extending the paper drawer)

When loading Legal size paper, the paper drawer needs to be extended. Press this lever to release the lock and extend the length of the paper drawer.

3 Paper level indicator

Indicates the remaining amount of paper. The mark moves downward as the remaining amount of paper decreases.

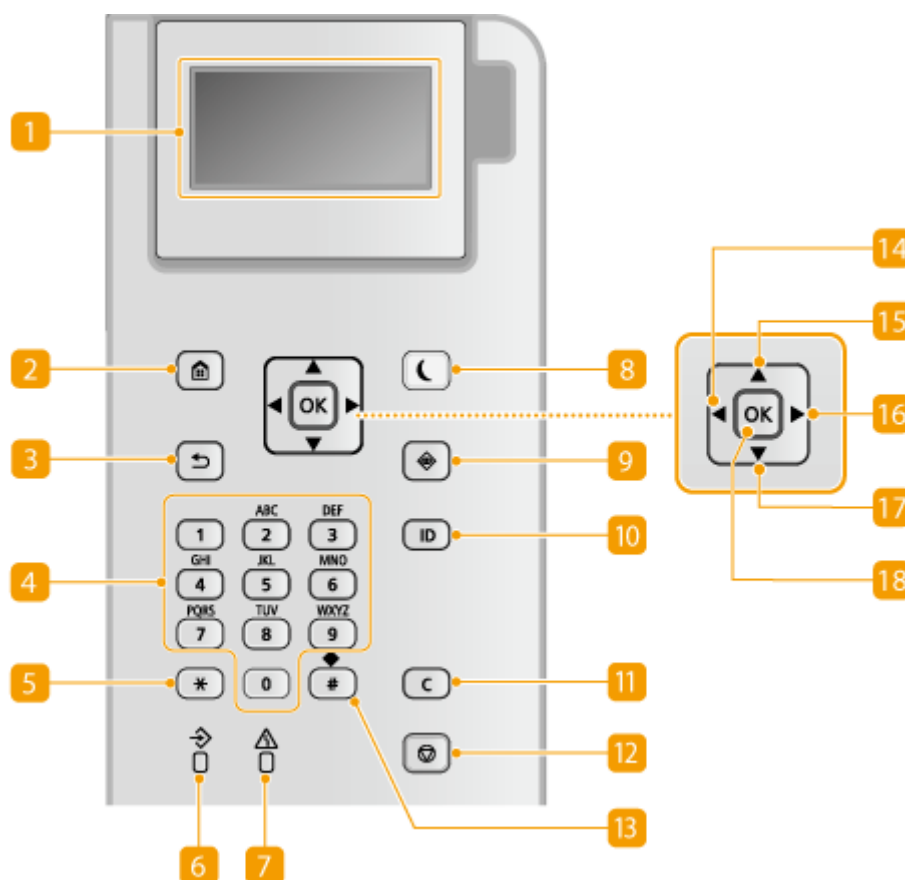
LINKS

▶ **Loading Paper in the Paper Drawer(P. 33)**

Control Panel

E9SJ-00J

This section describes the names and usage of the keys on the control panel.



1 Display

You can view the operation and error statuses of this machine, the amount remaining in the toner cartridges, and other conditions. ▶ **Basic Screens(P. 150)**

2 Home key

Press to display the Home screen, which provides access to the setting menu and functions such as Memory Media Print and paper settings. ▶ **Items Displayed on the <Home> Screen(P. 152)**

3 Back key

Press to return to the previous screen. If you press this key when specifying settings, for example, the settings are not applied and the display returns to the previous screen.

4 Numeric keys ([0]-[9] keys)

Press to enter numbers and text. ▶ **Entering Characters(P. 157)**

5 [*] key

Press to switch the type of text that is entered.

6 Data indicator

Blinks while an operation is being performed, such as data transmission or printing. Remains steadily lit when there are documents waiting to be processed.

7 Error indicator

Blinks or lights up when an error such as a paper jam occurs.

IMPORTANT:

- If the Error indicator blinks, follow the instructions that appear on the display. ➤ **Troubleshooting(P. 506)**
- If the Error indicator remains steadily lit, contact your dealer or service representative.

8 Energy Saver key

Press to put the machine into sleep mode. The key lights up green when the machine is in sleep mode. Press the key again to exit sleep mode. ➤ **Entering Sleep Mode(P. 164)**

9 Status Monitor key

Press to check the printing status, to view the usage history, or to view the network settings such as the IP address of the machine. You can also check the status of the machine, such as the remaining amount of paper and the amount remaining in the toner cartridges, or whether any errors occurred. ➤ **<Status Monitor> Screen(P. 150)**

10 [ID] key

Press after entering the ID and PIN to log on when Department ID Management is enabled. After you finish using the machine, press this key again to log off. ➤ **Logging into the Machine(P. 159)**

11 Clear key

Press to delete the entered numbers and text.

12 Stop key

Press to cancel printing and other operations.

13 [#] key

Press to enter symbols such as "@" or "/".

14 [◀] key

When specifying settings, press to return to the previous screen. When entering numbers, press to move the cursor to the left.

15 [▲] key

When specifying settings, press to select the item immediately above the currently selected item. When changing setting values, press to increase a value.

16 [▶] key

When specifying settings, press to proceed to the next screen. When entering numbers, press to move the cursor to the right.

17 [▼] key

When specifying settings, press to select the item immediately below the currently selected item. When changing setting values, press to decrease a value.

18 [OK] key

Press to apply settings or specified details.

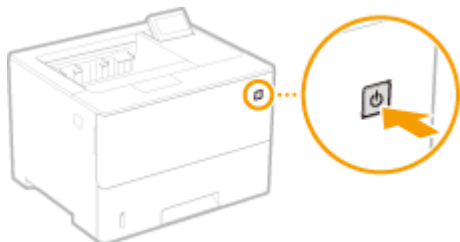
Turning ON the Machine

E9SJ-00K

This section describes how to turn ON the machine.

1 Make sure that the power plug is firmly inserted into the power outlet.

2 Press the power switch.



⇒ The startup screen appears on the display.

NOTE

- You can select the screen displayed immediately after the machine is turned ON. ▶<Default Screen After Startup/Restoration>(P. 446)
- The response of the keys on the control panel may not be optimal immediately after the machine is turned ON.
- If the machine is connected to a powered off Mac computer by USB cable, the computer may turn on automatically when this machine does. In this case, disconnect the USB cable from the machine. You may also be able to solve this problem by using a USB hub between the machine and the computer.

LINKS

▶Turning OFF the Machine(P. 30)

Turning OFF the Machine

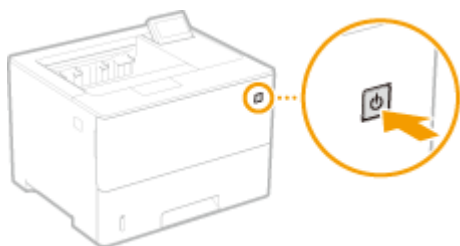
E9SJ-00L

This section describes how to turn OFF the machine.

NOTE

- You can shut down the machine from the Remote UI. ▶ **Turning OFF/Restarting the Machine(P. 336)**

1 Press the power switch.



NOTE

- The machine may take some time to completely shut down. Do not remove the power plug until the display and lamps turn OFF.
- To restart the machine, wait for at least 10 seconds after the system is turned off, and then turn the machine back ON. When <Quick Startup Settings for Main Power> is enabled, wait for at least 20 seconds to restart the machine. ▶ **<Quick Startup Settings for Main Power>(P. 448)**

LINKS

▶ **Turning ON the Machine(P. 29)**

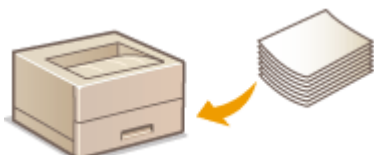
Loading Paper

E9SJ-00R

This section describes how to load the paper used for printing. You can check this section also for information on how to specify the paper size and type for loaded paper.

■ Paper Loading Operations

This section describes how to load the paper into the drawer and multi-purpose tray.



▶ **Paper Loading Operations(P. 32)**

■ Specifying Paper Size and Type

This section describes how to specify the paper size and type for the paper loaded into the paper source.



▶ **Specifying Paper Size and Type(P. 51)**

Paper Loading Operations

E9SJ-00S

You can load the paper into the paper drawer or multi-purpose tray. For more information about available paper types and sizes, see [▶Available Paper\(P. 91\)](#) . To obtain the optimum printing results, make sure to correctly specify the size and type of paper that is loaded. [▶Specifying Paper Size and Type\(P. 51\)](#)



[▶Basic Paper Loading Method\(P. 33\)](#)

[▶Loading Envelopes\(P. 41\)](#)

[▶Loading Postcards\(P. 45\)](#)

[▶Loading Preprinted Paper\(P. 48\)](#)

IMPORTANT

- Before using any paper, confirm the precautions regarding paper and the correct way to store it. [▶Available Paper\(P. 91\)](#)
- Loading paper while stock remains may cause a multiple sheet feed or a paper jam. If there is paper remaining, it is recommended that you wait until all of it has been used before loading more paper.
- Do not load different sizes or types of paper together.

LINKS

[▶Registering Free Size Paper \(Custom Size Paper\)\(P. 59\)](#)

[▶Paper Feeder PF-C\(P. 87\)](#)

Basic Paper Loading Method

E9SJ-00U

This section describes the general method for loading paper such as plain or recycled paper. Load frequently used paper types or sizes in the paper drawer. When temporarily using paper that is not loaded in the paper drawer, load it in the multi-purpose tray.

▶ **Loading Paper in the Paper Drawer(P. 33)**

▶ **Loading Paper in the Multi-Purpose Tray(P. 38)**

NOTE

- For the optional Paper Feeder PF-C, follow the procedure of paper drawer to load paper.
- If there are instructions on the paper package about which side of the paper to load, follow those instructions.
- Paper may overlap when it is fed or a paper jam may occur, depending on the cut surface of the paper. Changing the paper orientation and loading it again may reduce the effect of the cut surface.
- If paper runs out and printing is stopped, load a new paper stack. Printing restarts after the new paper stack is loaded.

Loading Paper in the Paper Drawer

▶ **Loading Standard Size Paper(P. 33)**

▶ **Loading a Custom Size Paper(P. 35)**

Paper Orientation

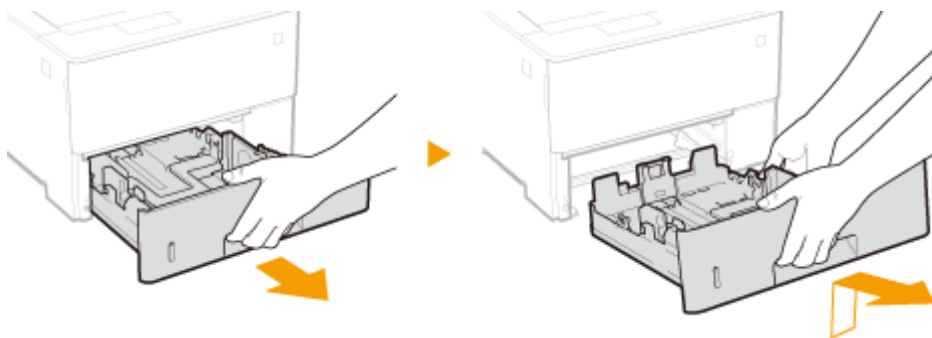
See the table below to load available paper in correct orientation.

Paper	Orientation
A4, B5, A5 (portrait), A6, Legal, Legal (India), Letter, Statement, Executive, Oficio, Brazil-Oficio, Mexico-Oficio, Government Letter, Government Legal, Australia Foolscap, Foolscap/Folio, 16K, F4A, Custom (portrait), Free (portrait)	
A5 (landscape), Custom (landscape), Free (landscape)	

■ Loading Standard Size Paper

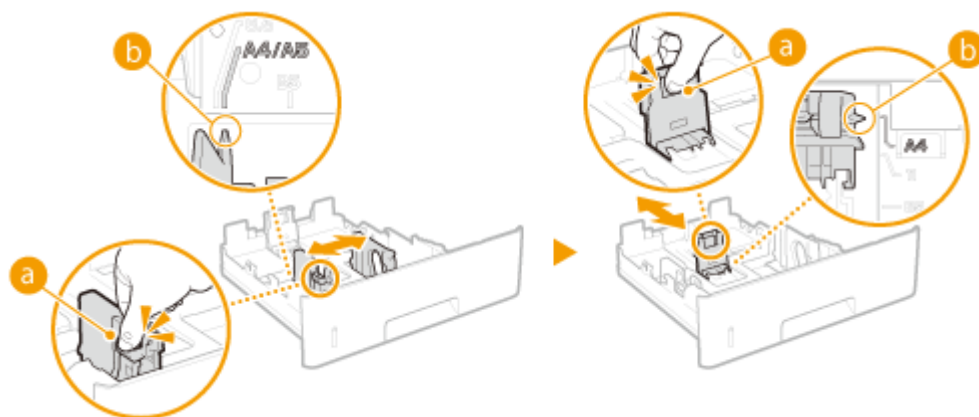
To load paper whose size is found in the paper size markings on the paper drawer, use the following procedure. For paper whose size is not found in the paper size markings, see ▶ **Loading a Custom Size Paper(P. 35)** .

- 1 Pull out the paper drawer until it stops, and remove it while lifting the front side.**



2 Adjust the positions of the paper guides to the paper size you want to use.

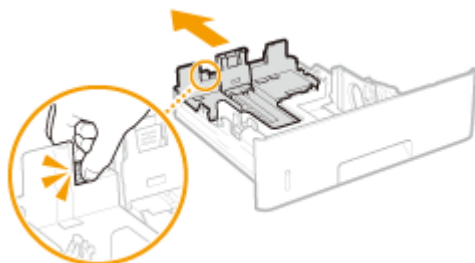
- Press the lock release lever (a) to align the projection (b) to the appropriate paper size marking.



NOTE:

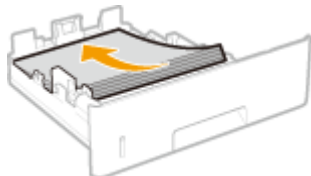
When loading Legal size paper

- Press the lock release lever, and extend the paper drawer.



3 Load the paper so that the edge of the paper stack is aligned against the paper guide on the rear side of the paper drawer.

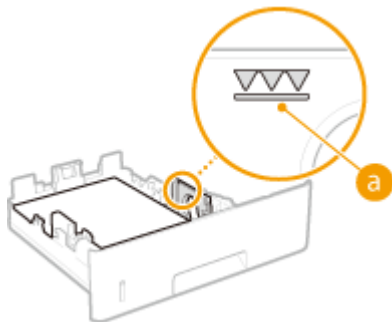
- Insert the paper with the print side face down.
- Fan the paper stack well, and tap it on a flat surface to align the edges.



! IMPORTANT:

Do not exceed the load limit line when loading paper

- Make sure that the paper stack does not exceed the load limit line (a). Loading too much paper can cause paper jams.

**NOTE:**

- When loading paper with a logo, see **▶ Loading Preprinted Paper (P. 48)**.

4 Insert the paper drawer into the machine.

» Continue to **▶ Specifying Paper Size and Type in the Paper Drawer (P. 52)**

! IMPORTANT:**When changing the paper size or type**

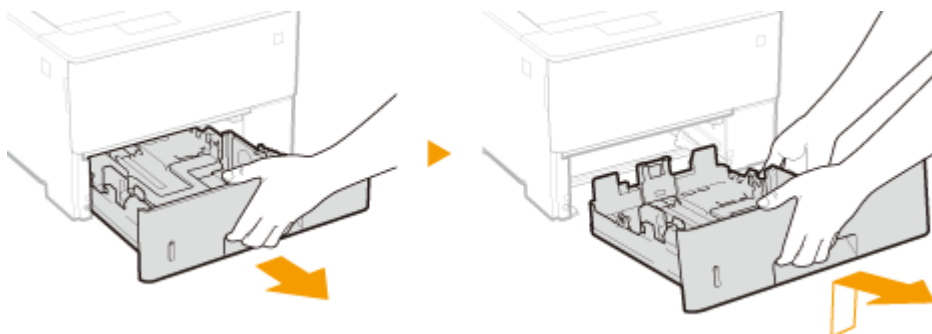
- The factory default settings for paper size and type are <A4> and <Free>, respectively. If you load a different size or type of paper into the machine, make sure to change the setting. If you do not change the paper size or type setting, the machine cannot print properly.

TIPS**Printing on the back side of printed paper (2nd Side of 2-Sided Page)**

- You can print on the back side of printed paper. Flatten any curls on the printed paper and insert it into the multi-purpose tray, with the side to print face up (previously printed side face down). Then select the paper type and select <Yes> for <Enable settings for 2nd side of 2-sided page?>.
- Use only the paper printed with this machine.
- You cannot print on the side that has previously been printed on.

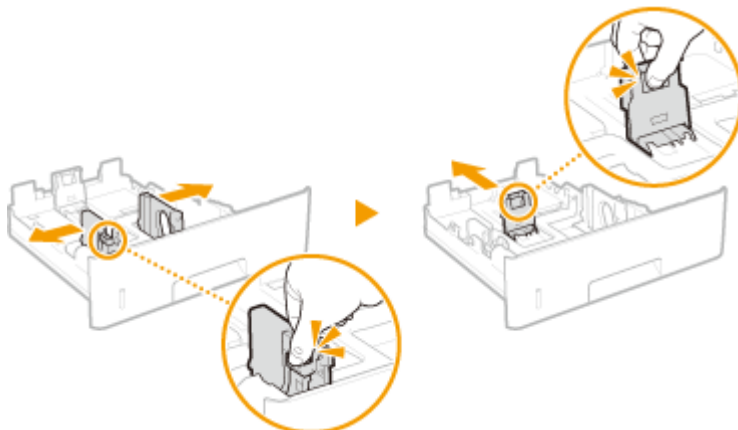
■ Loading a Custom Size Paper

To load custom size paper or other paper whose size is not found in the paper size markings on the paper drawer, use the following procedure.

1 Pull out the paper drawer until it stops, and remove it while lifting the front side.

2 Slide the paper guides apart.

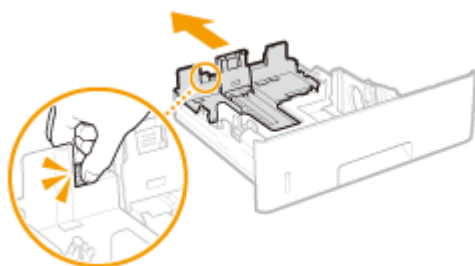
- Press the lock release lever to slide the paper guides outward.



NOTE:

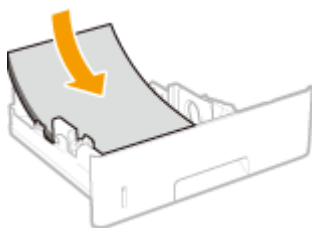
When loading longer paper than A4 size

- Press the lock release lever, and extend the paper drawer.



3 Load the paper so that the edge of the paper stack is aligned against the front side of the paper drawer.

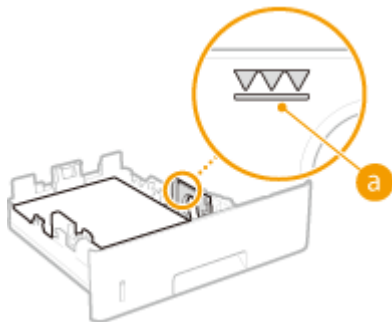
- Place the paper stack with the print side face down.
- Fan the paper stack well, and tap it on a flat surface to align the edges.



! IMPORTANT:

Do not exceed the load limit line when loading paper

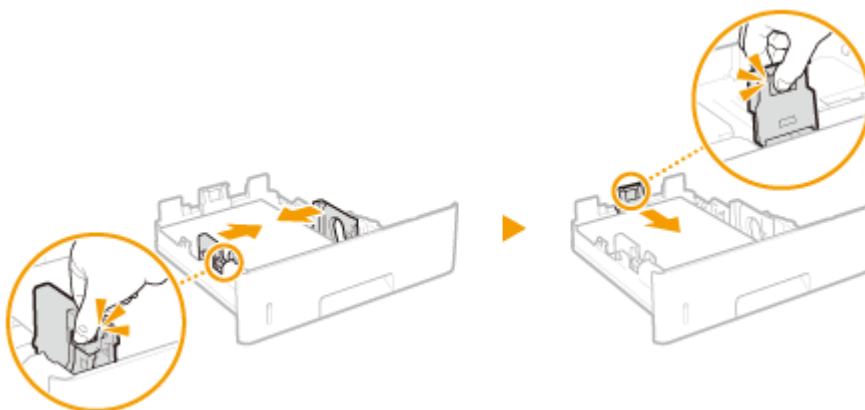
- Make sure that the paper stack does not exceed the load limit line (a). Loading too much paper can cause paper jams.

**NOTE:**

- When loading paper with a logo, see **▶ Loading Preprinted Paper (P. 48)**.

4 Align the paper guides against the edges of the paper.

- Press the lock release lever and slide the paper guides inward until they are aligned securely against the edges of the paper.

**! IMPORTANT:**

Align the paper guides securely against the edges of the paper

- Paper guides that are too loose or too tight can cause misfeeds or paper jams.

5 Insert the paper drawer into the machine.

» Continue to ▶ Specifying Paper Size and Type in the Paper Drawer (P. 52)

! IMPORTANT:

When changing the paper size or type

- If you load a different size or type of paper into the machine, make sure to change the settings. If you do not change the paper size or type setting, the machine cannot print properly.

TIPS**Printing on the back side of printed paper (2nd Side of 2-Sided Page)**

- You can print on the back side of printed paper. Flatten any curls on the printed paper and insert it into the multi-purpose tray, with the side to print face up (previously printed side face down). Then select the paper type and select <Yes> for <Enable settings for 2nd side of 2-sided page?>.
- Use only the paper printed with this machine.

- You cannot print on the side that has previously been printed on.

Loading Paper in the Multi-Purpose Tray

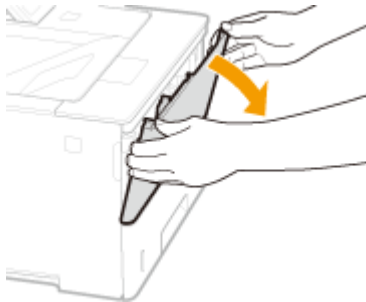
Paper Orientation

See the table below to load available paper in correct orientation.

Paper	Orientation
A4, B5, A5 (portrait), A6, Legal, Legal (India), Letter, Statement, Executive, Oficio, Brazil-Oficio, Mexico-Oficio, Government Letter, Government Legal, Australia Foolscap, Foolscap/Folio, 16K, F4A, 3"x5", Postcard, Reply Postcard, 4 on 1 Postcard, Envelope, Custom (portrait), Free (portrait)	
A5 (landscape), Custom (landscape), Free (landscape)	

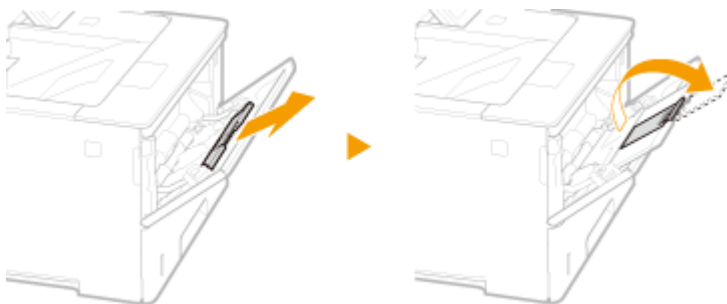
1 Open the cover.

- Hold the left and right side handles, and open the cover.



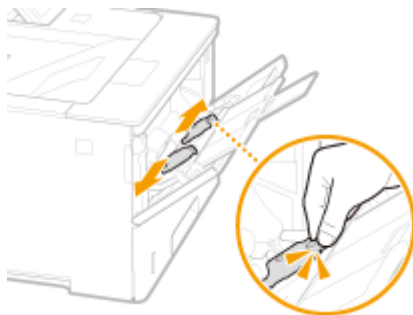
2 Pull out the paper tray and the tray extension.

- Pull out the tray extension when loading large paper.



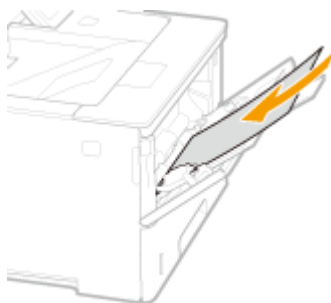
3 Spread the paper guides apart.

- Press the lock release lever to slide the paper guides outward.



4 Insert the paper into the multi-purpose tray until the paper stops.

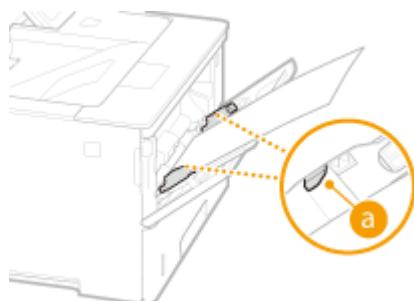
- Insert the paper with the print side face up.
- Fan the paper stack well, and tap it on a flat surface to align the edges.



! IMPORTANT:

Do not exceed the load limit guide when loading paper

- Make sure that the paper stack does not exceed the load limit guide (a). Loading too much paper can cause paper jams.

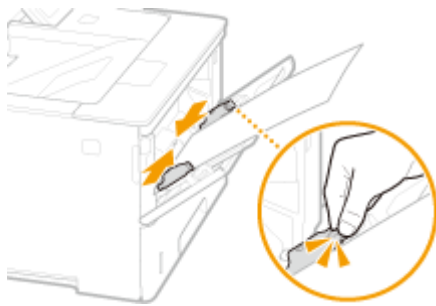


NOTE:

- If you use envelopes, postcards or paper with a logo mark, pay attention to the orientation when loading them in the paper source.
 - ▶ Loading Envelopes(P. 41)
 - ▶ Loading Postcards(P. 45)
 - ▶ Loading Preprinted Paper(P. 48) .

5 Align the paper guides against the edges of the paper.

- Press the lock release lever and slide the paper guides inward until they are aligned securely against the edges of the paper.



! IMPORTANT:

Align the paper guides securely against the edges of the paper

- Paper guides that are too loose or too tight can cause misfeeds or paper jams.

» Continue to **▶ Specifying Paper Size and Type in the Multi-purpose Tray(P. 54)**

! IMPORTANT:

When changing the paper size or type

- If you load a different size or type of paper into the machine, make sure to change the setting. If you do not change the paper size or type setting, the machine cannot print properly.

TIPS

Printing on the back side of printed paper (2nd Side of 2-Sided Page)

- You can print on the back side of printed paper. Flatten any curls on the printed paper and insert it into the multi-purpose tray, with the side to print face up (previously printed side face down). Then select the paper type and select <Yes> for <Enable settings for 2nd side of 2-sided page?>.
- Use only the paper printed with this machine.
- You cannot print on the side that has previously been printed on.

LINKS

▶ Available Paper(P. 91)

Loading Envelopes

E9SJ-00W

Load envelopes in the paper drawer or multi-purpose tray. When printing on envelopes, to prevent paper jams and wrinkles, make sure to flatten any curls on envelopes before loading them. Also pay attention to the orientation of envelopes and which side is face up. Note that neither envelopes nor postcards can be loaded in the paper drawer.

▶ **Before Loading Envelopes(P. 41)**

▶ **Loading Envelopes in the Multi-Purpose Tray(P. 43)**

NOTE

- This section describes how to load envelopes with the proper orientation, as well as procedures that you need to complete before loading envelopes. For a description of the general procedure for loading envelopes in the multi-purpose tray, see ▶ **Basic Paper Loading Method(P. 33)** .

Before Loading Envelopes

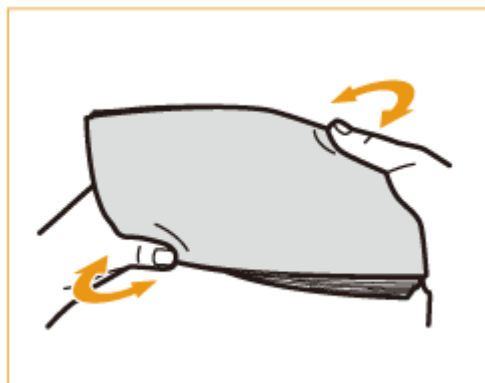
Follow the procedure below to prepare the envelopes before loading.

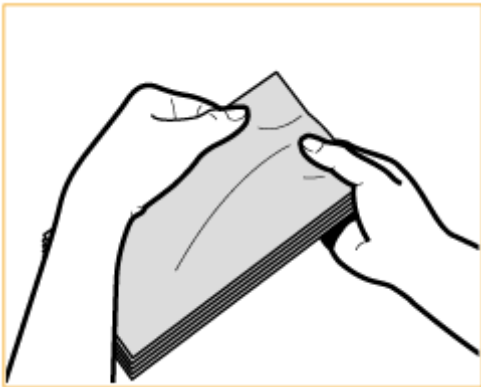
! IMPORTANT

- Do not use envelopes that have glue attached to their flaps, as the glue may melt due to the heat and pressure of the fixing unit.
- Envelopes may become creased, depending on the type of envelopes or the conditions in which they are stored.
- Streaks may appear where envelopes overlap.

1 Flatten any curls.

- Pick up about five envelopes. Flatten any curls, and loosen the stiff areas in the four corners.





- Repeat this step five times for each set of five envelopes.

2 Smooth the envelopes out, and remove any air inside them.

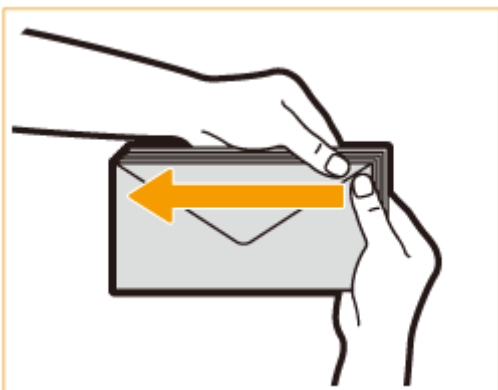
- Place the envelopes on a flat surface, and move your hands in the direction of the arrows to remove the air inside the envelopes.



- Repeat this step five times for each set of five envelopes.

3 Press down on the four sides.

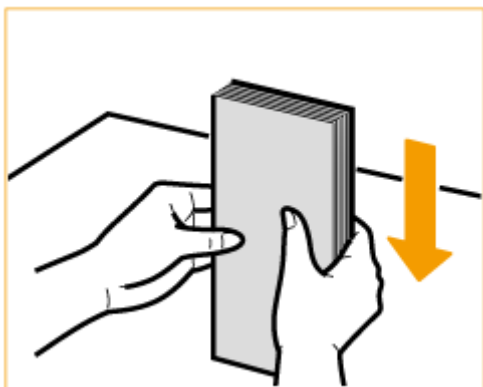
- Press down firmly on all four sides. In particular, carefully press down on the side facing the direction in which the envelopes will be fed. Press down firmly so that the flap stays flat.



! IMPORTANT:

- Failure to firmly press down on the flap may result in a paper jam. If this happens, press down firmly on all four sides of each individual envelope.

4 Align the envelopes on a flat surface.



NOTE:

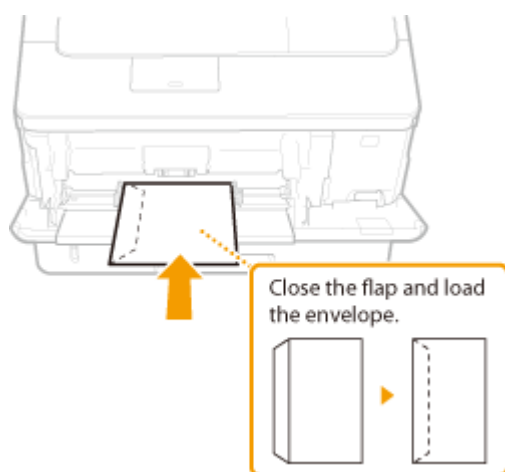
- Check that no envelopes are tucked underneath the flap of the envelope above or below them.

Loading Envelopes in the Multi-Purpose Tray

Load the envelopes in portrait orientation (with the short edge toward the machine), with the non-glued side (front side) face down. You cannot print on the reverse side of envelopes.

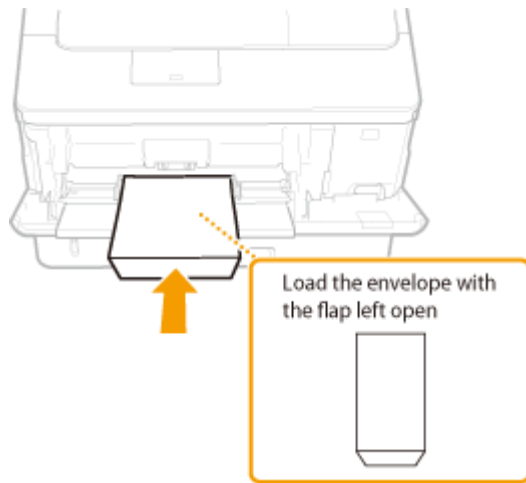
Yougatanaga 3, ISO-C5, Monarch, No. 10 (COM10), DL

Load the envelope so that the edge with the flap is toward the left side as shown in the illustration.



Nagagata 3, Nagagata 4, Nagagata 40

Insert the envelope with the flap toward you.



Loading Postcards

E9SJ-00X

Before loading postcards, make some preparations such as flattening any curls on them. Also pay attention to the orientation of postcards and which side is face up. Note that neither envelopes nor postcards can be loaded in the paper drawer.

▶ **Before Loading Postcards(P. 45)**

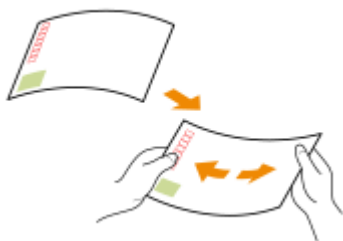
▶ **Loading Postcards in the Multi-Purpose Tray(P. 45)**

NOTE

- This section describes how to load postcards with the proper orientation, as well as procedures that you need to complete before loading postcards. For a description of the general procedure for loading postcards in the multi-purpose tray, see ▶ **Basic Paper Loading Method(P. 33)** .

Before Loading Postcards

Before loading the postcards, flatten any curls on them. With curls remaining, printouts may be skewed or images may be printed distorted. If the postcards curl downward, a paper jam is more likely to occur.



! IMPORTANT

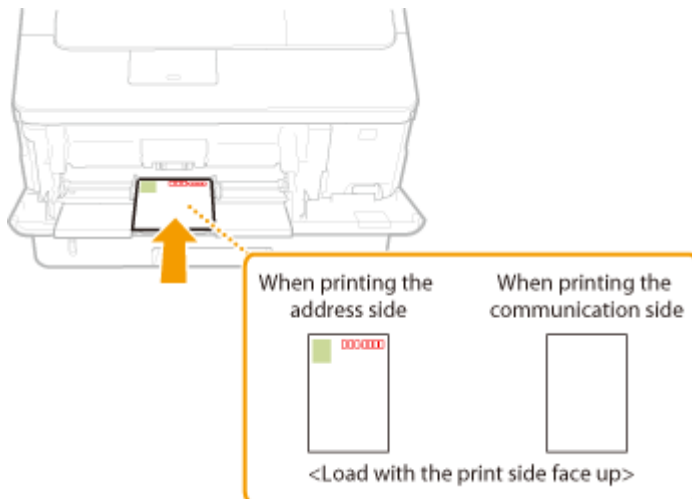
- The inkjet printable postcard cannot be used.

Loading Postcards in the Multi-Purpose Tray

Insert the postcard with the print side face up and with the short edge toward the machine if the type of postcard is regular or 4-on-1 or the long edge toward the machine if the type of postcard is reply.

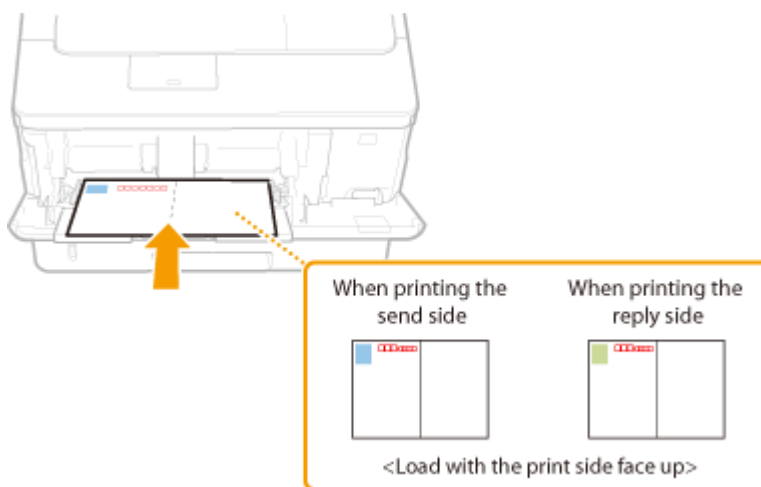
Postcard

Insert the postcard with the upper end toward the machine.



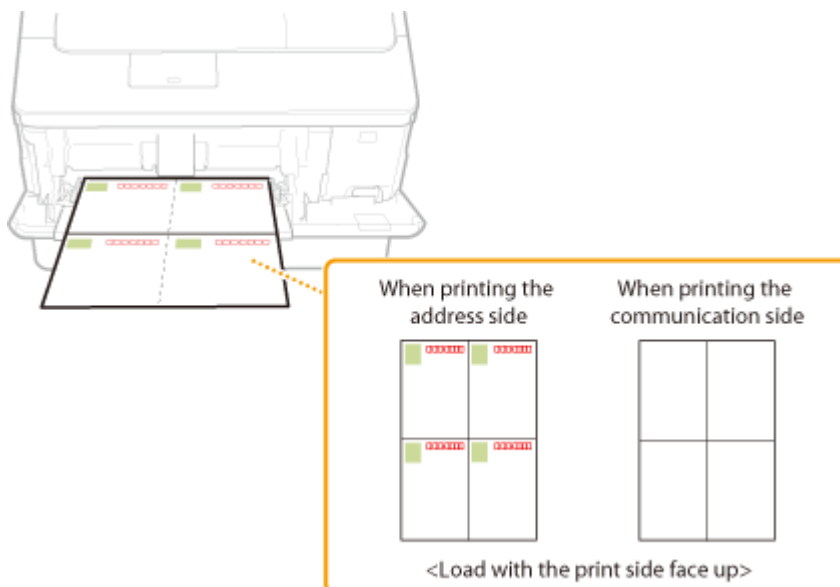
Reply Postcard

Unfold the postcard and insert it with the upper end toward the machine.



4 on 1 Postcard

Insert the postcard with the upper end toward the machine.



- Do not exceed the load limit guide when loading postcards. If the postcards are not fed properly, even if they have been prepared according to the procedures, load the postcards individually in the multi-purpose tray instead of loading several sheets together.

Loading Preprinted Paper

E9SJ-00Y

When you load paper that has been preprinted with a logo, pay attention to the orientation of the paper regardless of whether you use the paper drawer or the multi-purpose tray. Load the paper properly so that printing is performed on the same side as the logo.



▶ Loading Paper with Logos in the Paper Drawer(P. 48)

▶ Loading Paper with Logos in the Multi-Purpose Tray(P. 49)

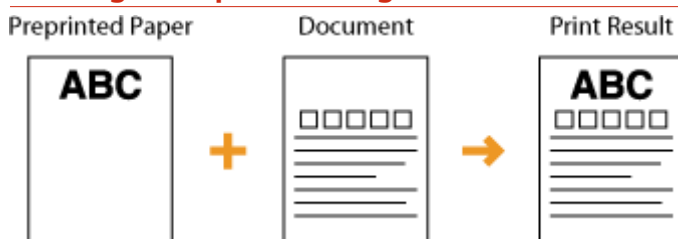
NOTE

- This section describes how to load preprinted paper with the proper orientation. For a description of the general procedure for loading paper in the paper drawer or multi-purpose tray, see ▶ **Basic Paper Loading Method(P. 33)** .
- Proper manner of loading preprinted paper when <Switch Paper Feed Method> is set to <Print Side Priority>
 - Paper drawer: the logo side face up
 - Paper source other than the paper drawer: the logo side face down

Loading Paper with Logos in the Paper Drawer

The loading method varies depending on whether the orientation of the logo printed paper is portrait or landscape.

Printing on Paper with Logos in Portrait Orientation



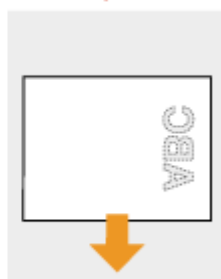
Load the paper with the logo side (the side to print the document) face down.

Loading Orientation

Portrait



Landscape (A5)



Printing on Paper with Logos in Landscape Orientation



Load the paper with the logo side (the side to print the document) face down.

Loading Orientation

Portrait



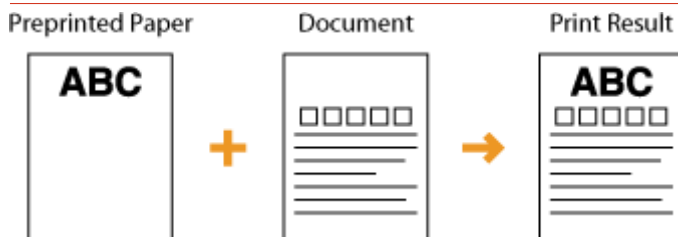
Landscape (A5)



Loading Paper with Logos in the Multi-Purpose Tray

The loading method varies depending on whether the orientation of the logo printed paper is portrait or landscape. Load the paper with the logo printed side (the side to print) face down, as shown in the following illustrations.

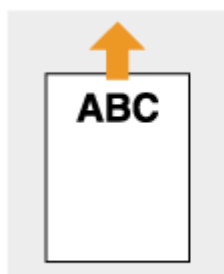
Printing on Paper with Logos in Portrait Orientation



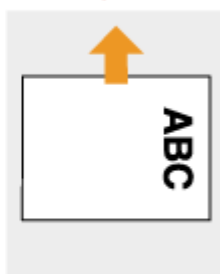
Load the paper with the logo side (the side to print the document) face up.

Loading Orientation

Portrait



Landscape (A5)



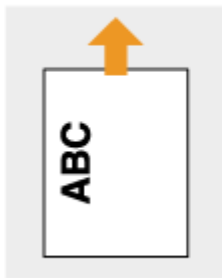
Printing on Paper with Logos in Landscape Orientation



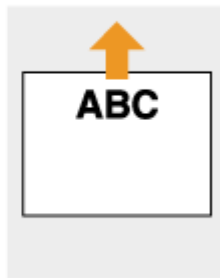
Load the paper with the logo side (the side to print the document) face up.

Loading Orientation

Portrait



Landscape (A5)



Specifying Paper Size and Type

E9SJ-010

You must specify the paper size and type settings to match the paper that is loaded. Make sure to change the paper settings when you load paper that is different from the previously loaded paper.

- ▶ **Specifying Paper Size and Type in the Paper Drawer(P. 52)**
- ▶ **Specifying Paper Size and Type in the Multi-purpose Tray(P. 54)**
- ▶ **Registering Frequently Used Paper Size and Type for the Multi-purpose Tray(P. 57)**
- ▶ **Registering Free Size Paper (Custom Size Paper)(P. 59)**
- ▶ **Automatically Selecting the Appropriate Paper Source for a Specific Function (P. 60)**

IMPORTANT

- If the setting does not match the size and type of loaded paper, a paper jam or printing error may occur.

NOTE

Batch importing/batch exporting

- <Paper Settings> can only be imported from/exported to the same series machines. ▶ **Importing/Exporting the Setting Data(P. 357)**
- <Paper Settings> is included in [Settings/Registration Basic Information] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

Specifying Paper Size and Type in the Paper Drawer

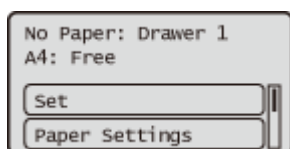
E9SJ-011

1 Load the paper in the paper drawer. **Basic Paper Loading Method(P. 33)**

When you open the paper drawer, the current paper settings are displayed on the top of the screen.

- If <Confirm When Loading Paper in Drawer> is set to <On>, the screen prompting the user to check the paper settings is displayed when the paper drawer is inserted into the machine.  **<Confirm When Loading Paper in Drawer>(P. 446)**
- To configure the paper settings later, select <Paper Settings> on the <Home> screen.

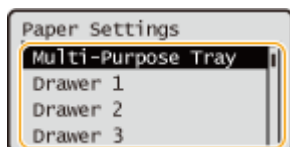
2 Check the paper size that is displayed.



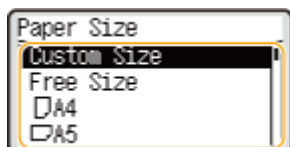
NOTE:

- If the displayed paper size is different from the loaded paper size, the paper may not be loaded properly. Load the paper again.

3 If the displayed paper size/type is different from the loaded paper size/type, select <Paper Settings>, and select the paper source in which paper is loaded.



4 Select the paper size .



NOTE:

About <Free Size>

- If you frequently need to change the paper to be loaded, set to <Free Size>; this will reduce the number of steps required to change the setting each time. You can also display an error message when the setting in the printer driver is significantly different from the size of the loaded paper.  **<Ppr Size Mismatch for Free Size Ppr Src>(P. 479)**

■When loading custom size paper

Specify the size of paper loaded in the paper drawer.

- 1 Select <Custom Size>.
- 2 Specify the length of the <X> side and <Y> side.



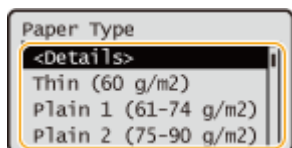
- Select <X> or <Y> to specify the length of each side using the numeric keys or ▲ / ▼ .

NOTE:

- By registering frequently used paper sizes to the <S1> to <S5> buttons, they can be recalled by selecting <Registered Sizes>. **▶Registering Free Size Paper (Custom Size Paper)(P. 59)**

- 3 Select <Apply>.

5 Select the paper type.



NOTE:

About <Free>

- If you frequently need to change the paper to be loaded, set to <Free>; this will reduce the number of steps required to change the setting each time. However, take note that this setting lets the machine perform printing even if there is mismatch between the paper type setting in the printer driver and the paper type actually loaded in the machine.
- When the paper type setting in the printer driver is [Auto], the machine operates the same way as when the paper type is [Plain 1].
- To check the detailed settings for a paper type, select <Details> ▶ select the paper type to check.

LINKS

▶Hardware Specifications(P. 88)

Specifying Paper Size and Type in the Multi-purpose Tray

E9SJ-012

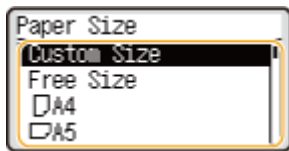
! IMPORTANT

- A paper jam or other printing problems may occur if the size and type of paper specified in the printer driver do not match those of the actual paper loaded in the multi-purpose tray.

1 Load the paper in the multi-purpose tray. Loading Paper in the Multi-Purpose Tray(P. 38)

⇒ The screen for specifying the paper size and type is displayed.

2 Specify the paper size.



NOTE:

About <Free Size>

- If you frequently need to change the paper to be loaded, set to <Free Size>; this will reduce the number of steps required to change the setting each time. You can also display an error message when the setting in the printer driver is significantly different from the size of the loaded paper.  <Ppr Size Mismatch for Free Size Ppr Src>(P. 479)
- If the displayed paper size is different from the loaded paper size, the paper may not be loaded properly. Load the paper again.

■When loading standard size paper

Select the paper size from <Paper Size>.

■When loading custom size paper

- Select <Custom Size>.
- Specify the length of the <X> side and <Y> side.



- Select <X> or <Y> to specify the length of each side using the numeric keys or ▲/▼.

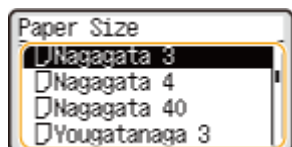
NOTE:

- By registering frequently used paper sizes to the <S1> to <S5> buttons, they can be recalled by selecting <Registered Sizes>. ➤ **Registering Free Size Paper (Custom Size Paper)(P. 59)**

3 Press <Apply>.

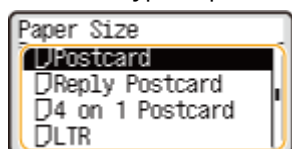
■When loading envelopes

1 Select the type of envelopes.



■When loading postcards

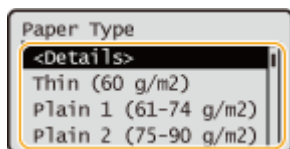
1 Select the type of postcards.



! IMPORTANT

- If you want to print on both sides of the postcard, first print on one side and then print on the other side.
- Before loading the postcards, flatten any curls on them.

3 Select the paper type.



NOTE:

About <Free>

- If you frequently need to change the paper to be loaded, set to <Free>; this will reduce the number of steps required to change the setting each time. However, take note that this setting lets the machine perform printing even if there is mismatch between the paper type setting in the printer driver and the paper type actually loaded in the machine.
- When the paper type setting in the printer driver is [Auto], the machine operates the same way as when the paper type is [Plain 1].
- To check the detailed settings for a paper type, select <Details> ► select the paper type to check.

LINKS

➤ **Hardware Specifications(P. 88)**

Registering Frequently Used Paper Size and Type for the Multi-purpose Tray

E9SJ-013

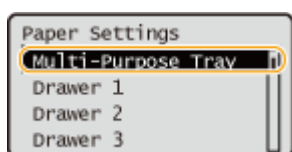
You can register default paper settings for the multi-purpose tray. Registering default settings can save yourself the effort of having to specify the settings each time you load the same paper into the multi-purpose tray.

NOTE

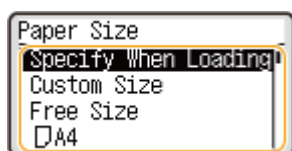
- After the default paper setting is registered, the paper setting screen is not displayed when paper is loaded, and the same setting is always used. If you load a different paper size or type without changing the paper settings, the machine may not print properly. To avoid this problem, select <Specify When Loading Paper> in step 3, and then load the paper.

1 Select <Paper Settings> on the <Home> screen.  <Home> Screen(P. 150)

2 Select <Multi-Purpose Tray>.



3 Select the paper size.



NOTE:

About <Free Size>

- If you frequently need to change the paper to be loaded, set to <Free Size>; this will reduce the number of steps required to change the setting each time. You can also display an error message when the setting in the printer driver is significantly different from the size of the loaded paper.  <Ppr Size Mismatch for Free Size Ppr Src>(P. 479)

When registering standard size paper

1 Select the standard size paper.

■When registering custom size paper

1 Press <Custom Size>.

2 Specify the length of the <X> side and <Y> side.



- Select <X> or <Y> to specify the length of each side using the numeric keys or ▲/▼.

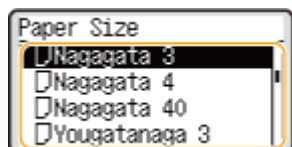
NOTE:

- By registering frequently used paper sizes to the <S1> to <S5> buttons, they can be recalled by selecting <Registered Sizes>. ➤ **Registering Free Size Paper (Custom Size Paper)(P. 59)**

3 Select <Apply>.

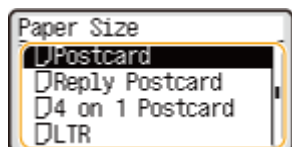
■When registering envelopes

1 Select the type of envelopes.



■When registering postcards

1 Select the type of postcards.



4 Select the paper type.

NOTE:

About <Free>

- If you frequently need to change the paper to be loaded, set to <Free>; this will reduce the number of steps required to change the setting each time. However, take note that this setting lets the machine perform printing even if there is mismatch between the paper type setting in the printer driver and the paper type actually loaded in the machine.
- When the paper type setting in the printer driver is [Auto], the machine operates the same way as when the paper type is [Plain 1].
- To check the detailed settings for a paper type, select <Details> ➤ select the paper type to check.

LINKS

- **Loading Paper in the Multi-Purpose Tray(P. 38)**
- **Hardware Specifications(P. 88)**

Registering Free Size Paper (Custom Size Paper)

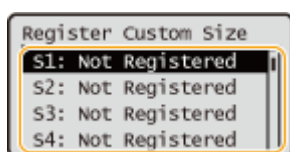
E9SJ-014

You can register up to five frequently used free sizes of paper. The paper sizes registered here are displayed on the paper size selection screen for the paper drawer and multi-purpose tray ([▶Specifying Paper Size and Type in the Paper Drawer\(P. 52\)](#) or [▶Specifying Paper Size and Type in the Multi-purpose Tray\(P. 54\)](#)).

1 Select **<Paper Settings>** on the **<Home>** screen. [▶<Home> Screen\(P. 150\)](#)

2 Select **<Register Custom Size>**.

3 Select a button from **<S1>** to **<S5>** ▶ select **<Register>**.



- You can assign an easy to remember name to the button by selecting **<Rename>**.
- If you have selected the registered button, select **<Edit>**.

4 Set the paper size.



- Specify the length of the **<X>** side and **<Y>** side. Select **<X>** or **<Y>** to specify the length of each side using the numeric keys or ▲/▼.

5 Select **<Apply>**.

LINKS

[▶Basic Paper Loading Method\(P. 33\)](#)

Automatically Selecting the Appropriate Paper Source for a Specific Function

E9SJ-015

You can enable or disable the automatic paper source selection function for each paper source. If this function is set to <On>, the machine automatically selects a paper source that is loaded with paper of the appropriate size for each print job. Also, when the paper in the selected paper source runs out, this function enables continuous printing by switching from that paper source to another that is loaded with paper of the same size.

NOTE

- Always specify <On> for at least one of the paper sources. If you select <Off> for all the paper sources, then you cannot finish the setting procedure.

- 1** Select <Set> on the <Home> screen.  <Home> Screen(P. 150)
- 2** Select <Function Settings> ► <Common> ► <Paper Feed Settings> ► <Paper Source Auto Selection>.
- 3** Select the function.
 - <Other> enables you to make settings for a paper source that is used for outputting reports.
- 4** Select <On> for each paper source that you want to be selected automatically.

If you selected <Printer> in step 3

Set whether to put multiple paper sources in a group. If paper source grouping is specified, paper source selection is automatically performed within a group when you print by specifying any paper source belonging to that group. To specify paper source grouping, select <Group Settings> ► set <Use Group> to <On> ► select the paper source ► select a group which you want to put each paper source in ► select <Apply>.

Main Unit Maintenance

E9SJ-016

This section describes the maintenance and management of the machine, such as regular cleaning and the replacement of consumables. It also describes the maintenance service provided by Canon. For information on precautions to take during maintenance, see the Important Safety Instructions.

! IMPORTANT

Maintenance and Inspections

- The minimum holding period for performance parts for repairs and toner cartridges is seven (7) years after production of the machine model is discontinued.
- If a problem occurs during operation, see " **▶ Troubleshooting(P. 506)** " in the User's Guide. If the problem still cannot be resolved or you think the machine needs to be checked, contact your dealer or service representative.

Installation

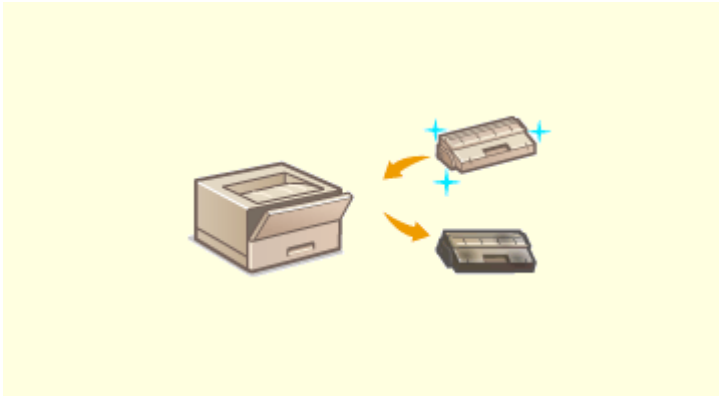
- If you find the machine's operation to be noisy in some operating modes or due to your surroundings, we recommend setting up the machine in a separate location from your office.
- Water droplets (condensation) may form inside the machine if the room where the machine is installed is heated rapidly, or if the machine is moved from a cool, dry location to a warm, humid location. Using the machine under these conditions may result in problems such as paper jams, poor print quality, or faults. Let the machine adjust to the ambient temperature and humidity for at least two hours before use.
- The machine may not operate properly when used at high altitudes (3,000 meters (3,280 yards) above sea level or higher).

■ Basic Cleaning

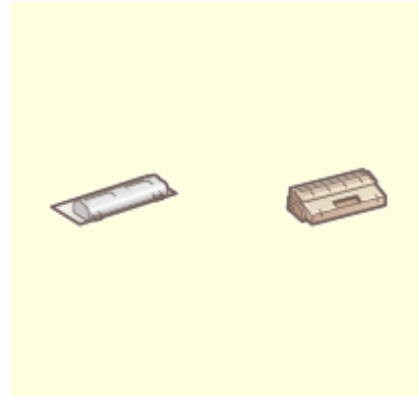


▶ Regular Cleaning(P. 63)

■ Replacing Consumables



▶ Replacing the Toner Cartridge(P. 65)

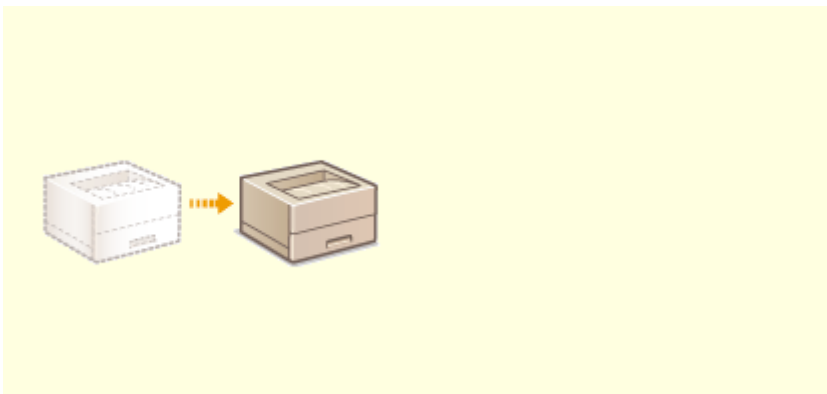


▶ Replacement Parts(P. 70)



▶ Checking the Remaining Amount of Consumables(P. 72)

■ Other Maintenance and Adjustment

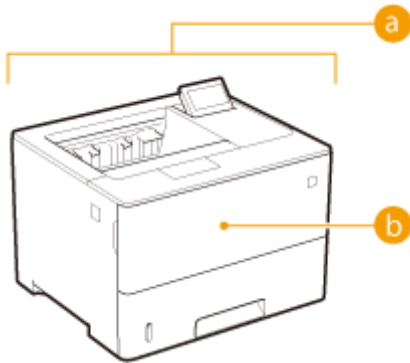


▶ Relocating the Machine(P. 68)

Regular Cleaning

E9SJ-017

It is recommended that you periodically clean the machine to prevent loss of print quality and enable you to use the machine comfortably and safely.



a Exterior of the machine and ventilation slots ▶ **Cleaning the Exterior(P. 64)**

b Pressure roller for fixing ▶ **<Clean Pressure Roller for Fixing>(P. 474)**

Cleaning the Exterior

E9SJ-018

Regularly wipe the exterior of the machine, especially around the ventilation slots, to keep the machine in good condition.

1 Turn the power OFF, and remove the power plug from the power outlet.

▶Turning OFF the Machine(P. 30)

! IMPORTANT:

- Check the operation status of the machine before turning the power OFF. You can turn the power OFF even if the machine is executing an operation, but this may cause the operation to be interrupted or data to become damaged.

2 Wipe the surface of the machine.

- Wet a soft cloth with water or diluted mild detergent, wring the cloth out well, and wipe the machine.
- To locate the ventilation slots, see ▶Front Side(P. 19) and ▶Back Side(P. 21) .



- Wait until the moisture has completely dried before proceeding to the next step.

3 Insert the power plug into the power outlet, and turn the power ON.

▶Turning ON the Machine(P. 29)

Replacing the Toner Cartridge

E9SJ-019

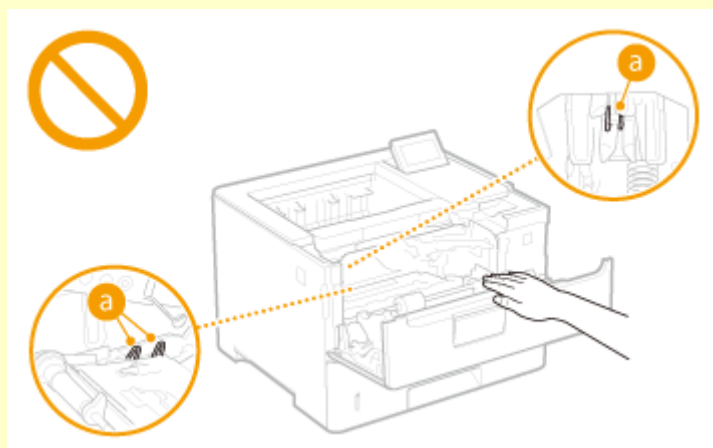
When toner starts running low or has run out, a message is displayed prompting you to prepare a new toner cartridge or perform toner cartridge replacement. Prepare a new toner cartridge or perform toner cartridge replacement according to the displayed message.

- ▶ **Cautions When Replacing the Toner Cartridge(P. 65)**
- ▶ **Procedure for Replacing the Toner Cartridge(P. 66)**

Cautions When Replacing the Toner Cartridge

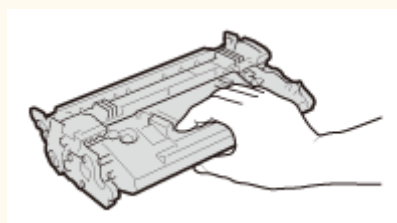
CAUTION

- Do not touch the contacts (**a**) inside the machine. Doing so may result in damage to the machine.

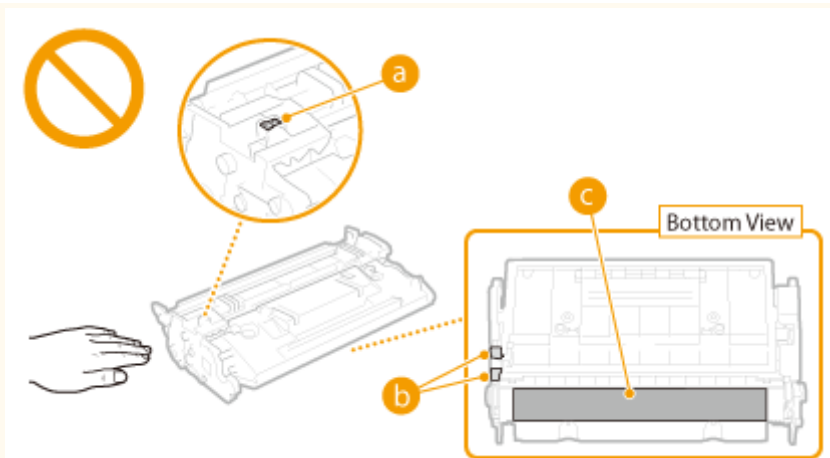


IMPORTANT

- Do not replace toner cartridges until the message prompting you to do so appears.
- Be sure to hold the toner cartridge using the handle.



- Do not touch the toner cartridge memory (**a**), the electrical contacts (**b**) or the drum (**c**).



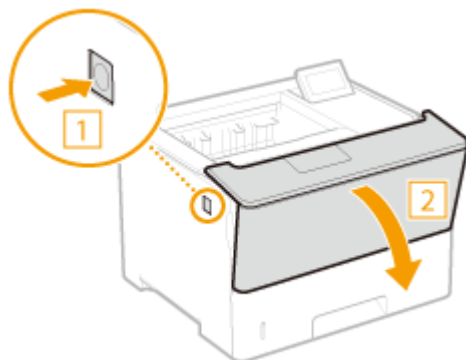
NOTE

- For details about each message, see ▶ **Countermeasures for Each Message(P. 532)** .
- For information on the product numbers for toner cartridges, see ▶ **Consumables(P. 70)** .
- You can check the current amount of toner remaining. ▶ **Checking the Remaining Amount of Consumables(P. 72)**

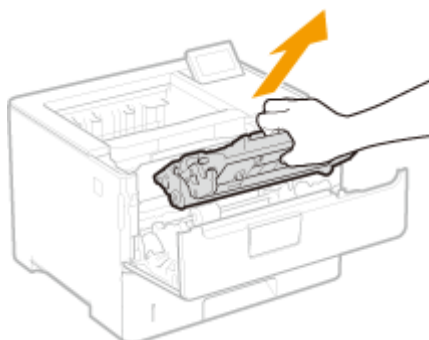
Procedure for Replacing the Toner Cartridge

Read the precautions in ▶ **Replacement Parts(P. 70)** before replacing the toner cartridges.

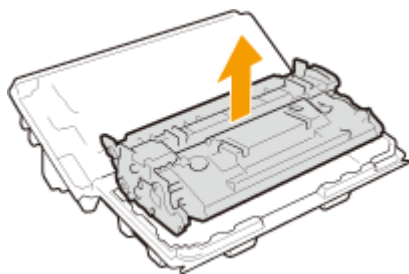
1 Press the button to open the Front cover.



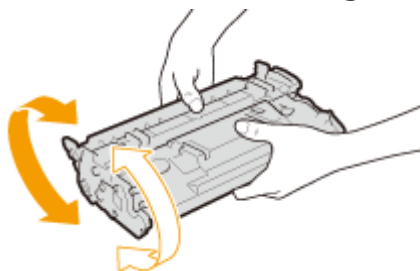
2 Pull out the toner cartridge.



3 Remove the replacement toner cartridge from the protective case.

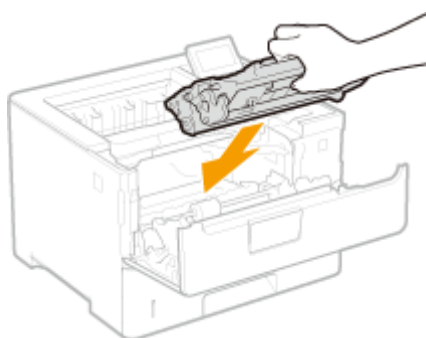


4 Shake the toner cartridge five or six times as shown below to evenly distribute the toner inside the cartridge.



5 Install the toner cartridge.

- Fully push it in until it cannot go any further.



6 Close the front cover.

Relocating the Machine

E9SJ-01A

The machine is heavy. Make sure to follow the procedures below to avoid injury when moving the machine. Also, to confirm the safety precautions before you begin to move, read the Important Safety Instructions included with the machine.

! IMPORTANT

- If the machine is to be transported for relocation, removals, etc., take the following steps to prevent damage and faults during transportation:
 - Remove the toner cartridges.
 - Securely pack the machine in the original packaging (box) and packing materials.

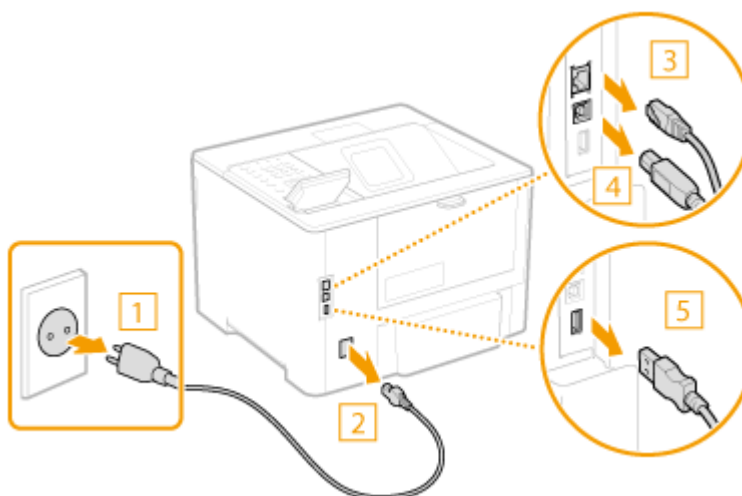
1 Turn OFF the machine and computer.

▶Turning OFF the Machine(P. 30)

2 Disconnect the cables and cord from the machine in numerical order as in the illustration below.

- Whether the cables with "*" are connected depends on your environment.

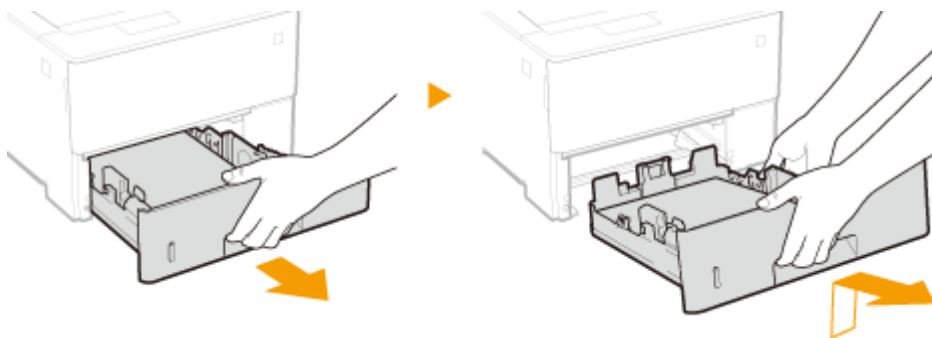
- 1 Power plug
- 2 Power cord
- 3 LAN cable*
- 4 USB cable*
- 5 USB device *



3 When transporting the machine across a long distance, remove the toner cartridge.

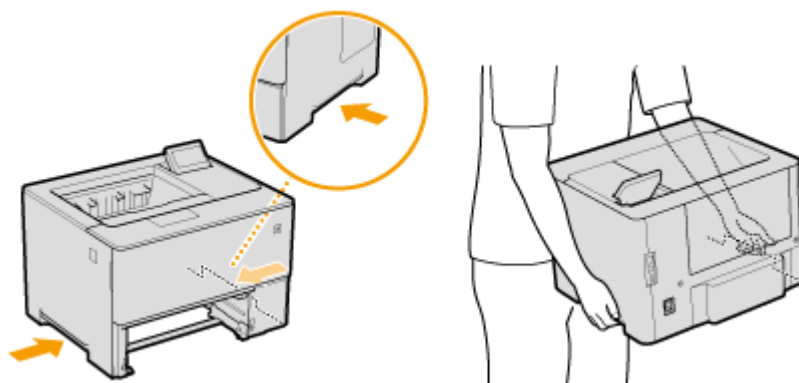
▶Replacing the Toner Cartridge(P. 65)

4 Pull out the paper drawer until it stops, and remove it while lifting the front side.



5 Close all the open covers and multi-purpose tray, and move the machine to a new location.

- The machine is heavy (▶ **Hardware Specifications(P. 88)**). Do not try hard to carry the machine.
- Position yourself toward the front side of the machine and hold the lift handles, then lift up the machine.



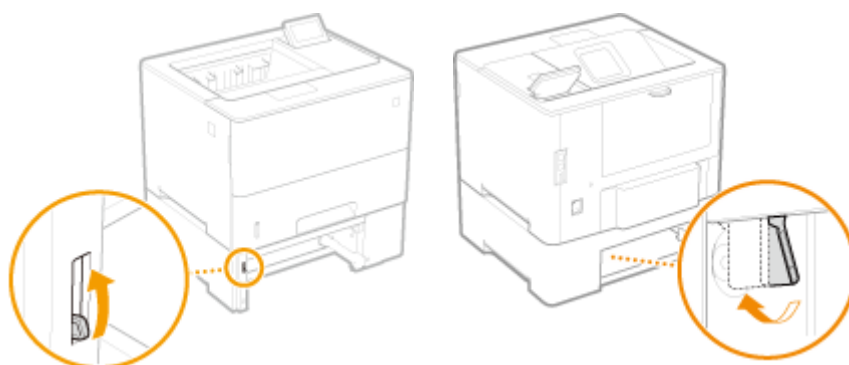
! IMPORTANT:

If the optional paper feeder is attached to the machine.

- Unlock the paper feeder before lifting the machine, and transport the paper feeder separately.

Front Side

Back Side



6 Carefully place the machine at the new installation site.

- For information about how to install the machine after relocating it, see Setup Guide. ▶ **Manuals and Their Contents(P. 9)**

Replacement Parts

E9SJ-01C

This section describes the replacement parts (consumables/consumable parts) used by the machine. Follow the precautions when handling and storing the replacement parts.

For optimum print quality, using Canon genuine toner cartridges is recommended.

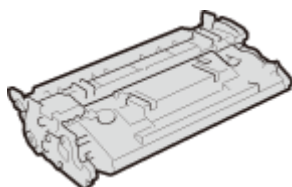


NOTE

- Depending on the installation environment, printing paper size, or document type, you may need to replace consumables before the end of the estimated lifetime.
- You can check the current amount of replacement parts remaining.
Checking the Remaining Amount of Consumables(P. 72)

Consumables

■ Toner Cartridge



Supplied Toner Cartridge

The average yield of the toner cartridge that comes with the machine are shown below.

Average yield *: 5,100 Sheets

Replacement Toner Cartridge

Canon Genuine Toner Cartridge	Average yield and weight of toner cartridge
Canon Cartridge 056 L Black	Average yield * 5,100 Sheets
Canon Cartridge 056 Black	Average yield * 10,000 Sheets
Canon Cartridge 056 H Black	Average yield * 21,000 Sheets

* The average yield is based on "ISO/IEC 19752" (the global standard related to "Method for the determination of toner cartridge yield for monochromatic electrophotographic printers and multi-function devices that contain printer components" issued by ISO [International Organization for Standardization]) when printing A4 size paper with the default print density setting.

CAUTION

Store toner cartridges as described below

Storing toner cartridges in an improper location or environment may cause problems such as data loss.

- Store unopened until immediately prior to use.
- Store toner cartridges in the following conditions:
 - Storage temperature range: 0-35°C
 - Storage humidity range: 35% to 85% RH (relative humidity, condensation-free)*

*Even within the approved storage humidity range, water droplets (condensation) may develop inside the toner cartridge if the temperatures inside and outside the toner cartridge differ. Condensation will adversely affect the print quality.

- Do not store toner cartridges in the following locations:
 - Locations exposed to open flames
 - Locations exposed to direct sunlight or bright light for five minutes or more
 - Locations exposed to excessively salty air
 - Locations heavily exposed to corrosive gases (e.g. aerosol sprays or ammonia)
 - Very hot and/or humid locations
 - Locations subject to dramatic changes in temperature and humidity likely to cause condensation
 - Very dusty locations
 - Locations within the reach of children
 - Locations close to products affected by magnetism (e.g. floppy disks or disk drives)
- Do not store toner cartridges upright or upside down.
- Store the packaging material safely for future use. It will be needed for situations such as storing the machine with the toner cartridges removed.
- Canon reserves the right to reposition, reshape, add or remove packaging material without notice.

IMPORTANT

Be careful of counterfeit toner cartridges

- Please be aware that there are counterfeit Canon toner cartridges in the marketplace. Use of counterfeit toner cartridge may result in poor print quality or machine performance. Canon is not responsible for any malfunction, accident or damage caused by the use of counterfeit toner cartridge.
For more information, see global.canon/ctc.

NOTE

- For information on the collection of used toner cartridges, see the  **Disclaimers(P. 11)** .

Checking the Remaining Amount of Consumables

E9SJ-01E

Perform the procedures below to check the remaining amount of consumables. In particular, check whether you need to prepare a new toner cartridge before printing a large quantity of documents.



 (Status Monitor) ▶ <Device Status> ▶ <Consumables Information>

TIPS

- You can check the remaining amount of consumables from the Remote UI. [▶Checking the Machine Status\(P. 335\)](#)

LINKS

- [▶Replacing the Toner Cartridge\(P. 65\)](#)
- [▶Countermeasures for Each Message\(P. 532\)](#)

Clearing Paper Jams

E9SJ-01F

If a paper jam occurs, a message, the location of the paper jam, and the procedure for clearing it are displayed on the screen. If you do not know how to clear the paper jam from viewing the screen, see **Paper Jam Locations(P. 74)** to clear the paper jam. For information on cautions when clearing paper jams, see the Important Safety Instructions.

CAUTION

- Do not forcibly remove the jammed paper from the machine. Forcibly removing the paper may result in injury or damage parts of the machine.
 - If you cannot remove the paper, contact your dealer or service representative.
- When all paper jams have been cleared, immediately remove your hands from the machine and optional equipment so that your clothing and hands do not get caught in the rollers.

IMPORTANT

Cautions when clearing paper jams

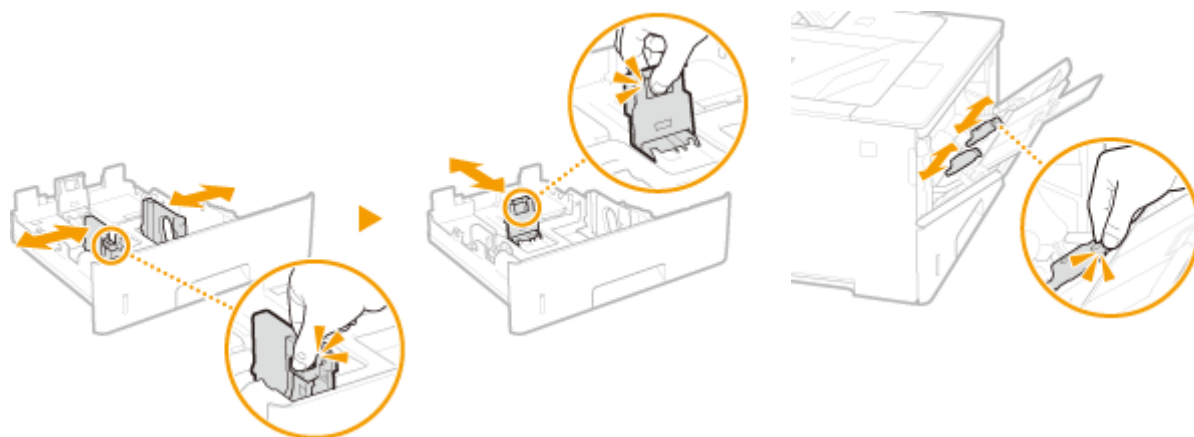
- When clearing paper jams, do not turn the power OFF. Data being printed is erased when you turn the power OFF.
- When the paper gets torn, be sure to remove the torn pieces so that they do not remain.

■ If Paper Jams Frequently Occur

If paper jams frequently occur even though there are no problems with the machine and its optional equipment, check the following.

Are the paper guides misaligned?

- Match the paper guides with the paper loaded in the paper source.

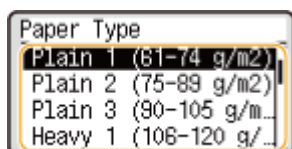


Do sheets of paper overlap when being fed?

- If paper jams occur due to overlapping of sheets of paper when being fed, reload the paper by changing the orientation.

Is the paper type correct?

- On the <Paper Type> display, check the paper type. **▶Specifying Paper Size and Type(P. 51)**



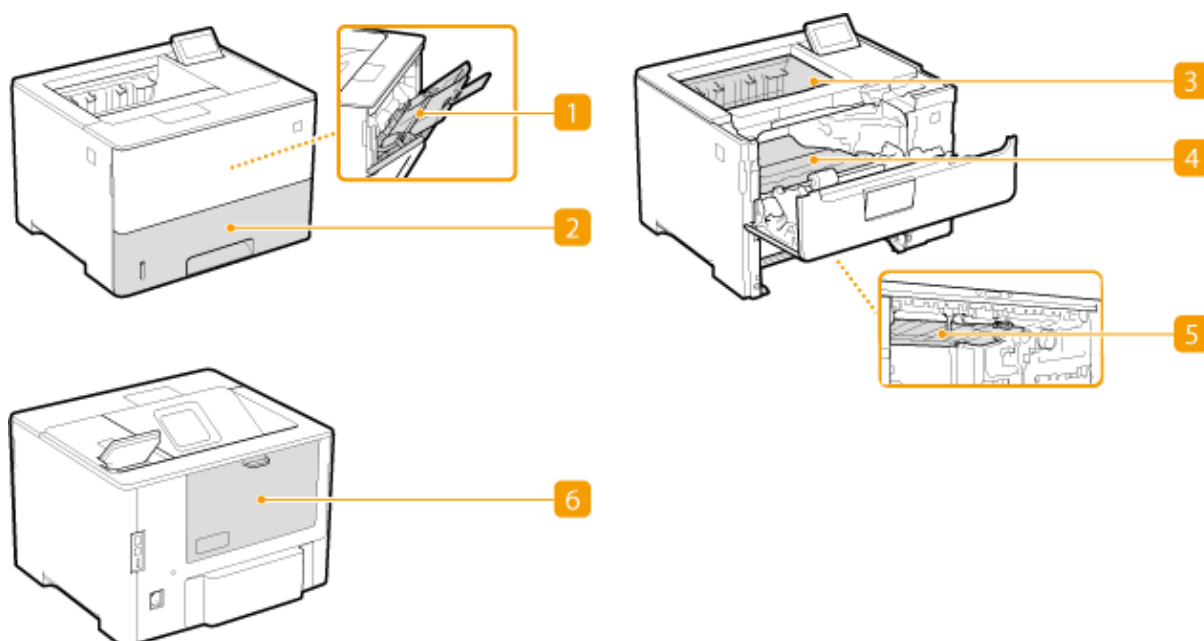
- If the paper loaded in a paper source differs from the paper type setting, see **▶Paper Loading Operations(P. 32)** to set the paper type again.

Do pieces of paper remain in the machine?

- Pieces of paper may remain in the machine after removing a paper jam. Open the location where the paper was jammed, and remove any pieces of paper (Do not forcibly remove the jammed paper from the machine. Forcibly removing the paper may result in injury or damage parts of the machine. If you cannot remove the paper, contact your dealer or service representative.).

Paper Jam Locations

For information on the paper jam locations and the method for clearing paper jams, see the following diagram and references.



- 1** Multi-purpose tray **▶Paper Jams in the Multi-Purpose Tray(P. 80)**
- 2** Paper drawer **▶Paper Jams in the Paper Drawer(P. 81)**
- 3** Output tray **▶Paper Jams inside the Machine or in the Back Side(P. 76)**
- 4** Interior **▶Paper Jams inside the Machine or in the Back Side(P. 76)**

5 Duplex transport guide ▶ **Paper Jams at the Duplex Transport Guide(P. 83)**

6 Back side ▶ **Paper Jams inside the Machine or in the Back Side(P. 76)**

NOTE

- Paper may not actually be jammed in the location you check. Even in this case, follow the instructions on the screen to check all the locations.
- The screen indicating that there is a paper jam is repeatedly displayed until you clear the paper jam.
- Do not remove paper from a location other than that displayed as a paper jam location on the screen. This may cause paper jams in other locations or missing pages in output documents.

Paper Jams inside the Machine or in the Back Side

E9SJ-01H

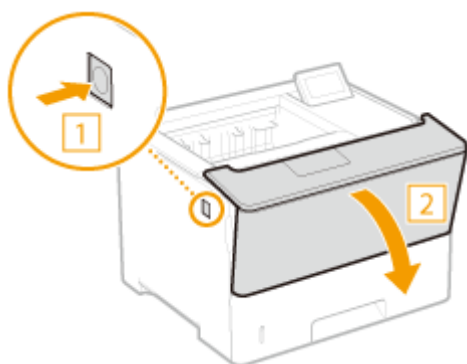
Check the paper jam location on the screen, and follow the procedure below to remove the paper.

NOTE

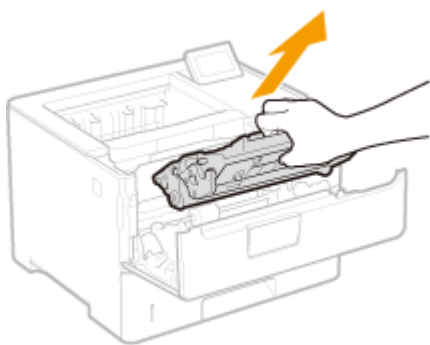
Confirm before handling

- Before starting the operation to clear paper jams, confirm that the covers and paper drawers of the machine and optional equipment are closed.

1 Press the button to open the Front cover.

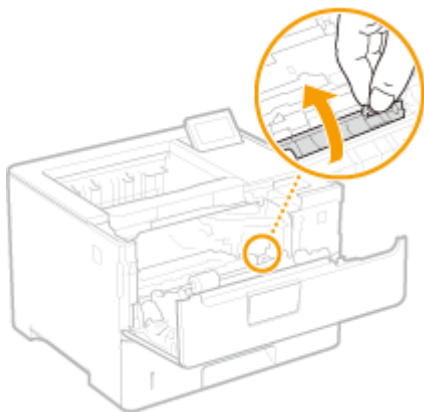


2 Remove the toner cartridge.

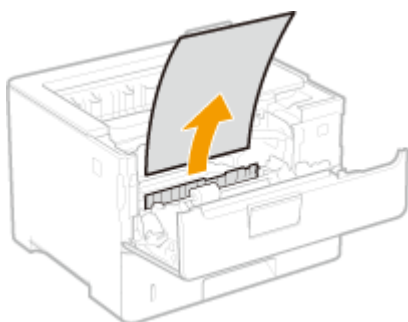


3 Hold the front side green knob and lift the transport guide.

- Keep holding the transport guide until returning it to the original position in step 5.



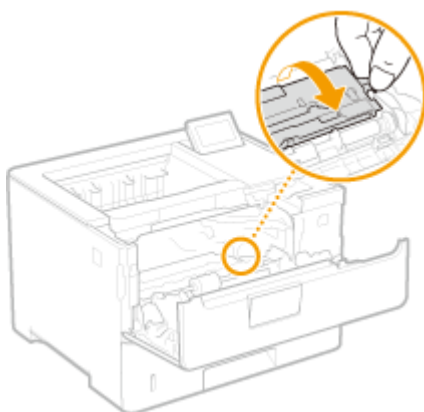
4 Gently pull out the paper.



5 Gently return the transport guide back in place.

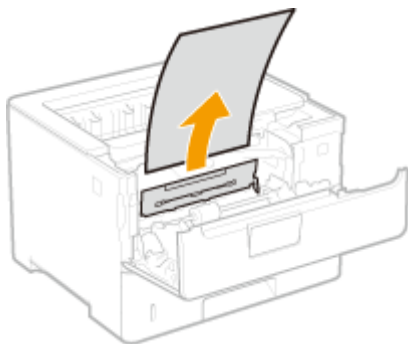
6 Hold the rear side green knob and lift the transport guide.

- Keep holding the transport guide until returning it to the original position in step 8.



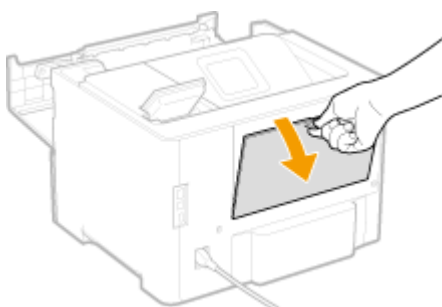
7 Gently pull out the paper.

- Pull out the paper flatly as much as possible to prevent unfixed toner from being dropped.



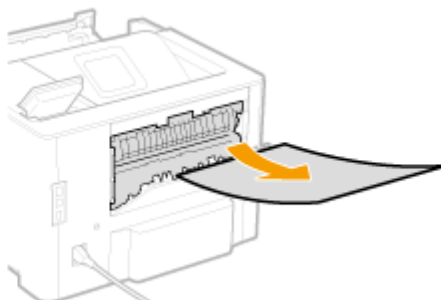
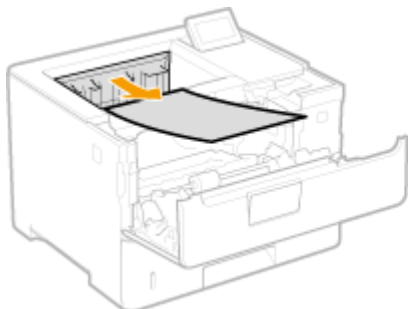
8 Gently return the transport guide back in place.

9 Open the rear cover.



10 Gently pull out the paper.

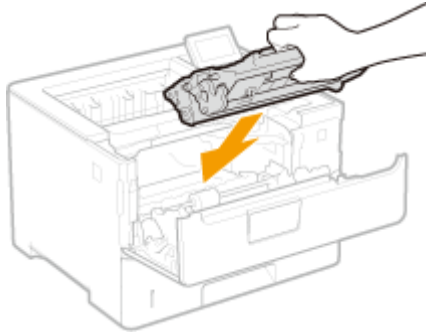
- Determine in which way you can pull out the jammed paper more easily, and try that way first.
- Pull out the paper flatly as much as possible to prevent unfixed toner from being dropped.



11 Close the rear cover.

12 Install the toner cartridge.

- Make sure to push in the cartridge until it stops.



13 Close the front cover.

NOTE:

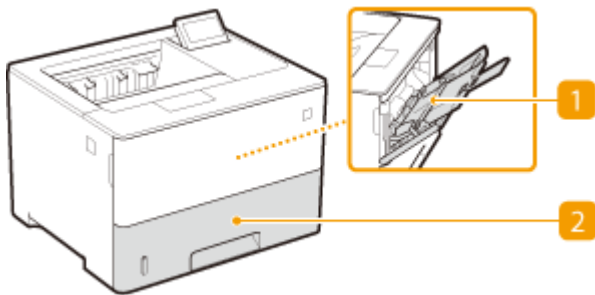
When the message is still displayed

- Paper may be jammed in other locations. Check other locations, and remove jammed paper if any. If the message is still displayed, check whether the front cover is securely closed.

Paper Jams in a Paper Source

E9SJ-01J

Check the paper jam location on the screen, and follow the procedure below to remove the paper.



1 Multi-purpose tray ➤ **Paper Jams in the Multi-Purpose Tray(P. 80)**

2 Paper drawer ➤ **Paper Jams in the Paper Drawer(P. 81)**

NOTE

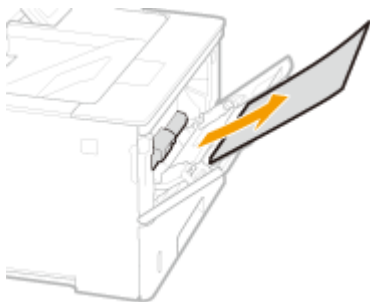
Confirm before handling

- Before starting the operation to clear paper jams, confirm that the covers and paper drawers of the machine and optional equipment are closed.

Paper Jams in the Multi-Purpose Tray

If there is paper loaded in the tray, remove it first. If the jammed paper cannot be removed easily, do not forcibly pull it out, but follow the procedure for a different paper jam location indicated by the message.

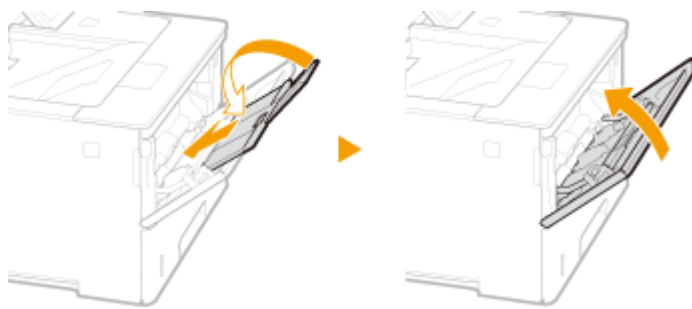
1 Gently pull out the paper.



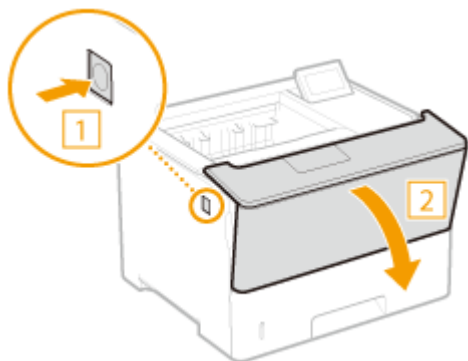
2 Open and close the front cover.

- When the front cover is opened and closed, the paper jam message disappears.

1 Close the tray.



- 2** Press the button to open the front cover.



- 3** Close the front cover.

NOTE:

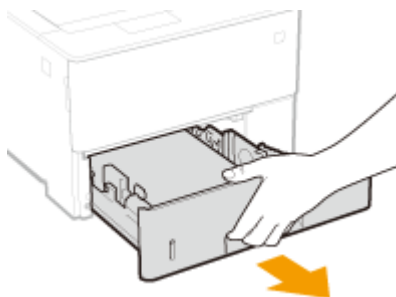
When the message is still displayed

- Paper may be jammed in other locations. Check other locations, and remove jammed paper if any. If the message is still displayed, check whether the front cover is securely closed.

Paper Jams in the Paper Drawer

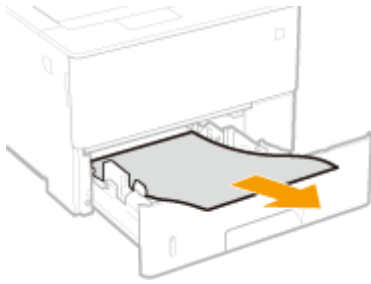
If the jammed paper cannot be removed easily, do not forcibly pull it out, but follow the procedure for a different paper jam location indicated by the message.

- 1** Pull out the paper drawer until it stops.



- 2** Gently pull out the paper.

- When the optional paper feeder is attached, gently pull out the paper in the same way.

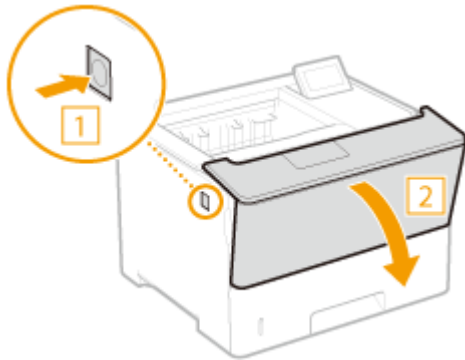


3 Set the paper drawer.

4 Open and close the front cover.

- When the front cover is opened and closed, the paper jam message disappears.

1 Press the button to open the front cover.



2 Close the front cover.

NOTE:

When the message is still displayed

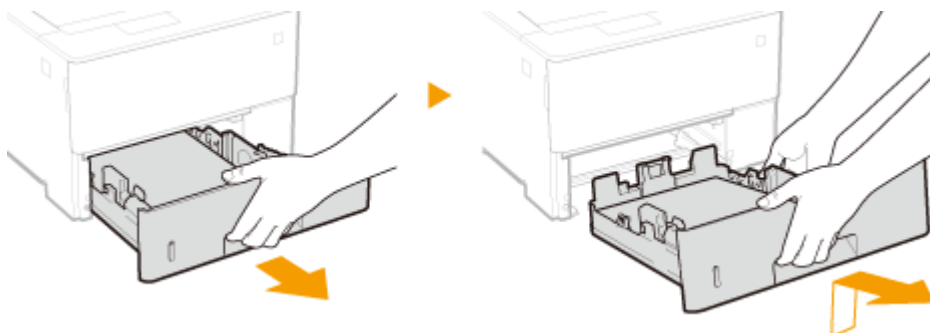
- Paper may be jammed in other locations. Check other locations, and remove jammed paper if any. If the message is still displayed, check whether the front cover is securely closed.

Paper Jams at the Duplex Transport Guide

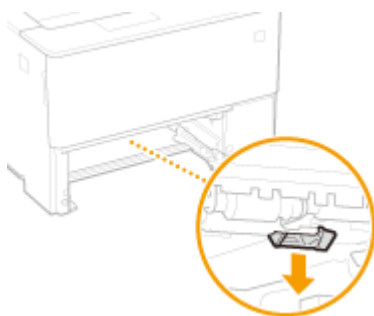
E9SJ-01K

If the jammed paper cannot be removed easily, do not forcibly pull it out, but follow the procedure for a different paper jam location indicated by the message.

- 1 Pull out the paper drawer until it stops, and remove it while lifting the front side.**



- 2 Press the green knob and lower the duplex transport guide.**

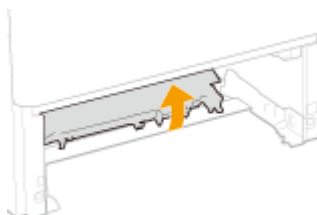


- 3 Gently pull out the paper.**



- 4 Return the duplex transport guide back to position.**

- Fully close the guide until it clicks.

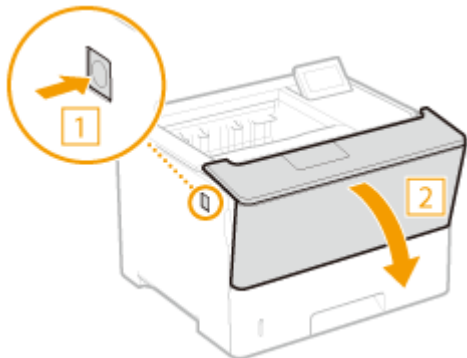


5 Set the paper drawer.

6 Open and close the front cover.

- When the front cover is opened and closed, the paper jam message disappears.

- 1 Press the button to open the front cover.



- 2 Close the front cover.

NOTE:

When the message is still displayed

- Paper may be jammed in other locations. Check other locations, and remove jammed paper if any. If the message is still displayed, check whether the front cover is securely closed.

Options

E9SJ-01L

The functionality of the machine can be expanded by installing options to the machine.

NOTE

- For information on system-related optional equipment, see [▶System Options\(P. 610\)](#) .

■ Available Options

▶Optional Equipment(P. 86)

■ Finding Options According to Your Purposes

To add paper drawers

▶Paper Feeder PF-C(P. 87)

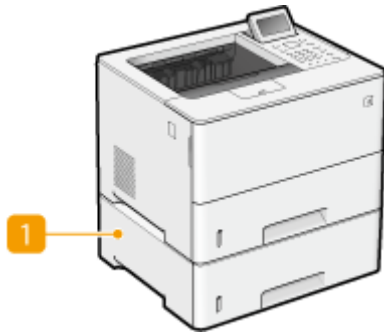
NOTE

- Some of the settings may not be displayed depending on the configuration of optional equipment installed on the machine.

Optional Equipment

E9SJ-01R

By combining options, you can use functions more efficiently.



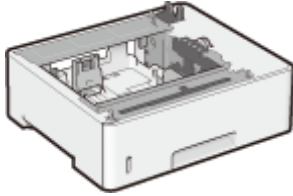
1 Paper Feeder PF-C

Load frequently used paper in the paper drawer of this product. ▶ **Paper Feeder PF-C(P. 87)**

Paper Feeder PF-C

E9SJ-01S

Enables you to add a paper drawer. Loading different sized paper in the optional paper drawer enables reduced work for switching paper.



NOTE

- Up to three units of the Paper Feeder PF-C can be attached.
- See the Setup Guide for the attaching procedure of the Paper Feeder PF-C.

Hardware Specifications

E9SJ-01U

This section presents the specifications of the main unit and optional equipment of this product. Note that the specifications are subject to change without notice for product improvement or future release.

NOTE

- To check the system specifications for this product, see [▶System Specifications\(P. 598\)](#) .

■ Machine Specifications

▶Main Unit(P. 89)

▶Available Paper(P. 91)

■ Specifications of Optional Equipment

▶Paper Feeder PF-C(P. 98)

Main Unit

E9SJ-01W

Name	Canon imageCLASS LBP335x
Type	Desktop
Resolution for Writing	600 dpi x 600 dpi
Number of Tones	256
Acceptable Paper Stock	Paper Sizes Paper Drawer • Max: 216.0 mm x 355.6 mm • Min: 105.0 mm x 148.0 mm Multi-Purpose Tray • Max: 216.0 mm x 355.6 mm • Min: 76.2 mm x 127.0 mm Paper Weight • Paper Drawer: 60 g/m² to 199 g/m² • Multi-Purpose Tray: 60 g/m² to 199 g/m²
Paper Type	▶Available Paper(P. 91)
Warm-Up Time ^{*1}	After Powering ON • When <Quick Startup Settings for Main Power> is set to <On>: 2 seconds or less^{*2} • When <Quick Startup Settings for Main Power> is set to <Off>: 22 seconds or less Returning from the Sleep mode 5 seconds or less
First Print Time	Paper Drawer • A4: Approx. 6.2 sec • LTR: Approx. 6.1 seconds Multi-Purpose Tray • A4/LTR: Approx. 6.2 sec
Print Speed ^{*3} (Plain A4/LTR, 100%)	• A4: 43.0 sheets/minute • LTR: 45.5 sheets/minute
Paper Feeding System/Capacity ^{*4}	Paper Drawer • Plain: 550 sheets (80 g/m²) • Plain: 640 sheets (64 g/m²) • Recycle: 550 sheets • Heavy: 440 sheets (90 g/m² to 120 g/m²) • Bond: 252 sheets

About the Machine

	Multi-Purpose Tray • Plain: 100 sheets (80 g/m² / 64 g/m²) • Recycle: 100 sheets • Heavy, Bond: 80 sheets (90 g/m² to 120 g/m²) • Heavy: 50 sheets (128 g/m² to 163 g/m²) • Labels: 40 sheets • Envelopes: 10 sheets • Postcards: 50 sheets • 3 x 5 inch: 35 sheets
Inner Tray Capacity ^{*4}	• 250 sheets (68 g/m²) • 150 sheets (64 g/m² to 80 g/m²)
Power Source	220 V - 240 V AC, 50/60 Hz, 3.3 A
Power Consumption	Maximum Power Consumption 1,400 W or less When the machine is in the Sleep mode 1.0 W or less When the main power switch is turned OFF 0.1 W or less
Dimensions (W x D x H)	409.0 mm x 376.0 mm x 275.0 mm
Weight (Toner cartridges included)	Main Unit Approximately 11.5 kg
Installation Space (W x D)	409 mm x 667 mm (When the paper drawer is pulled out and the rear cover is opened.) * Provide a space of 100 mm or more around the machine.
Memory Capacity	RAM: 2.0 GB eMMC: 15 GB
Environmental Conditions	Temperature: 10 °C to 30 °C Humidity: 20 % to 80 % RH (no condensation)

^{*1} May vary depending on the environment and conditions under which the machine is being used.

^{*2} Depending on the situations, the machine does not startup quickly.

^{*3} Print speed is measured based on internal testing using A4/LTR size paper printed with 100% print ratio to original on one-sided paper. Internal testing involved continuously printing the same one page of content on plain paper. Print speed may vary depending on paper type, paper size or paper feeding direction. The device may automatically pause or slow down in order to adjust printer condition such as controlling temperature of a certain unit or limiting impact to image quality during continuous printing.

^{*4} May vary depending on the installation environment and paper to use.

Available Paper

E9SJ-01X

The paper types that can be used with this machine are shown in the following table.
Also, confirm the precautions regarding paper use.

- ▶Supported Paper Sizes(P. 91)
- ▶Supported Paper Types(P. 95)
- ▶Unusable Paper(P. 96)
- ▶Precautions Regarding Paper(P. 97)
- ▶Storing Paper Printed With the Machine(P. 97)

Supported Paper Sizes

Paper Sizes	Paper Source (Standard)		Paper Source (Optional)
	Paper Drawer 1	Multi-Purpose Tray	Paper Feeder PF-C
A4	✓	✓	✓
A5	✓	✓	✓
A5R	✓	✓	✓
A6	✓	✓	✓
B5	✓	✓	✓
16K	✓	✓	✓
LTR	✓	✓	✓
LGL	✓	✓	✓
STMT	✓	✓	✓
EXEC	✓	✓	✓
FOOLSCAP/FOLIO	✓	✓	✓
OFICIO	✓	✓	✓
OFICIO (Mexico)	✓	✓	✓
LETTER (Government)	✓	✓	✓
OFICIO (Brazil)	✓	✓	✓

Paper Sizes	Paper Source (Standard)		Paper Source (Optional)
	Paper Drawer 1	Multi-Purpose Tray	Paper Feeder PF-C
LEGAL (India)	✓	✓	✓
LEGAL (Government)	✓	✓	✓
FOOLSCAP (Australia)	✓	✓	✓
F4A	✓	✓	✓
3x5 inch	-	✓	-
Free Size	✓*1	✓*2	✓*1
Custom Size	✓*1	✓*2	✓*1
Postcard	-	✓	-
Reply Postcard	-	✓	-
4 on 1 Postcard	-	✓	-
No.10 (COM10)	-	✓	-
ISO-C5	-	✓	-
DL	-	✓	-
Monarch	-	✓	-
Nagagata 3	-	✓	-
Nagagata 4	-	✓	-
Nagagata 40	-	✓	-
Yougatanaga 3	-	✓	-

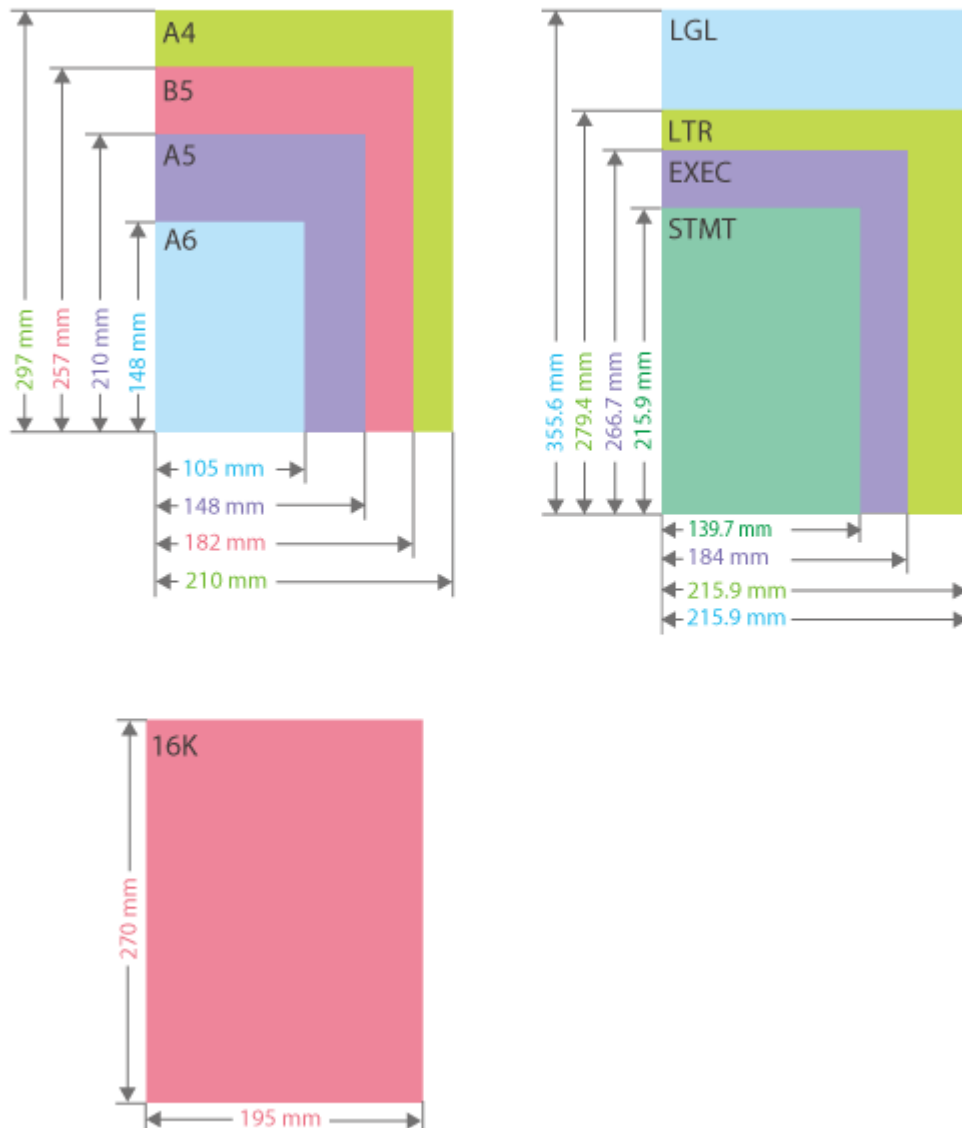
*1 You can use custom size settings ranging from 105.0 mm x 148.0 mm to 216.0 mm x 355.6 mm.

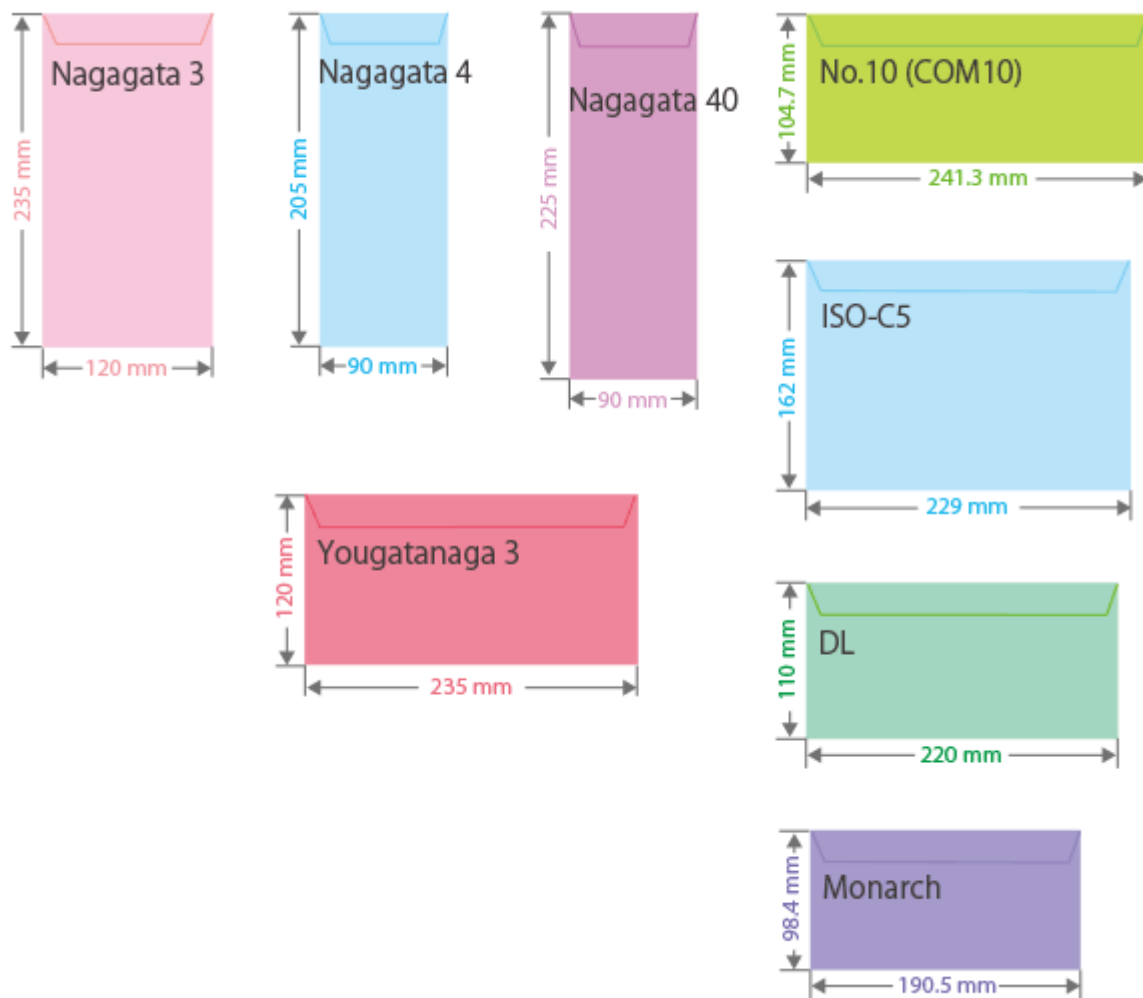
*2 You can use custom size settings ranging from 76.2 mm x 127.0 mm to 216.0 mm x 355.6 mm.

NOTE

Paper sizes supported by this machine

- The following table shows most of the sizes of paper and envelope that can be used with the machine.





- Other supported paper sizes are as follows.

FOOLSCAP/FOLIO (215.9 mm x 330.2 mm)

OFICIO (215.9 mm x 317.5 mm)

OFICIO (Mexico) (216.0 mm x 341.0 mm)

LETTER (Government) (203.2 mm x 266.7 mm)

OFICIO (Brazil) (216.0 mm x 355.0 mm)

LEGAL (India) (215.0 mm x 345.0 mm)

LEGAL (Government) (203.2 mm x 330.2 mm)

FOOLSCAP (Australia) (206.0 mm x 337.0 mm)

F4A (215.9 mm x 342.9 mm)

Postcard (100.0 x 148.0 mm)

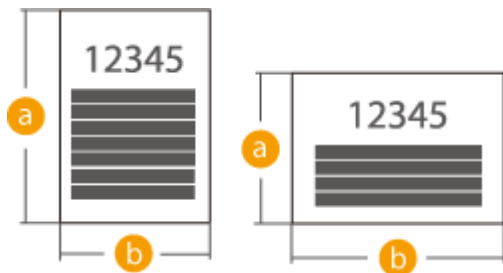
Reply Postcard (148.0 x 200.0 mm)

4 on 1 Postcard (200.0 x 296.0 mm)

3x5 inch (76.2 mm x 127.0 mm)

"Vertical" side and "Horizontal" side of paper

- In the User's Guide, regardless of the paper orientation, the side of paper perpendicular (a) to the front of the machine is referred to as the "vertical" side while the side parallel (b) to the front of the machine is referred to as the "horizontal" side.



Supported Paper Types

Chlorine-free paper can be used with this machine.

Paper Type	Paper Weight	Paper Source (Standard)		Paper Source (Optional)
		Paper Drawer 1	Multi-Purpose Tray	Paper Feeder PF-C
Thin	60 g/m ²	✓	✓	✓
Plain 1	61 to 74 g/m ²	✓	✓	✓
Plain 2	75 to 89 g/m ²	✓	✓	✓
Plain 3	90 to 105 g/m ²	✓	✓	✓
Heavy 1	106 to 120 g/m ²	✓	✓	✓
Heavy 2	121 to 149 g/m ²	-	✓	-
Heavy 3	150 to 199 g/m ²	-	✓	-
Color	61 to 74 g/m ²	✓	✓	✓
Recycled 1 ^{*1}	61 to 74 g/m ²	✓	✓	✓
Recycled 2 ^{*1}	75 to 89 g/m ²	✓	✓	✓
Letterhead 1	61 to 74 g/m ²	✓	✓	✓
Letterhead 2	75 to 89 g/m ²	✓	✓	✓
Letterhead 3	90 to 105 g/m ²	✓	✓	✓
Letterhead 4	106 to 120 g/m ²	✓	✓	✓
Letterhead 5	121 to 149 g/m ²	-	✓	-
Letterhead 6	150 to 199 g/m ²	-	✓	-

Paper Type	Paper Weight	Paper Source (Standard)		Paper Source (Optional)
		Paper Drawer 1	Multi-Purpose Tray	Paper Feeder PF-C
Labels	118 g/m ²	-	✓	-
Bond 1	60 to 74 g/m ²	✓	✓	✓
Bond 2	75 to 104 g/m ²	✓	✓	✓
Bond 3	105 to 120 g/m ²	✓	✓	✓
Envelope	80 to 105 g/m ²	-	✓	-
Postcard ^{*2}	190 g/m ²	-	✓	-

^{*1} You can use 100% recycled paper.

^{*2} The inkjet printable postcard or reply postcard can not be used.

■ Paper Available for Two-Sided Printing

- When performing 2-sided printing, use paper that meets the following requirements.

Paper size: A4, LGL, LTR, FOOLSCAP/FOLIO, OFICIO, OFICIO (Mexico), OFICIO (Brazil), LEGAL (India), F4A, Free Size (76.2 mm x 127.0 mm to 216.0 mm x 355.6 mm), Custom Size (210.0 mm x 279.4 mm to 216.0 mm x 355.6 mm)

Paper type: Thin, Plain 1, Plain 2, Plain 3, Heavy 1, Recycled 1, Recycled 2, Letterhead 1, Letterhead 2, Letterhead 3, Letterhead 4, Bond 1, Bond 2, Bond 3 and Color

Paper weight: 60 g/m² to 120 g/m²

If using other paper, use <2nd Side of 2-Sided Page> to print on the back side of printed paper.

Unusable Paper

Before printing, check whether the paper to use is suitable. Do not use the following types of paper, as they can cause paper jams or printing errors:

- Wrinkled, creased, curled, torn, or damp paper^{*1}
- Thin straw paper, very thin paper, coarse paper, glossy paper
- Paper with glue or other adhesive sticking out or label paper whose back side can be easily peeled off
- Paper printed by a thermal transfer printer, back side of paper printed by a thermal transfer printer
- The inkjet printable postcard cannot be used.

^{*1} Printing on damp paper may cause steam to be emitted from the output area or water droplets to adhere to the output part, but this does not indicate a malfunction. This is because the water contained in the paper evaporates due to the heat generated when the toner fixes to the paper. This is more likely to occur when the room temperature is low.

Precautions Regarding Paper

IMPORTANT

When using paper

- Only use paper that has fully acclimatized to the environment in which this machine is installed. Using paper that has been stored under different temperature or humidity may cause paper jams or result in poor print quality.

Paper handling and storage

- We recommend using the paper immediately after opening the package. Rewrap any remaining paper in its original package, and store it on a flat surface.
- Keep the paper wrapped in its original package to protect the paper from moisture or dryness.
- Do not store the paper in such a way that may cause it to curl or fold.
- Do not store the paper vertically or stack too much paper.
- Do not store the paper in direct sunlight, or in a place subject to high humidity, dryness, or drastic changes in temperature or humidity.

NOTE

When printing on paper that has absorbed moisture

- Steam may emit from the paper output area, or water droplets may form around the paper output area. There is nothing unusual about any of these occurrences, which occur when the heat generated from fixing toner on the paper causes moisture in the paper to evaporate (most likely to occur at low room temperatures).

Storing Paper Printed With the Machine

Be aware of the following precautions when handling and storing paper printed using the machine.

■ Storing Printed Paper

- Store the paper on a flat surface.
- Do not store paper together with items made from PVC (polyvinyl chloride), such as clear folders. The toner may melt, causing paper to become stuck to PVC-based material.
- Store paper so that it does not become folded or wrinkled. Doing so may cause the toner to come off.
- If you intend to store paper for long periods (two or more years), preserve them in a binder, etc.
- Long-term storage may cause paper to discolor, which in turn may cause print to appear discolored.
- Do not store paper in places with high temperatures.

■ Precautions when sticking printouts with adhesive

- Be sure to use insoluble adhesive.
- Test the adhesive on an unneeded printout before using.
- Before stacking printouts that stuck with adhesive, check that the adhesive completely dried.

Paper Feeder PF-C

E9SJ-01Y

Paper Size/Weight/Type	 Available Paper(P. 91)
Paper Drawers Capacity *	• Plain: 550 sheets (80 g/m²) • Plain: 640 sheets (64 g/m²) • Recycle: 550 sheets • Heavy: 440 sheets (90 g/m² to 120 g/m²) • Bond: 252 sheets
Dimensions	409 mm x 371 mm x 130 mm
Weight	Approximately 4.0 kg

* May vary depending on the installation environment and paper to use.

Setting Up

Setting Up	100
Preparations Required Before Use	101
Preventing Unauthorized Access	102
Setting up Using the Setup Guide	104
Setting the Date/Time	105
Setting up the Network Environment	106
Selecting the Network Connection Method	108
Connecting to a Wired LAN	110
Connecting to a Wireless LAN	112
Setting Up the Connection Using WPS Push Button Mode	114
Setting Up the Connection Using WPS PIN Code Mode	115
Setting Up Connection by Selecting a Wireless Router	116
Setting Up a Connection by Specifying Detailed Settings	117
Checking the SSID and Network Key	118
Setting an IP Address	119
Setting an IPv4 Address	120
Setting an IPv6 Address	122
Setting the IPv4 Address of the Sub Line	124
Adapting to the Network Environment	125
Making Ethernet Settings	126
Setting the Wait Time When Connecting to a Network	127
Making DNS Settings	128
Monitoring and Controlling the Machine with SNMP	132
Setting Static Routing	136
Other Network Settings	138
Configuring System Data Communication	140
Installing Drivers	142
Configuring E-Mail Print Settings	143

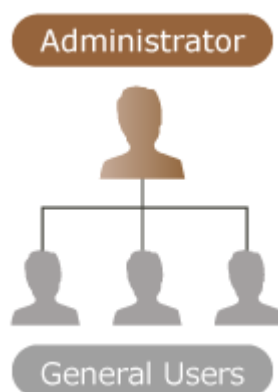
Setting Up

E9SJ-020

Setting up the usage environment is required before using each function of the machine. First, confirm the processes to complete "setting up" prior to actual setup. ➤ **Preparations Required Before Use(P. 101)**

■ Administrators and General Users

To manage the machine, it is recommended to construct a system in which someone is appointed as an administrator and general users operate the machine under the management of an administrator. Administrators decide the rules for using the machine and operate important setups such as networks and security. Administrators set the access for each user when necessary.



TIPS

Carrying out the initial setup of the machine (Setup Guide)

- You can easily set up to start using the machine, such as setting the date and time and networks, by following the on-screen instructions. ➤ **Setting up Using the Setup Guide(P. 104)**

Preparations Required Before Use

E9SJ-021

Set up the machine in order from steps 1 through 4. For details, click a link to display the corresponding pages. To use the machine safely, at the same time, confirm **Preventing Unauthorized Access(P. 102)** .

Step 1

Setting up Using the Setup Guide(P. 104)



Step 2

Setting up the Network Environment(P. 106)

- Set up the network environment not included on the Setup Guide. If you do not start the Setup Guide, start setting up from this procedure.



Step 3

Installing Drivers(P. 142)



Step 4

Configuring E-Mail Print Settings(P. 143)



TIPS

Setting from the Remote UI

- When you complete setup for the network environment, you can set up the machine from Remote UI efficiently. **Starting the Remote UI(P. 329)**

Saving setup time by importing data from other machines

- If you have any other Canon multifunction printer and save (export) its registered setup data to a computer beforehand, setup contents such as address book and paper type setting can be immediately used by importing them to the machine. **Importing/Exporting the Setting Data(P. 357)**

Preventing Unauthorized Access

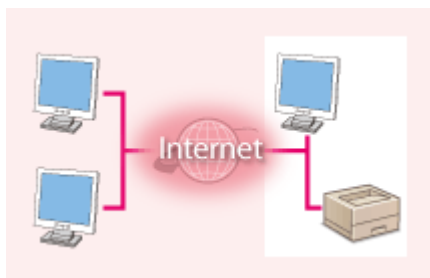
E9SJ-022

This section describes the security measures on how to prevent unauthorized access from the external network. This is a must-read for all users and administrators before using this machine, other printers, and multifunction machines connected to the network. In recent years, a printer/multifunction machine connected to the network can offer you a variety of useful functions, such as printing from a computer, operating from a computer using the remote function, and sending scan documents via the Internet. On the other hand, it is essential to take security measures to reduce the security risk for information leakage, as a printer/multifunction machine has become more exposed to threats, such as unauthorized access and theft, when it is connected to the network. This section explains necessary settings you need to specify to prevent unauthorized access before using a printer/multifunction machine connected to the network.

- ▶ **Assigning a Private IP Address(P. 102)**
- ▶ **Using Firewall to Restrict Transmission(P. 103)**
- ▶ **Specifying the TLS Encrypted Communication(P. 103)**
- ▶ **Setting PIN to Manage Information Stored in the Multifunction Machine(P. 103)**

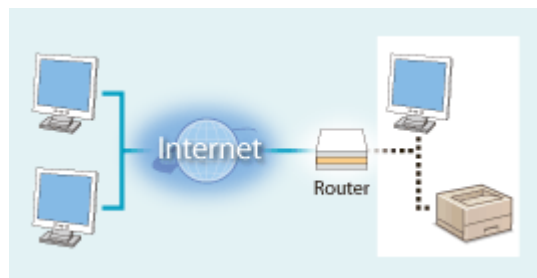
Assigning a Private IP Address

An IP address is a numerical label assigned to each device participating in a computer network. A "global IP address" is used for the communication connecting to the Internet, and a "private IP address" is used for the communication within a local area network, such as a LAN in the company. If a global IP address is assigned, your printer/multifunction machine is open to the public and can be accessed via the Internet. Thus, the risk of information leakage due to unauthorized access from external network increases. On the other hand, if a private IP address is assigned, your printer/multifunction machine is closed to a local area network and can be accessed by only users on your local area network, such as a LAN in the company.



Global IP address

Accessible from outside your network



Private IP address

Accessible only from within a local area network

Basically, assign a private IP address to your printer/multifunction machine. Make sure to confirm the IP address, assigned to the printer/multifunction machine you are using, is a private IP address or not. A private IP address is found in one of the following ranges.

■ Ranges of Private IP Addresses

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

For information on how to confirm IP addresses, see ▶ **Setting an IPv4 Address(P. 120)** .

NOTE

- If a global IP address is assigned to a printer/multifunction machine, you can create a network environment to reduce the risk of unauthorized access by installing security software, such as a firewall that prevents

access from the external networks. If you want to assign a global IP address to and use a printer/multifunction machine, contact your network administrator.

Using Firewall to Restrict Transmission

A firewall is a system that prevents unauthorized access from the external networks and protects against attacks/intrusions to a local area network. You can use a firewall on your network environment to block access from the external network that appears to be dangerous, by restricting communication from specified IP address of the external network. The function installed to a Canon printer/multifunction machine enables you to set up the IP address filter. For information on how to set up an IP address filter, see [▶Specifying IP Addresses in Firewall Settings\(P. 289\)](#) .

Specifying the TLS Encrypted Communication

For information on the TLS Encrypted Communication, see [▶Configuring the Network Security Settings\(P. 286\)](#) , and on the procedures to specify, see [▶Configuring the Key and Certificate for TLS\(P. 303\)](#) .

Setting PIN to Manage Information Stored in the Multifunction Machine

If a malicious third party attempts to gain unauthorized access to a printer/multifunction machine, setting PIN to information stored in the machine will reduce the risk of information leakage. Canon printers/multifunction machines enable you to protect various type of information by setting PIN.

Password for each function / PIN code setting

- Personal authentication management using User Authentication [▶Configuring the Personal Authentication Management Settings\(P. 243\)](#)
- PIN code setting for system management contents [▶Changing the System Manager ID and PIN\(P. 277\)](#)

These are examples of preventing unauthorized access. For other details, see [▶Managing the Machine\(P. 229\)](#) and carry out necessary settings according to your environment.

Setting up Using the Setup Guide

E9SJ-023

When the machine is turned ON for the first time ([▶Turning ON the Machine\(P. 29\)](#)), the initial setup of the machine begins automatically. You can adjust the basic setup necessary to use the machine. Configure the basic setup in accordance with each screen, or click a link to display the corresponding page and see details.

Step 1	Specify the display language. Select the display language. Select the display language, and select the country/region where the machine will be used if countries/regions are displayed.
Step 2	Set the time zone. Select the time zone where the machine is used.
Step 3	Specify the date and time. Specify the date and time of the machine.
Step 4	Set the "Administrator" password for Remote UI authentication. Set the password used when logging into the Remote UI as the "Administrator" user. - If you do not want to set a password, select <No> on the confirmation screen and proceed to step 5. - This machine is set to use the user authentication as the login service. For more information, see ▶Configuring the Personal Authentication Management Settings(P. 243) .
Step 5	Set the network connection method. Specify the method for connecting the machine to a network. - If you select <Wired LAN>, the Setup Guide finishes and the <Home> screen is displayed. - For details on wireless LAN connections, see ▶Connecting to a Wireless LAN(P. 112) .

■ Starting the Setup Guide later

IMPORTANT

The Setup Guide cannot be started in the following cases.

- If the user authentication or department ID authentication is set.
- If the authentication with a card is performed.



<Set> ▶ <Management Settings> ▶ <License/Other> ▶ <Start Setup Guide> ▶ <Yes>

NOTE

- If the Setup Guide was started after the "Administrator" password for Remote UI authentication was set, step 4 is not displayed and the Setup Guide proceeds to step 5.

Setting the Date/Time

E9SJ-024

Set the date and time for the machine. The date and time are used as the reference for the functions specifying the time, therefore, they need to be set accurately.

▶ **Setting the Time Zone(P. 105)**

▶ **Setting the Current Date and Time(P. 105)**

Setting the Time Zone



<Set> ▶ <Preferences> ▶ <Timer/Energy Settings> ▶ <Date/Time Settings> ▶ <Time Zone>

NOTE

What is UTC?

- Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time. Time differences exist depending on the country or area where the machine is used. The correct UTC time zone setting is required for Internet communications.

Setting the Current Date and Time



<Set> ▶ <Preferences> ▶ <Timer/Energy Settings> ▶ <Date/Time Settings> ▶ <Current Date/Time Settings>

NOTE

- You can change the display format for the time.
▶ **<Time Format>(P. 448)**
- You can also specify to automatically synchronize the date and time with a server on the network using SNTP. ▶ **Making SNTP Settings(P. 138)**
- If you are concerned about clock drift, periodically adjust the time of the machine.

Setting up the Network Environment

E9SJ-025

To connect the machine to a network, connect the machine to a router using a LAN cable or Wi-Fi and specify a unique IP address in the network. To specify an IP address, there are two methods: automatic setting and manual setting. Select one of the methods that is suitable for your communication environment and devices. The machine adopts not only basic network functions, but also advanced technologies in order to flexibly cope with various environments. Carry out the necessary setup required for your environment.

! IMPORTANT

For safe use

- If you connect the machine to a network without appropriate security measures, there are risks that the machine might receive unauthorized access from third parties. Set up network security to secure important data and information. ➤ **Configuring the Network Security Settings(P. 286)**

NOTE

- You can connect the machine to a computer using a USB cable (➤ **Parts and Their Functions(P. 18)**).
- You can establish a wireless direct connection between the machine and mobile devices. ➤ **Connecting Directly(P. 210)**

■ Confirm before handling

Follow the procedure below to make a connection to a network.

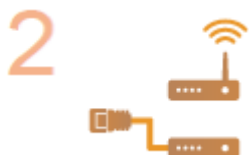


Confirm first.

- Are a computer and a router properly connected using a LAN cable? For details, see the instruction manual for each device or contact the manufacturers.
- Is setup of the computer network completed? If the setup is not completed, you cannot use the devices on a network even after completing the following steps.

NOTE

- Depending on your environment, you may need to change the settings of the network communication system (half-duplex/full-duplex) and Ethernet type (1000BASE-T/100BASE-TX/10BASE-T) (➤ **Making Ethernet Settings(P. 126)**). For details, contact the network administrator.
- To confirm the MAC address, see ➤ **<Network>(P. 452)** .
- To connect to a network employing IEEE802.1X, see ➤ **Configuring the IEEE 802.1X Authentication Settings(P. 317)** .



Select a wired LAN or wireless LAN for connection.

- **Selecting the Network Connection Method(P. 108)**

3

**Connect the machine to a router.**

- Is the LAN cable connector plugged into the proper place securely? Insert the connector until it clicks.
- For a wireless LAN connection, check the connection between the machine and the router.

▶ **Connecting to a Wired LAN(P. 110)**

▶ **Connecting to a Wireless LAN(P. 112)**

4

**Set an IP address as necessary.**

- Normally, an IP address is automatically allocated by DHCP, so this setting is not necessary. If you want to use a specific IP address or change the protocol of the automatic setting of an IP address from DHCP (initial setting) to another, this setting is necessary.

▶ **Setting an IP Address(P. 119)**

5

**Confirm that proper connection is completed.**

- Start the Remote UI from a computer (▶ **Starting the Remote UI(P. 329)**). If the Remote UI screen is displayed, the connection is completed.

NOTE

When <Sleep Mode Energy Use> is set to <Low>

- Depending on the utility software, communication may fail if the machine is in sleep mode. Press  (Energy Saver) to recover from the Sleep mode before configuring this setting.

LINKS

▶ **Adapting to the Network Environment(P. 125)**

Selecting the Network Connection Method

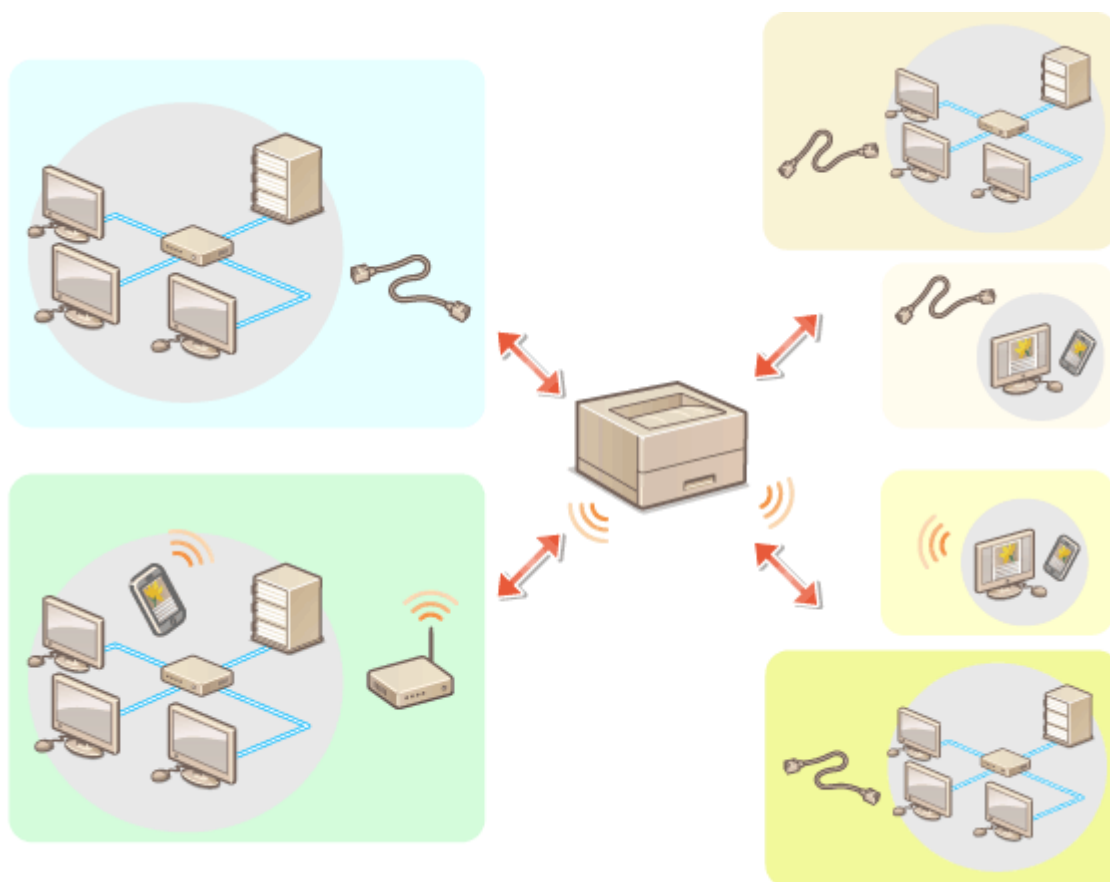
E9SJ-026

You can select the method for connecting the machine to computers, etc. The following connection methods are available.

- Wired LAN only
- Wireless LAN only
- Connecting to a wired LAN and wireless LAN at the same time^{*1}
- Connecting to a wired LAN and other wired LAN using a USB-LAN adapter at the same time^{*1}

^{*1}You must configure the settings separately for each network when connecting to multiple LANs at the same time. **▶ Building a Dual Network Environment(P. 570)**

On the machine and in the User's Guide (this manual), the primary line used in a dual network is called the "main line," and the secondary line is called the "sub line."



1 Select <Set> on the <Home> screen. **▶ <Home> Screen(P. 150)**

2 Select <Preferences> ▶ <Network> ▶ <Select Interface>.

3 Select the network connection method.

Connection method		<Main Line>	<Sub Line>
Wired LAN only	Wired LAN (main line) only	<Wired LAN>	<Off>
Wireless LAN only	Wireless LAN (main line) only	<Wireless LAN>	<Off>
Connecting to a wired LAN and wireless LAN at the same time ^{*1}	Wired LAN (main line) and wireless LAN (sub line)	<Wired LAN>	<Wireless LAN>
	Wired LAN (sub line) and wireless LAN (main line) ^{*2}	<Wireless LAN>	<Wired LAN>
Connecting to a wired LAN and other wired LAN at the same time	Wired LAN (main line) and wired LAN (sub line) ^{*3}	<Wired LAN>	<Wired LAN>

^{*1}If you change the settings from <Main Line> to <Sub Line> or from <Sub Line> to <Main Line>, the previous wireless LAN connection settings will be cleared, so you must reconnect to the wireless LAN.

^{*2}The wired LAN connected to the LAN port on the machine becomes the sub line. The wired LAN connected to the machine via a USB-LAN adapter cannot connect using the sub line.

^{*3}The wired LAN connected to the LAN port on the machine becomes the main line, and the wired LAN connected to the machine via a USB-LAN adapter becomes the sub line.

4 Press .

IMPORTANT

- When using a sub line, see  **Cautions When Using the Sub Line(P. 571)** .

When <Main Line> Is Set to <Wired LAN>, and <Sub Line> Is Set to a Setting Other Than [Off]

- Set <Sleep Mode Energy Use> to <High>.  **<Sleep Mode Energy Use>(P. 450)**

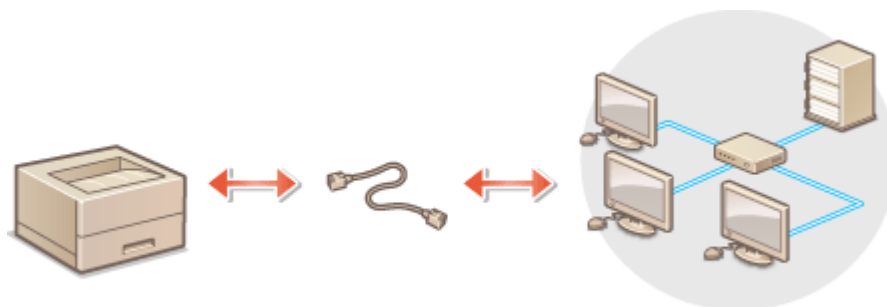
LINK

-  **Connecting to a Wired LAN(P. 110)**
-  **Connecting to a Wireless LAN(P. 112)**

Connecting to a Wired LAN

E9SJ-027

Connect the machine to a computer via a router using a LAN cable.



NOTE

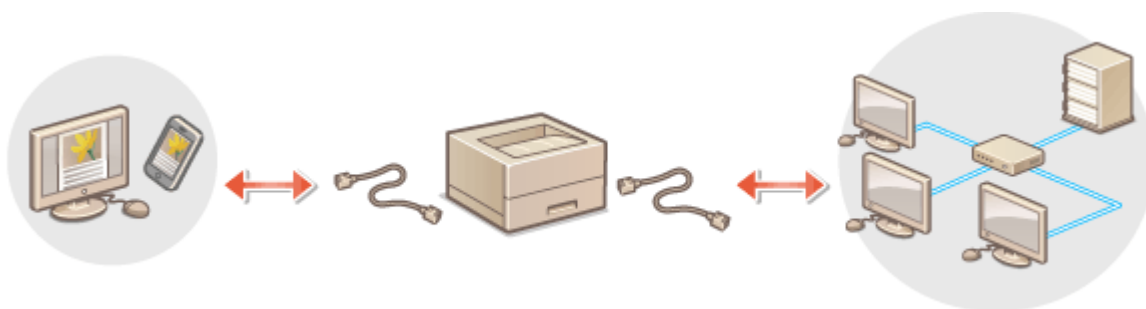
- A router and LAN cable are not included with the machine, so please prepare them separately.
- The machine supports 1000BASE-T/100BASE-TX/10BASE-T Ethernet.
- To make a connection using 100BASE-TX/10BASE-T, use a category 5 twisted pair cable. It is recommended to use an enhanced category 5 twisted pair cable to make a connection using 1000BASE-T.
- If devices supporting 1000BASE-T, 100BASE-TX and 10BASE-T are used together, a device (such as a switching hub) supporting all of the Ethernet types you use is necessary. For more information, contact your dealer or service representative.

1 Connect the machine to a router using a LAN cable.

- Push the connector in until it clicks into place.

■ Connecting to a Wired LAN for the Sub Line

If you set <Main Line> and <Sub Line> to <Wired LAN> in <Select Interface>, connect the wired LAN for the sub line.



- 1 Connect the USB-LAN adapter to the USB port of the machine (located towards the back on the right side of the machine). **Parts and Their Functions(P. 18)**

! IMPORTANT:

- Multiple USB-LAN adapters cannot be connected.

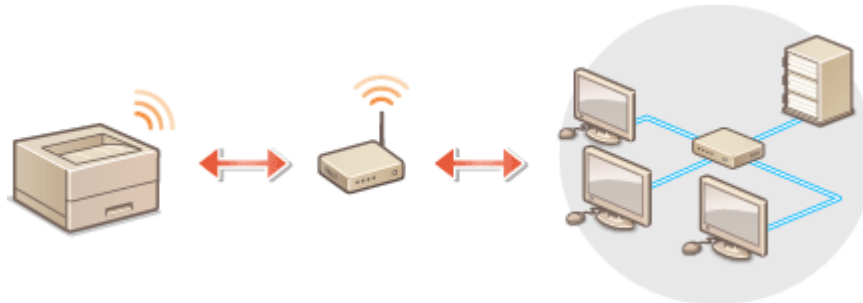
NOTE:

- For information on the USB-LAN adapters that can be used, contact your dealer or service representative.

Connecting to a Wireless LAN

E9SJ-028

Wirelessly connect the machine to a computer or mobile device via a wireless LAN router (access point). If the wireless router is equipped with Wi-Fi Protected Setup (WPS), configuring your network is automatic and easy. If the wireless router does not support with WPS, or if you want to specify authentication and encryption settings in detail, you need to manually set up the connection. Configure connection on the computer or mobile device side in advance.



■ Setting Up the Connection Using WPS

If your wireless LAN router supports WPS, two setting modes are available: push button mode and PIN code mode.

➤ **Setting Up the Connection Using WPS Push Button Mode(P. 114)**

➤ **Setting Up the Connection Using WPS PIN Code Mode(P. 115)**

■ Setting Up the Connection Manually

There are two manual setting methods: manually configure the setting with a wireless LAN router selected, or manually enter all the required information for wireless LAN connection. Regardless of the method, make sure that you have the required setup information, including the SSID and network key.

➤ **Setting Up Connection by Selecting a Wireless Router(P. 116)**

➤ **Setting Up a Connection by Specifying Detailed Settings(P. 117)**

➤ **Checking the SSID and Network Key(P. 118)**

■ Check the settings and information of the wireless LAN

Check the information you set.



<Set> ► <Preferences> ► <Network> ► <Wireless LAN Settings> ► <Connection Information>

! IMPORTANT

- Use wireless LAN connection at your own discretion and at your own risk. If the machine is connected to an unsecured network, your personal information might be leaked to a third party because radio waves used in wireless communication can go anywhere nearby, even beyond walls.
- The wireless LAN security that is supported by the machine is listed below. For the wireless security compatibility of your wireless router, see the instruction manuals for your networking devices or contact your manufacturer.
WPA-PSK (AES-CCMP)

WPA2-PSK (AES-CCMP)

WPA3-SAE (AES-CCMP)

WPA-EAP (AES-CCMP)

WPA2-EAP (AES-CCMP)

WPA3-EAP (AES-CCMP)

* You cannot use WPA-EAP and WPA2-EAP when connecting to a wired LAN and wireless LAN at the same time.

- Depending on the network device, the operation of the wireless LAN router differs. See the instruction manuals for your networking device for help.
- If the machine is configured to not use weak encryption, it cannot be connected to the wireless LAN routers without security settings. ➤ **Setting the Security Strength and Encryption Method(P. 305)**)

NOTE

- This machine does not come with a wireless router. Have the router ready.
- The wireless router must conform to IEEE 802.11b/g/n and be able to communication in 2.4 GHz bandwidth. For more information, see the instruction manuals for your networking devices or contact your manufacturer.

TIPS

Connecting directly

- You can establish a direct wireless connection between a mobile device and the machine without using a wireless LAN router. ➤ **Connecting Directly(P. 210)**



Reducing the power consumption

- If you set <Power Save Mode> to <On>, you can regularly set the machine to the power saving mode to match the signal that the wireless LAN router sends. <Wireless LAN Settings> ➤ ➤ **<Power Save Mode>(P. 460)**

Setting Up the Connection Using WPS Push Button Mode

E9SJ-029

If your wireless router supports the WPS (Wi-Fi Protected Setup) Push Button mode, you can easily set up a connection with the WPS button on the router.



<Set> ► <Preferences> ► <Network> ► <Wireless LAN Settings> ► <WPS Push Button Mode> ► select <Yes> on the confirmation screen ► press and hold the WPS button on the wireless router

➡ When the wireless LAN router is detected and the configuration is complete, the screen <Connected.> will be displayed.

NOTE

- Depending on the networking device, you may need to press and hold the WPS button for 2 seconds or longer. See the instruction manuals for your networking device for help.
- If the wireless LAN router is set up to use WEP authentication, you cannot connect with WPS. In this case, set the wireless LAN router to use a security standard that is supported by the machine.

Setting Up the Connection Using WPS PIN Code Mode

E9SJ-02A

Some WPS (Wi-Fi Protected Setup) routers do not support the Push Button mode. In this case, register the PIN code generated on the machine to the networking device.



Generating a PIN code on the machine



<Set> ► <Preferences> ► <Network> ► <Wireless LAN Settings> ► <WPS PIN Code Mode> ► select <Yes> on the confirmation screen

⇒ A PIN code is generated.



Registering the PIN code to the wireless router

Register the PIN code within two minutes after the PIN code is generated. For details, see the instruction manual for your networking device.

- 1 Access a wireless router from a computer.**
- 2 Display the screen for entering a WPS PIN code.**
- 3 Register the generated PIN code to the wireless router.**

⇒ When the wireless LAN router is detected and the configuration is complete, the screen <Connected.> will be displayed.

NOTE

- If the wireless LAN router is set up to use WEP authentication, you cannot connect with WPS. In this case, set the wireless LAN router to use a security standard that is supported by the machine.

Setting Up Connection by Selecting a Wireless Router

E9SJ-02C

You can search the wireless routers available for connection and select one from the display of the machine. If the security standard for your wireless LAN router is WPA/WPA2-PSK or WPA3-SAE, enter a PSK for the network key. Confirm and write down in advance information regarding your SSID, network key, security standard, or authentication/encryption method, etc. [▶Checking the SSID and Network Key\(P. 118\)](#)

NOTE

Security settings

- If the wireless connection is set up by selecting a wireless router, the encryption method for WPA/WPA2-PSK and WPA3-SAE is set to <Auto> (AES-CCMP). If you want to specify <AES-CCMP> as the encryption method for WPA/WPA2-PSK and WPA3-SAE, set up the connection in <Enter Manually>. [▶Setting Up a Connection by Specifying Detailed Settings\(P. 117\)](#)
- If the security standard for your wireless LAN router is WPA/WPA2-EAP/WPA3-EAP, the encryption method is set to AES-CCMP. Also, specify the IEEE 802.1X authentication settings for the machine before connecting to the wireless LAN. [▶Configuring the IEEE 802.1X Authentication Settings\(P. 317\)](#)

1 Select <Set> on the <Home> screen. [▶<Home> Screen\(P. 150\)](#)

2 Select <Preferences> ▶ <Network> ▶ <Wireless LAN Settings> ▶ <SSID Settings>.

3 Select <Select Access Point>.

- The machine starts searching for available wireless routers.

4 Select a wireless router, and connect to it.

■If the security setting of your wireless LAN router is WPA/WPA2-PSK or WPA3-SAE

- 1 Select the wireless LAN router to use.
- 2 Enter the network key.
- 3 Select <Yes> on the confirmation screen.

▶▶▶ When the configuration is complete, the screen <Connected.> will be displayed.

■If the security setting of your wireless LAN router is other than WPA/WPA2-PSK or WPA3-SAE

- 1 Select the wireless LAN router to use ▶ select <Yes> on the confirmation screen.

▶▶▶ When the configuration is complete, the screen <Connected.> will be displayed.

Setting Up a Connection by Specifying Detailed Settings

E9SJ-02E

If you want to specify the security settings in detail or cannot establish the wireless connection using the other procedures, manually enter all the required information for the wireless LAN connection. Confirm and write down in advance information regarding your SSID, network key, security standard, or authentication/encryption method, etc.

▶ Checking the SSID and Network Key(P. 118)

- 1** Select <Set> on the <Home> screen. ▶<Home> Screen(P. 150)
- 2** Select <Preferences> ▶ <Network> ▶ <Wireless LAN Settings> ▶ <SSID Settings>.
- 3** Select <Enter Manually> ▶ enter the SSID that you have checked.
 - Enter the SSID, and select <Apply>.
 - For instructions on how to enter text, see ▶<Entering Characters>(P. 157) .
- 4** Specify the security settings in <Security Settings>.

■ Using WPA-PSK, WPA2-PSK, or WPA3-SAE

- 1** Select <WPA/WPA2-PSK>, <WPA2-PSK/WPA3-SAE>, or <WPA3-SAE>.
- 2** Select an encryption method.
 - To set the machine to automatically select AES-CCMP to match the setting of the wireless router, press <Auto>.
 - If you selected <WPA3-SAE> in step 1, proceed to the next step.
- 3** Enter the network key that you have checked.
 - Enter the network key, and select <Apply>.

■ Using WPA-EAP, WPA2-EAP, or WPA3-EAP

- 1** Select <WPA/WPA2-EAP>.
- 2** Select <Yes> on the confirmation screen.

5 Select <Yes> on the confirmation screen.

- ➡ When the wireless LAN router is detected and the configuration is complete, the screen <Connected.> will be displayed.

Checking the SSID and Network Key

E9SJ-02F

When manually setting up a wireless LAN router connection, it is necessary to specify the SSID, network key, and security standard, etc., of the wireless LAN router. The SSID and network key may be indicated on these networking devices. Check your devices before setting up the connection. If the security standard for your wireless LAN router is WPA/WPA2-EAP/WPA3-EAP, specify the IEEE 802.1X authentication settings for the machine in advance ([▶Configuring the IEEE 802.1X Authentication Settings\(P. 317\)](#)). For more information, see the instruction manuals for your networking devices or contact your manufacturer.

SSID	A name given for identifying a specific wireless LAN. Some other terms used for SSID include "access point name" and "network name."
Network Key	A keyword or password used for encrypting data or authenticating a network. Some other terms used for network key include "encryption key," "WPA/WPA2 passphrase," "preshared key (PSK)."
Wireless Security Protocols (Authentication / Encryption)	• Security types (WPA-PSK/WPA2-PSK/WPA-EAP/WPA2-EAP/WPA3-SAE) • Authentication method (Open System/Shared Key/IEEE 802.1X authentication) • Encryption method (AES-CCMP)

IMPORTANT

- You cannot use WPA-EAP and WPA2-EAP when connecting to a wired LAN and wireless LAN at the same time.

Setting an IP Address

E9SJ-02H

To connect the machine to a network, a unique IP address on the network is required. The machine supports two versions of IP addresses: "IPv4" and "IPv6." Set and use them according to your environment. You can use either IPv4 or IPv6. You can also use both of them at the same time.

When a connection method with a main line and sub line is selected in <Select Interface>, specify the IP address of the sub line in <IP Address Settings> in <Sub Line Settings>.

- ▶ **Setting an IPv4 Address(P. 120)**
- ▶ **Setting an IPv6 Address(P. 122)**
- ▶ **Setting the IPv4 Address of the Sub Line(P. 124)**

Setting an IPv4 Address

E9SJ-02J

There are two methods to set an IPv4 address: allocating automatically using DHCP and entering manually. Select either of the two according to your environment. Conduct a connection test as necessary.

➤ **Setting an IPv4 Address(P. 120)**

➤ **Conducting a Connection Test for an IPv4 Address(P. 121)**

Setting an IPv4 Address

1 Select **<Set>** on the **<Home>** screen. ➤ **<Home> Screen(P. 150)**

2 Select **<Preferences>** ➤ **<Network>** ➤ **<TCP/IP Settings>** ➤ **<IPv4 Settings>**.

- If the screen for entering a Administrator PIN appears, enter the correct Administrator PIN. ➤ **<Set Administrator PIN>(P. 439)**

3 Select **<Use IPv4>** ➤ **<On>** to enable IPv4 settings.

4 Select **<IP Address Settings>** and set an IP address.

- You can also set both automatic retrieval and manual retrieval. If you set both and deselect [Release Address Last Acquired from DHCP Server When Address Cannot Be Acquired] in the Remote UI, the manually entered IP address is used when automatic IP address retrieval fails.

■ Automatically assigning an IP address

1 Select **<IP Address Settings>** ➤ **<Auto Acquire>**.

2 Select **<Select Protocol>** ➤ **<DHCP>**.

3 Check that **<Auto IP>** is set to **<On>**.

- If **<Off>** is selected, change the setting to **<On>**.

4 Select **<Apply>**.

NOTE:

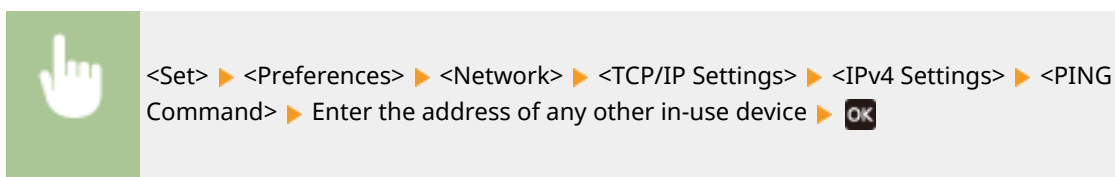
- If you press **<Auto IP>**, the available IP address is automatically searched in the network (LAN) and the value for each item is allocated. This function allocates the IP address without using a DHCP server. However, communication outside of the router range is not available.
- In an environment where both **<DHCP>** and **<Auto IP>** cannot be used, if either of the two is selected, useless communication occurs because the machine tries to check if the service is provided on the network.
- IP addresses assigned via DHCP override the address obtained via Auto IP.

■ Setting by manual entry

- 1 Configure a setting to disable auto-acquisition.
 - Select <Auto Acquire>, and set both <Select Protocol> and <Auto IP> to <Off>.
- 2 Select <Manually Acquire>.
- 3 Enter the IP address, the subnet mask, and the gateway address.
 - Enter these values in each screen using the numeric keys, and press .

Conducting a Connection Test for an IPv4 Address

When the machine is connected properly, the Remote UI login screen can be displayed from the computer (▶ **Starting the Remote UI(P. 329)**). You can conduct a connection test on the control panel of the machine.



⇒ When the machine is connected correctly, the <Received response from host.> message is displayed.

! IMPORTANT

- Even though IP addresses are properly set, if the machine is connected to a switching hub, the machine might not be connected to the network. In this case, delay the timing of the machine's communication start and try to connect again. ▶ **Setting the Wait Time When Connecting to a Network(P. 127)**

LINKS

▶ **Setting an IPv6 Address(P. 122)**

Setting an IPv6 Address

E9SJ-02K

The following are the types of IPv6 addresses. Register as necessary. Up to four stateless addresses can be registered. Conduct a connection test as necessary.

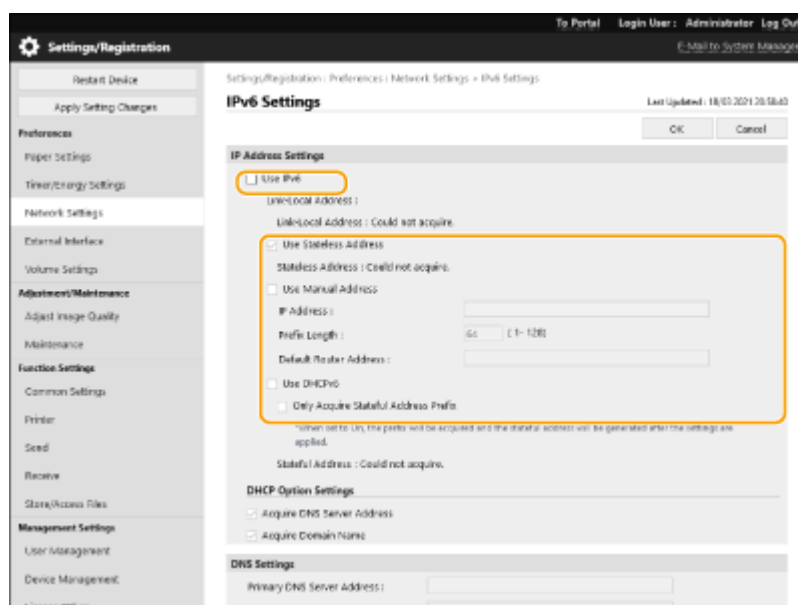
Type	Explanation
Link local address	Addresses that can be used only in the same link and that are automatically created without setting anything. Cannot be used out of the router range.
Stateless address	Addresses that are created automatically on the basis of the prefix notified by a router and the MAC address of the machine, even in an environment without a DHCP server.
Manual address	Addresses that are manually entered. Prefix length and a default router address are specified.
Stateful address	Addresses that are acquired from the DHCP server.

▶ **Setting an IPv6 Address(P. 122)**

▶ **Conducting a Connection Test for an IPv6 Address(P. 123)**

Setting an IPv6 Address

- 1 **Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 **Click [Settings/Registration] on the Portal page. ▶ Remote UI Screen(P. 331)**
- 3 **Click [Network Settings] ▶ [IPv6 Settings].**
- 4 **Select [Use IPv6] and configure the required settings.**



[Use IPv6]

Select the check box to enable IPv6 on the machine. When not using IPv6, deselect the check box.

[Use Stateless Address]

Select the check box when using a stateless address. When not using a stateless address, deselect the check box.

[Use Manual Address]

When you want to manually enter an IPv6 address, select the check box and enter the IP address, prefix length, and default router address in the corresponding text boxes.

The following addresses cannot be used.

- IPv4-compatible addresses (IPv6 addresses in which the upper 96 bits are "0" with an IPv4 address contained in the lower 32 bits)
- IPv4-mapped addresses (IPv6 addresses in which the upper 96 bits are "0:0:0:ffff:" with an IPv4 address contained in the lower 32 bits)

[IP Address]

Enter an IPv6 address. Addresses that start with "ff" (or multicast address) cannot be entered.

[Prefix Length]

Enter a number that indicates how many bits are available for the network address.

[Default Router Address]

Specify the IPv6 address of the default router as necessary. Addresses that start with "ff" (or multicast address) cannot be entered.

[Use DHCPv6]

Select the check box when using a stateful address. When not using DHCPv6, deselect the check box.

[Only Acquire Stateful Address Prefix]

Select this check box to only retrieve the first half of the stateful address from the DHCP server using DHCPv6.

5 Click [OK].

Conducting a Connection Test for an IPv6 Address

When the machine is connected properly, the Remote UI login screen can be displayed from a computer ([▶Starting the Remote UI\(P. 329\)](#)).

IMPORTANT

- Even though IP addresses are properly set, if the machine is connected to a switching hub, the machine might not be connected to the network. In this case, delay the timing of the machine's communication start and try to make a connection again. [▶Setting the Wait Time When Connecting to a Network\(P. 127\)](#)

LINKS

[▶Setting an IPv4 Address\(P. 120\)](#)

Setting the IPv4 Address of the Sub Line

E9SJ-02L

Specify the IPv4 address to use for the sub line.

NOTE

- Only IPv4 addresses can be used with the sub line.

1 Select <Set> on the <Home> screen.  <Home> Screen(P. 150)

2 Select <Preferences> ► <Network> ► <Sub Line Settings>.

3 Select <IP Address Settings> and set the IP address of the sub line.

- You can also set both automatic retrieval and manual retrieval. If you set both and deselect [Release Address Last Acquired from DHCP Server When Address Cannot Be Acquired] in the Remote UI, the manually entered IP address is used when automatic IP address retrieval fails.

■ Automatically Assigning the IP Address with DHCP

1 Select <IP Address Settings> ► <Auto Acquire>.

2 Select <DHCP>.

NOTE:

- If <DHCP> is selected, communication is performed to check whether network services are being provided, regardless of whether the environment can use DHCP. It is recommended that you deselect this item if you are not using DHCP.

■ Manually Entering the IP Address

1 Configure a setting to disable auto-acquisition.

- Select <Auto Acquire> ► <Off>.

2 Select <Manually Acquire>.

3 Enter the IP address and subnet mask.

- Enter these values in each screen using the numeric keys, and press .

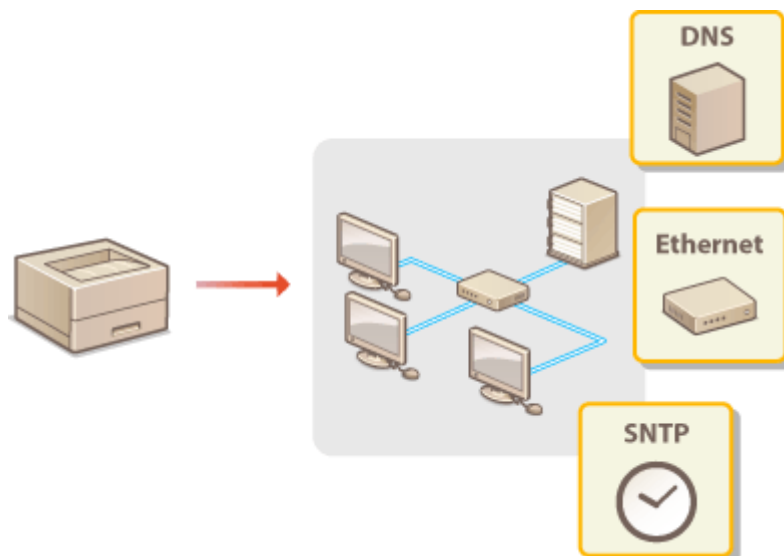
NOTE:

- When connecting to another network via a router, enter the gateway address and also configure <Static Routing Settings>.  **Setting Static Routing(P. 136)**

Adapting to the Network Environment

E9SJ-02R

The scale and form of a network varies depending on the purpose and use. The machine adopts various technologies for adapting to as many environments as possible. Consult your network administrator and carry out necessary settings according to your environment.



- ▶ Making Ethernet Settings(P. 126)
- ▶ Setting the Wait Time When Connecting to a Network(P. 127)
- ▶ Making DNS Settings(P. 128)
- ▶ Monitoring and Controlling the Machine with SNMP(P. 132)
- ▶ Setting Static Routing(P. 136)
- ▶ Other Network Settings(P. 138)
- ▶ Configuring System Data Communication(P. 140)

Making Ethernet Settings

Ethernet is a standard that stipulates communication methods within a LAN. Normally, the communication system (half-duplex/full-duplex) and Ethernet type (1000BASE-T/100BASE-TX/10BASE-T) can be set automatically. You can set them separately by switching the setting to manual operation.

<Ethernet Driver Settings> exists for both the main line and sub line. Register the settings as necessary.

1 Select <Set> on the <Home> screen. <Home> Screen(P. 150)

2 Select <Preferences> ▶ <Network> ▶ <Ethernet Driver Settings>.

- To specify the Ethernet settings for the sub line, select <Preferences> ▶ <Network> ▶ <Sub Line Settings> ▶ <Ethernet Driver Settings>.

3 Select whether to configure Ethernet settings automatically or manually.

- Normally, set <Auto Detect> to <On>. The communication system and Ethernet type are detected and automatically configured.

■ Configuring Ethernet settings automatically

- 1 Select <Auto Detect> ▶ <On>.

■ Making Ethernet settings manually

- 1 Configure a setting to disable Auto Detect.
 - Select <Auto Detect> ▶ <Off>.
- 2 Select <Communication Mode> ▶ select the communication mode.

<Half Duplex>

Alternately sends and receives communication data. Select when the machine is connected to a networking device using half duplex.

<Full Duplex>

Simultaneously sends and receives communication data. Use this setting for most environments.

- 3 Select <Ethernet Type> ▶ select the Ethernet type.
 - Select <10BASE-T>, <100BASE-TX>, or <1000BASE-T> in <Ethernet Type>.

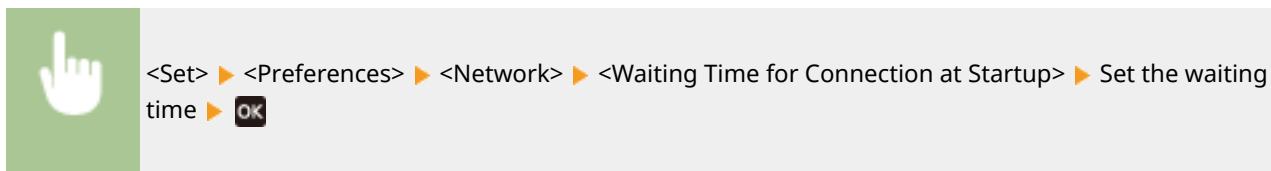
LINKS

Setting the Wait Time When Connecting to a Network(P. 127)

Setting the Wait Time When Connecting to a Network

E9SJ-02U

If you intend to implement network redundancy by connecting several switching hubs, a mechanism is necessary to avoid packet looping. In this case, it is effective to determine the roles of the switching ports, but communication may not be properly transmitted in cases just after changes such as adding a new device to the network. To connect the machine to such a network, set the waiting time which is the time until the communication starts.



LINKS

► Making Ethernet Settings(P. 126)

Making DNS Settings

E9SJ-02W

DNS (Domain Name System) provides a service for name resolution that associates a host (or domain) name with an IP address. Configure the DNS, mDNS, or DHCP option settings as necessary. Note that the procedures for configuring DNS are different for IPv4 and IPv6. Administrator privileges are required for this operation.



NOTE

- The DHCP optional setting only applies to the main line.

1 Start the Remote UI. ▶ [Starting the Remote UI\(P. 329\)](#)

2 Click [Settings/Registration] on the Portal page. ▶ [Remote UI Screen\(P. 331\)](#)

3 Click [Network Settings].

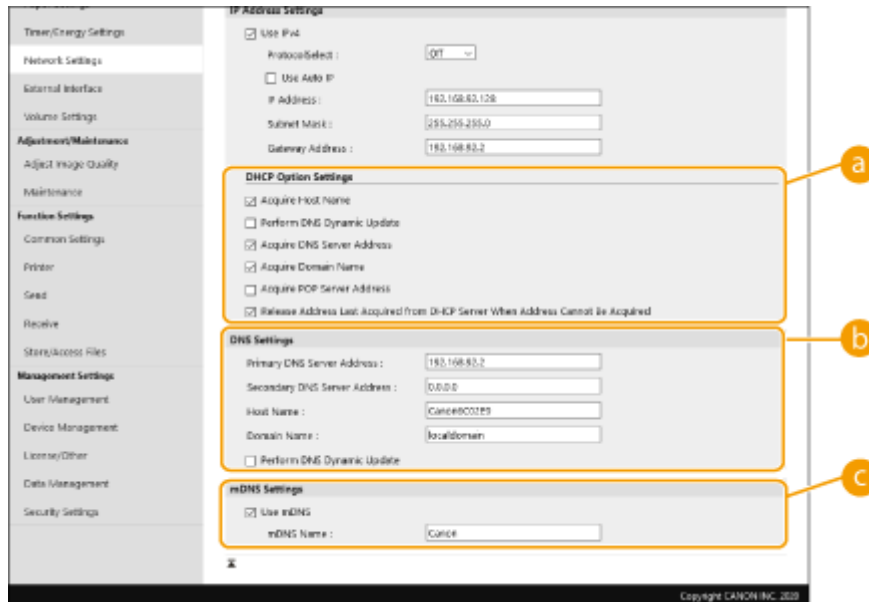
4 Configure DNS settings.

- For details about the setting information, contact your provider or network administrator. You can also refer to the computer settings. ▶ [Viewing the Network Connection Information of the Computer\(P. 527\)](#)

■ Configuring IPv4 DNS

1 Click [IPv4 Settings].

2 Configure IPv4 DNS settings.



a [DHCP Option Settings]

[Acquire Host Name]

Select the check box to enable Option 12 to obtain the host name from the DHCP server.

[Perform DNS Dynamic Update]

Select the check box to enable Option 81 to dynamically update the DNS records through the DHCP server.

[Acquire DNS Server Address]

Select the check box to enable Option 6 to obtain a DNS server address from the DHCP server.

[Acquire Domain Name]

Select the check box to enable Option 15 to obtain a domain name from the DHCP server.

[Acquire POP Server Address]

Select the check box to enable Option 70 to obtain a POP server address from the DHCP server.

[Release Address Last Acquired from DHCP Server When Address Cannot Be Acquired]

Deselect the check box to use the manually entered IP address when automatic IP address retrieval fails.

b [DNS Settings]

[Primary DNS Server Address]

Enter the IP address of a DNS server.

[Secondary DNS Server Address]

Enter the IP address of a secondary DNS server, if any.

[Host Name]

Enter alphanumeric characters for the host name of the machine that is to be registered to the DNS server.

[Domain Name]

Enter alphanumeric characters for the name of the domain the machine belongs to, such as "example.com."

[Perform DNS Dynamic Update]

Select the check box to dynamically update the DNS records whenever the machine's IP address is changed.

c [mDNS Settings]

[Use mDNS]

Adopted by Bonjour, mDNS (multicast DNS) is a protocol for associating a host name with an IP address without using DNS. Select the check box to enable mDNS and enter the mDNS name in the [mDNS Name] text box.

3 Click [OK].

■ Configuring IPv6 DNS

1 Click [IPv6 Settings].

2 Configure IPv6 DNS settings.

- The [Use IPv6] check box must be selected to configure the settings. ➤ **Setting an IPv6 Address(P. 122)**

a [DHCP Option Settings]

[Acquire DNS Server Address]

Select the check box to enable Option 23 to obtain a DNS server address from the DHCP server.

[Acquire Domain Name]

Select the check box to enable Option 24 to obtain a domain name from the DHCP server.

b [DNS Settings]

[Primary DNS Server Address]

Enter the IP address of a DNS server. Addresses that start with "ff" (or multicast address) cannot be entered.

[Secondary DNS Server Address]

Enter the IP address of a secondary DNS server, if any. Addresses that start with "ff" (or multicast address) cannot be entered.

[Use Same Host Name/Domain Name as IPv4]

Select the check box to use the same host and domain names as in IPv4.

[Host Name]

Enter alphanumeric characters for the host name of the machine that is to be registered to the DNS server.

[Domain Name]

Enter alphanumeric characters for the name of the domain the machine belongs to, such as "example.com."

[Perform DNS Dynamic Update]

Select the check box to dynamically update the DNS records whenever the machine's IP address is changed. To specify the type(s) of addresses you want to register to the DNS server, select the check box for [Register Manual Address], [Register Stateful Address], or [Register Stateless Address].

[mDNS Settings]

[Use mDNS]

Adopted by Bonjour, mDNS (multicast DNS) is a protocol for associating a host name with an IP address without using DNS. Select the check box to enable mDNS.

[Use Same mDNS Name as IPv4]

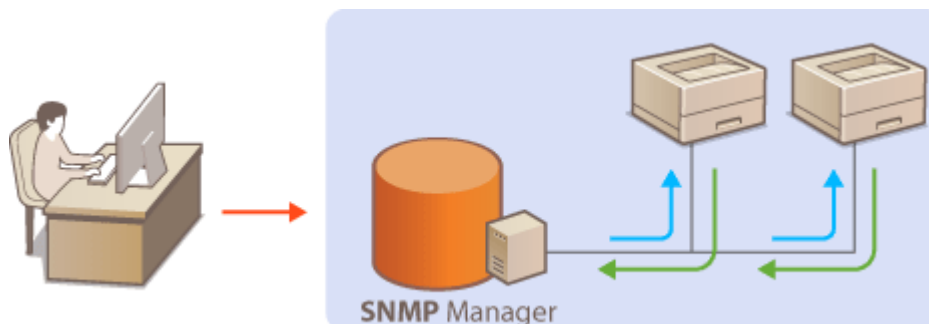
Select the check box to use the same mDNS name as in IPv4. To set a different name, deselect the check box and enter the mDNS name in the [mDNS Name] text box.

3 Click [OK].

Monitoring and Controlling the Machine with SNMP

E9SJ-02X

Simple Network Management Protocol (SNMP) is a protocol for monitoring and controlling communication devices in a network by using Management Information Base (MIB). The machine supports SNMPv1 and security-enhanced SNMPv3. You can check the status of the machine from a computer when you print documents or use the Remote UI. You can enable either SNMPv1 or SNMPv3, or both at the same time. Specify the settings for each version to suit your network environment and the purpose of use.



SNMPv1

SNMPv1 uses information called "community" to define the scope of SNMP communication. Because this information is exposed to the network in plain text, your network will be vulnerable to attacks. If you want to ensure network security, disable SNMPv1 and use SNMPv3.

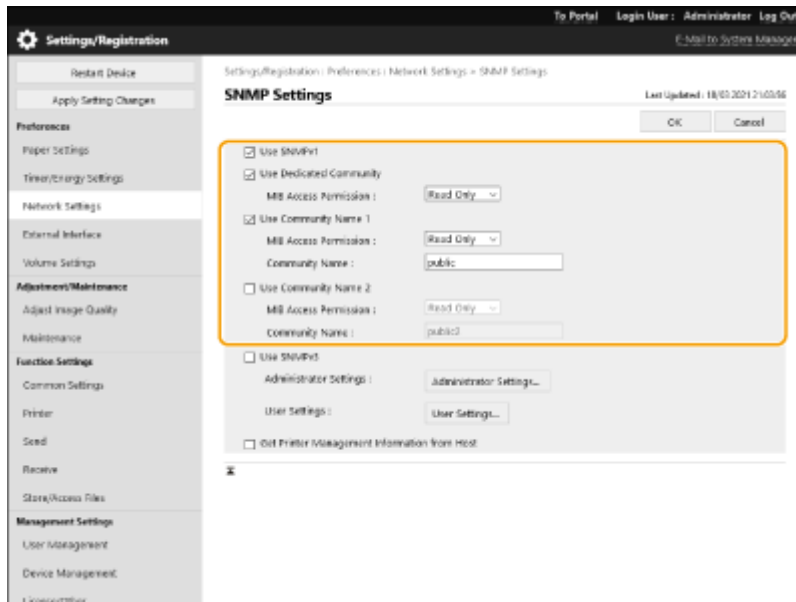
SNMPv3

With SNMPv3, you can implement network device management that is protected by robust security features. Note that TLS must be enabled for the Remote UI before configuring SNMPv3 ([▶Configuring the Key and Certificate for TLS\(P. 303\)](#)). Or, set <Remote UI Settings> to <Use TLS> in <On> ([▶<Remote UI Settings>\(P. 489\)](#)), then, turn the machine OFF and back ON.

NOTE

- SNMP management software, when installed on a computer on the network, enables you to configure, monitor, and control the machine remotely from the computer. For more information, see the instruction manuals for your management software.

- 1 Start the Remote UI.** [▶Starting the Remote UI\(P. 329\)](#)
- 2 Click [Settings/Registration] on the Portal page.** [▶Remote UI Screen\(P. 331\)](#)
- 3 Click [Network Settings] ▶ [SNMP Settings].**
- 4 Specify SNMPv1 settings.**
 - If you do not need to change SNMPv1 settings, proceed to the next step.



[Use SNMPv1]

Select the check box to enable SNMPv1. You can specify the rest of SNMPv1 settings only when this check box is selected.

[Use Dedicated Community]

A dedicated community is a community provided for Canon device management software. Select the check box to use a dedicated community, and specify [MIB Access Permission]. If you do not need to use a dedicated community, deselect the check box.

* For details, see the manual of the software you are using.

[Use Community Name 1]/[Use Community Name 2]

Select the check box to specify a community name. If you do not need to specify a community name, deselect the check box.

[MIB Access Permission]

For each community, select [Read/Write] or [Read Only] for the access privileges to MIB objects.

[Read/Write]	Permits both viewing and changing the values of MIB objects.
[Read Only]	Permits only viewing the values of MIB objects.

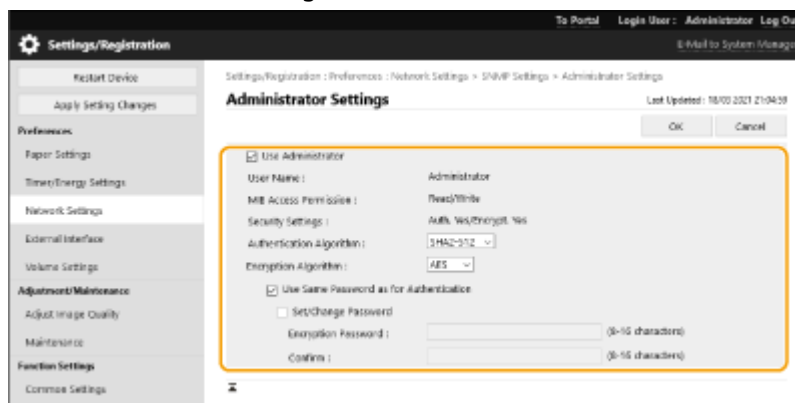
[Community Name]

Enter alphanumeric characters for the name of the community.

5 Select [Use SNMPv3] and configure SNMPv3.

- If you do not need to change SNMPv3 settings, proceed to the next step.

1 Click [Administrator Settings].



[Use Administrator]

Select the check box to use the Administrator user.

- [Authentication Algorithm] and [Encryption Algorithm] cannot be changed.

[Use Same Password as for Authentication]

Select the check box to use the same password as the password used in user authentication.

2 Click [OK].

3 Click [User Settings] ► [Register].

[User Name]

Enter alphanumeric characters for the user name.

[MIB Access Permission]

Select [Read/Write] or [Read Only] for the access privileges to MIB objects.

[Read/Write]	Permits both viewing and changing the values of MIB objects.
[Read Only]	Permits only viewing the values of MIB objects.

[Security Settings]

Select [Auth. Yes/Encrypt. Yes], [Auth. Yes/Encrypt. No], or [Auth. No/Encrypt. No] for the desired combination of authentication and encryption settings.

[Authentication Algorithm]

Select [MD5], [SHA1] or [SHA2] according to your environment. For [SHA2], select from four hash lengths (224 bit, 256 bit, 384 bit, or 512 bit).

[Encryption Algorithm]

If you have selected [Auth. Yes/Encrypt. Yes] in [Security Settings], select the appropriate encryption algorithm for your network environment.

[Authentication Password]/[Encryption Password]

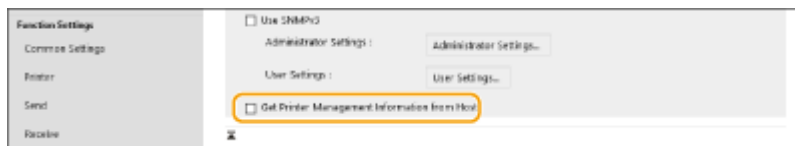
Use alphanumeric characters to enter the password in [Authentication Password] or both [Encryption Password] and [Confirm], depending on the settings in [Security Settings]. Set this for each algorithm (authentication/encryption).

4 Click [OK].

5 Click [Network Settings] ► [SNMP Settings].

6 Specify Printer Management Information Acquisition Settings.

- With SNMP, the printer management information, such as printing protocols and printer ports, can be monitored and obtained regularly from a computer on the network.



[Get Printer Management Information from Host]

Select the check box to enable monitoring of the printer management information of the machine via SNMP. To disable monitoring of the printer management information, deselect the check box.

7 Click [OK].

NOTE

Disabling SNMPv1

- If SNMPv1 is disabled, some of the functions of the machine become unavailable, such as obtaining machine information via the printer driver.

Using the control panel

- You can enable or disable the SNMP settings from <Set>. ▶<SNMP Settings>(P. 457)

Enabling Both SNMPv1 and SNMPv3

- If both versions of SNMP are enabled, it is recommended that MIB access permission in SNMPv1 be set to [Read Only]. MIB access permission can be set independently in SNMPv1 and SNMPv3 (and for each user in SNMPv3). Selecting [Read/Write] (full access permission) in SNMPv1 negates the robust security features that characterize SNMPv3 because most of the machine settings can then be controlled with SNMPv1.

LINKS

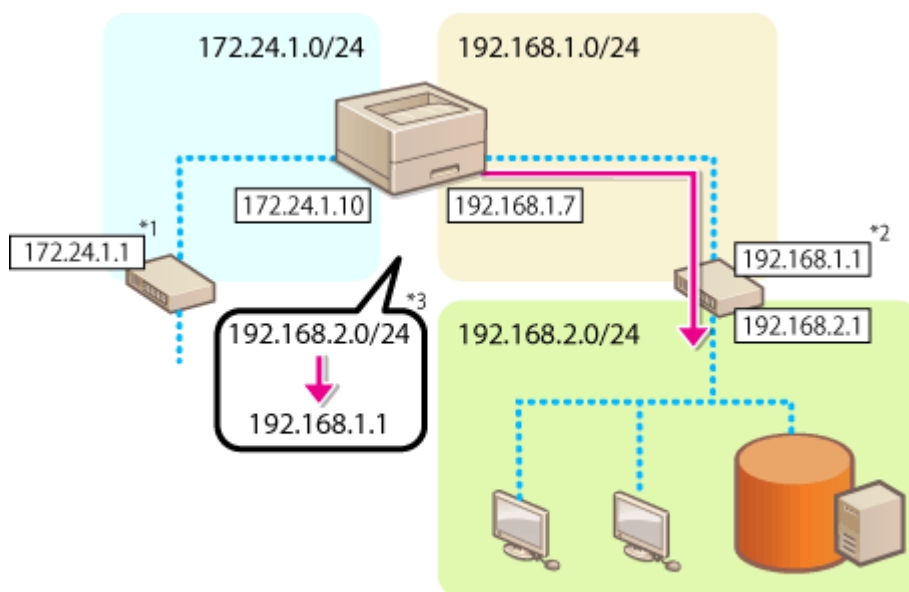
- ▶Configuring the Key and Certificate for TLS(P. 303)

Setting Static Routing

E9SJ-02Y

You can set static routing to manually specify the network route.

For example, when sending data from a machine connected to other networks via a router with both the main line and sub line, the data can be sent via the gateway of the sub line instead of the gateway of the main line that is normally used.



*1 Main line gateway

*2 Sub line gateway

*3 Static routing settings

NOTE

- When connecting to another network via a router, enter the gateway address in [IPv4 Settings]/[Sub Line Settings: Basic Settings] in advance. [▶Setting an IPv4 Address\(P. 120\)](#) [▶Setting the IPv4 Address of the Sub Line\(P. 124\)](#)

- 1** Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)
- 2** Click [Settings/Registration] on the Portal page. [▶Remote UI Screen\(P. 331\)](#)
- 3** Click [Network Settings] ▶ [Static Routing Settings].
- 4** Select [Use Static Routing].
- 5** Click [Register] in the line of the static routing information to register.

- [Edit] or [Delete] is displayed for lines that already have information registered.

6 Enter [Destination Address] and [Gateway Address] ► click [OK] ► [OK].

- Press each button and enter the required setting.

NOTE

- The route order is displayed in [Priority] on the static routing settings screen.
- You can register up to 16 devices that can be connected.
- The success/failure of the static routing settings is displayed in [Routing Registration].
- When failure is indicated in [Routing Registration], select the static routing settings that failed and set the address and gateway address again.

Other Network Settings

E9SJ-030

Set the following according to your network environment.

- ▶ **Making SNTP Settings(P. 138)**
- ▶ **Monitoring the Machine From Device Management Systems(P. 139)**

Making SNTP Settings

Simple Network Time Protocol (SNTP) enables you to adjust the system clock by using the time server on the network. If SNTP is used, the time server is checked at the specified intervals; therefore, the correct time can always be maintained. SNTP settings can be specified via the Remote UI.

NOTE

- To perform time synchronization via SNTP with the NTP server, setting the time zone where the machine is used is required in advance. ▶ **Setting the Date/Time(P. 105)**
- If SNTP is not set, the machine may access an external SNTP server to synchronize the clock when certain services are used.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the Portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [Network Settings] ▶ [SNTP Settings].**
- 4 Select [Use SNTP] and specify the required settings.**



[Use SNTP]

Select the check box to use SNTP for synchronization. If you do not want to use SNTP, deselect the check box.

[Polling Interval]

Specify the interval between one synchronization and the next.

[NTP Server Address]

Enter the IP address of the NTP or the SNTP server. If DNS is available on the network, you can enter a host name (or FQDN) consisting of alphanumeric characters instead (example: ntp.example.com).

[Check NTP Server Connection]

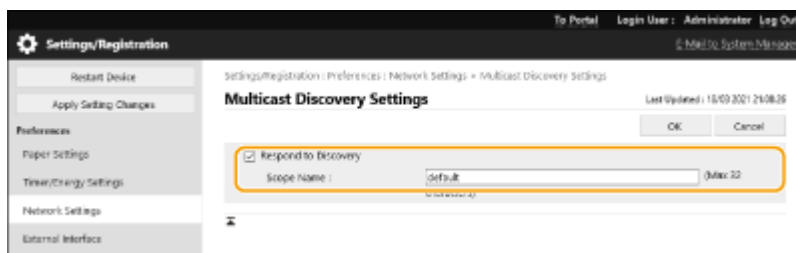
You can check the communication status between the machine and a registered server by using SNTP. However, only the communication status is confirmed and time adjustment is not carried out.

5 Click [OK].

Monitoring the Machine From Device Management Systems

When device management software is employed, you can collect/manage various information such as setting information and device failure information on the network through a server.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the Portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [Network Settings] ▶ [Multicast Discovery Settings].
- 4 Select [Respond to Discovery] and specify the required settings.



[Respond to Discovery]

Select the check box to set the machine to respond to device management software multicast discovery packets and enable monitoring by device management software.

[Scope Name]

To include the machine into a specific scope, enter alphanumeric characters for the scope name.

5 Click [OK].

LINKS

▶<Network>(P. 452)

Configuring System Data Communication

E9SJ-031

The settings described in this section are required to use the sub line for performing DNS name resolution and data communication via a proxy. Administrator privileges are required to specify these settings.

NOTE

- The DNS server address setting and proxy settings for the sub line can only be used for specific system data communication, such as using the sub line to access a firmware distribution server. They cannot be used for a regular internet connection. When using a DNS server or proxy server for the sub line for applications other than system data communication, register the addresses and port numbers to use with the sub line in the settings of the main line.
- You can also perform certain types of system data communication with the main line.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the Portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Network Settings] ▶ [Settings for System Data Communication].**
- 4 Specify the required settings.**

■Setting the DNS of the sub line

- 1** Enter the IP address of the DNS server in [IPv4 DNS Settings], according to your environment.

■Setting the proxy of the sub line

- 1** Select [Use Proxy].
- 2** Enter the address and port number of the proxy server, according to your environment.
- 3** To use proxy authentication, select [Use Proxy Authentication] and enter the user name and password.

■Selecting the line to use

- 1** Select [Main Line] or [Sub Line] for [Select Line to Use].

NOTE:

- If you select <Main Line> for <Select Line to Use>, the settings for <Main Line> are reflected in <DNS Server Address Settings> and <Proxy Settings>.
 - ▶Making DNS Settings(P. 128)
 - ▶Setting a Proxy(P. 301)

5 Click [OK].

Installing Drivers

E9SJ-032

Install the various drivers and associated software on your computer.

1 Make preparations before installation.

- Equip the main unit with optional equipment ( **Optional Equipment(P. 86)**).
- Install the drivers and software to use from the included CD/DVD-ROM or by downloading them from the Canon website for your country/region accessed via the URL indicated below.
(<https://global.canon/en/support/>)

NOTE

- The latest versions of drivers and software are uploaded to the Canon website when they become available. Download them as needed after checking the operating environment for your machine.
- Some functions of drivers and software may not be available depending on the model of the machine or operating environment.
- Some drivers may not be fully compatible with the operating system you are using. Check the driver compatibility with latest versions of operating systems on the Canon website.

2 Carry out installation of the drivers.

- For details on the installation, see the manuals for the drivers and software you want to use.

IMPORTANT

- If communication via the relevant IP address is not permitted in [Firewall Settings], you cannot install the driver. For more information, see  **Specifying IP Addresses in Firewall Settings(P. 289)** .
- After you have installed the driver, if communication via the IP address of the computer you have installed it on is not permitted in [Firewall Settings], you cannot print from that computer.

Configuring E-Mail Print Settings

E9SJ-033

This section describes how to specify the settings for receiving and printing e-mails on this machine. Use a computer to specify the settings for receiving e-mails and the control panel of the machine to specify the settings for printing e-mails. Administrator privileges are required in order to configure these settings.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the Portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [Send] ▶ [Network Settings - E-Mail Settings].
- 4 Specify the settings for E-Mail Print.

■When performing E-Mail Print by using SMTP protocol

If e-mails are sent to the machine via SMTP, the machine prints the e-mails immediately after receiving them. Enable this function when you want to forward fax documents from Canon multifunction printers to this machine and print them on the machine.



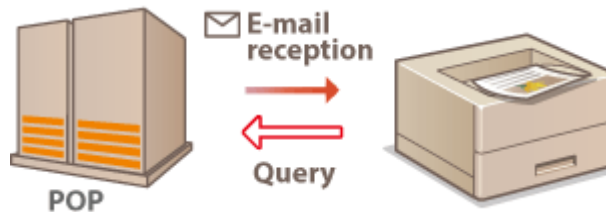
The screenshot shows the 'Network Settings - E-Mail Settings' page. On the left is a sidebar with various settings categories. The main area is titled 'Network Settings - E-Mail Settings' and contains the 'SMTP/POP Settings' section. In this section, the 'SMTP RX' checkbox is checked and highlighted with a yellow box. Below it are fields for 'POP Server', 'POP Login Name', 'POP Password', 'Confirm', and 'POP Interval'. There is also a 'Specify Port Number for POP RX' section with a dropdown menu showing '110'. At the bottom, there are 'Authentication/Encryption Settings' including 'Allow TLS (POP)', 'POP Authentication Method', 'Confirm TLS Certificate for POP RX', 'Add CN to Verification Items', and 'Allow TLS (SMTP RX)'.

[SMTP RX]

Select the check box to enable E-Mail Print by using the SMTP protocol.

■ When performing E-Mail Print from POP mail server

When the e-mail receiving starts, all e-mails stored in the mailbox of the mail server are printed. If you send e-mails that you want to print to the machine in advance, you can automatically print the e-mails at regular time intervals or print all stored e-mails in an arbitrary timing.



! IMPORTANT:

- We recommend using the mail address exclusively for E-Mail Print because all e-mails received into the machine are deleted from the mail server.

Conditions of use for POP protocol

- The POP mail server must support the UIDL command. For details, contact your network administrator or server administrator.

[POP RX]

Select the check box to enable E-Mail Print from the POP mail server. You can also specify this setting by using <Use POP RX> in the setting menu of the control panel.

[POP Server]

Enter the mail server name or IP address for receiving e-mails.

[POP Login Name]

Enter up to 32 alphanumeric characters for the user name used to connect to the mail server.

[POP Password]/[Confirm]

When setting a password for connecting to the mail server, enter the same password in [POP Password] and [Confirm] using up to 32 alphanumeric characters.

[POP Interval]

Specify the interval for automatically connecting to the mail server in minutes. New e-mails in the mailbox of the mail server are automatically received and printed at the specified time intervals. You can also specify this setting by using <POP Interval> in the setting menu of the control panel.

NOTE:

Preventing E-mails from Being Automatically Received

- Set [POP Interval] to [0]. If you set [0], you must manually receive e-mails.

[POP RX]

Specify the port number of the mail server that receives e-mails.

■ Setting authentication and encryption

The screenshot shows the 'Network Settings - E-Mail Settings' page. The left sidebar contains a navigation menu with categories like 'Preference', 'Adjustment/Maintenance', 'Function Settings', and 'Management Settings'. The main content area is titled 'Network Settings - E-Mail Settings' and includes a 'Last Updated' timestamp. The 'SMTP/POP Settings' section contains fields for POP Server, POP Login Name, POP Password, Confirm, and POP Interval. Below this is the 'Specify Port Number for POP RX' section with a dropdown for POP RX. The 'Authentication/Encryption Settings' section, highlighted with an orange box, includes checkboxes for 'Allow TLS (POP)', 'Confirm TLS Certificate for POP RX', and 'Add CN to Verification Items', along with a dropdown for 'Allow TLS (SMTP RX)'.

[Allow TLS (POP)]

Select the check box to encrypt the communication with the POP server using TLS.

[POP Authentication Method]

Set the authentication method of the POP server. Select [APOP] to encrypt the password when performing authentication or [POP AUTH] to perform user authentication via e-mail reception (POP).

[Confirm TLS Certificate for POP RX]

Select the check box to confirm whether the TLS server certificate is valid when receiving with POP. The machine verifies that the certificate has not expired or been revoked and checks the certificate chain for problems.

[Add CN to Verification Items]

Select the check box to also check the CN (Common Name) when checking the certificate used for POP reception.

[Allow TLS (SMTP RX)]

Select [Always TLS] or [On] to encrypt communication with TLS when receiving e-mail or I-fax using the SMTP server function.

5 Click [OK].

Basic Operations

Basic Operations	147
Using the Control Panel	149
Basic Screens	150
Items Displayed on the <Home> Screen	152
Basic Operation	154
Entering Characters	157
Logging into the Machine	159
Customizing the Display	160
Customizing the <Home> Screen	161
Switching the Displayed Language	162
Setting Sounds	163
Entering Sleep Mode	164

Basic Operations

E9SJ-034

This chapter describes basic operations that are common to the use of all functions, such as how to use the control panel.

■ Using the Control Panel

This section describes how to use the keys on the control panel to perform various operations, such as adjusting and checking the settings.



▶ **Using the Control Panel(P. 149)**

■ Logging into the Machine

This section describes how to log in when a login screen is displayed.



▶ **Logging into the Machine(P. 159)**

■ Customizing the <Home> Screen

This section describes how to rearrange the displayed items in order to make it easier to use screens shown in the <Home> Screen.



▶ **Customizing the <Home> Screen(P. 161)**

■ Specifying the Sound Settings

This section describes how to adjust the volume of various machine sounds, such as those produced when an error occurs.



▶ **Setting Sounds(P. 163)**

■ **Entering Sleep Mode**

This section describes how to set sleep mode.



▶ **Entering Sleep Mode(P. 164)**

Using the Control Panel

E9SJ-035

You can use the display and keys of the control panel to configure machine settings or operate functions. This section describes basic usage of the display and keys.



- ▶ **Basic Screens(P. 150)**
- ▶ **Basic Operation(P. 154)**
- ▶ **Entering Characters(P. 157)**

Adjust the brightness of the display

If it is hard to see the content of the display, adjust the brightness by operating the control panel.



<Set> ▶ <Preferences> ▶ <Accessibility> ▶ <Backlight Brightness> ▶ adjust the brightness with ◀ or ▶ ▶ **OK**

LINKS

- ▶ **Control Panel(P. 26)**

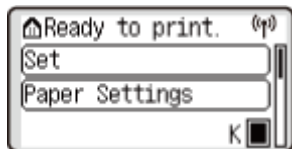
Basic Screens

E9SJ-036

This section describes the various screens displayed on the display.

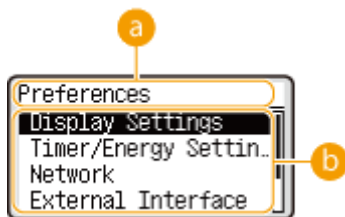
<Home> Screen

The <Home> screen is displayed when you press  (Home). The <Home> screen or settings screen appears on the display, allowing you to initiate functions such as <Memory Media> and <Mobile Portal>. You can also use the display to check information such as error messages and the machine's operation status.  **Items Displayed on the <Home> Screen(P. 152)**



<Menu> Screen

Select <Set> to display the <Menu> screen. Many of the settings of the machine, such as the management settings, display settings, and network settings, are configured by selecting <Set> first.



a Current menu level

The screen name of the current level is displayed.

b Setting item list

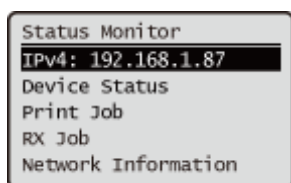
Setting items that belong to the current menu level are displayed in a list.

NOTE:

- When there is no menu under the lower level, the setting screen is displayed.

<Status Monitor> Screen

When you press  (Status Monitor), the <Status Monitor> screen is displayed. On this screen, you can check the printing status, as well as the remaining amount of toner and paper.



Error Screen

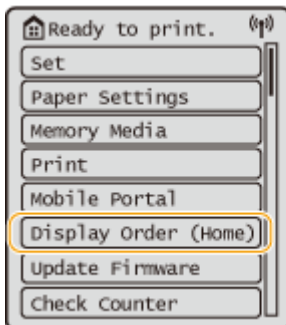
In some cases when an error occurs, instructions on how to respond to the error are displayed. Follow the on-screen instructions to solve the problem.  **Countermeasures for Each Message(P. 532)**

Example: When a paper jam occurs



TIPS

- Select <Display Order (Home)> to customize the <Home> screen by rearranging the buttons. [▶Customizing the Display\(P. 160\)](#)



- You can change settings regarding the screen display, such as which screen appears immediately after turning ON the machine, and whether the message appears for remaining paper and toner. [▶<Display Settings>\(P. 446\)](#)
- You can set the screen to be displayed when a certain amount of time has passed without operation. [▶<Function After Auto Reset>\(P. 449\)](#)

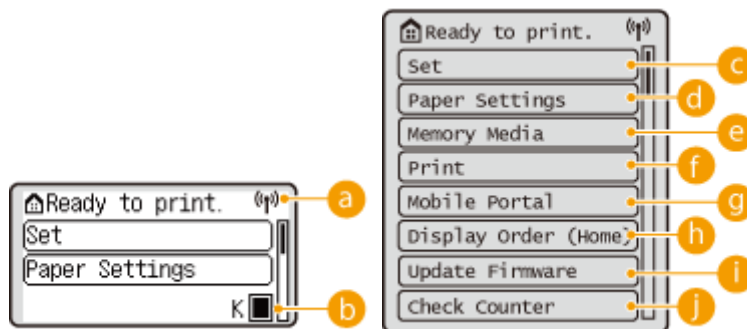
LINKS

- [▶Control Panel\(P. 26\)](#)

Items Displayed on the <Home> Screen

E9SJ-037

This section describes the items displayed on the <Home> screen.



a Wi-Fi icon

This icon is displayed when the machine is connected to wireless LAN.

b Amount remaining in the toner cartridge

The toner level of the toner cartridge is displayed. The remaining toner level can also be hidden. [▶<Display Icon Showing Remaining Toner>\(P. 447\)](#)

c <Set>

<Function Settings>, <Preferences>, and many other machine settings start from this button. [▶Settings/Registration\(P. 386\)](#)

d <Paper Settings>

This button enables you to specify the size and type of paper loaded in the paper drawer and multi-purpose tray. [▶Specifying Paper Size and Type\(P. 51\)](#)

e <Memory Media>

Select this to print files on USB memory. [▶Using Memory Media\(P. 202\)](#)

f <Print>

You can print documents held in the machine and check the status of print jobs.

g <Mobile Portal>

Select this to connect the machine to a mobile device. [▶Linking with Mobile Devices\(P. 208\)](#)

h <Display Order (Home)>

You can change the display order of the buttons on the <Home> screen. [▶Customizing the <Home> Screen\(P. 161\)](#)

i <Update Firmware>

You can update the firmware via the Internet. [▶Updating the Firmware\(P. 363\)](#)

<Check Counter>

You can display the total number of sheets printed.  **Checking the Number of Pages for Print(P. 378)**

You can also check the serial number of the machine, the IP address, and other device information such as information on optional equipment.

Basic Operation

E9SJ-038

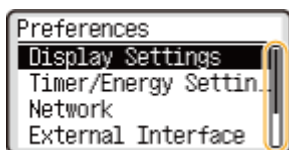
Even though functions and settings are different, the operation methods for buttons displayed on the screen and the procedure to select items are the same. This section describes the operation methods for buttons frequently displayed on the screen as well as how to select items.



Using ▲ / ▼

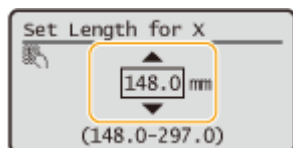
■ Scrolling the Screen

The scroll bar is displayed on the right side of the screen when not all of the information fits on one screen. If the scroll bar is displayed, use ▲ / ▼ to scroll up or down. The text and background colors of an item are inverted when it is selected.



■ Changing Setting Values

Use ▲ / ▼ to enter values. If  is displayed at the upper left of the screen, you can enter values directly using the numeric keys. **● Entering Characters(P. 157)**



NOTE:

- Values in () displayed below the entry box are the enterable value range.

Using ◀ / ▶

■ Proceeding to the Next Screen/Returning to the Previous Screen

Press ▶ to proceed to the next screen. Press ◀ to return to the previous screen.



NOTE:

- You can also proceed to the next screen by pressing **OK**, and return to the previous screen by pressing **↶** (Back).

■ Changing Setting Values

Use ◀ / ▶ to adjust the slider scale.



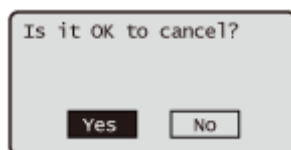
■ Moving the Cursor

Use ◀ / ▶ to enter text and values. ➤ **Entering Characters(P. 157)**



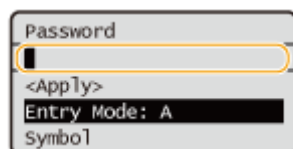
Using **OK**

Press **OK** to apply a setting.



Using the Numeric Keys

Use the numeric keys to enter text and values. ➤ **Entering Characters(P. 157)**



TIPS

- You can change a variety of display-related settings, such as the display language: ➤ **<Display Settings>(P. 446)**
- You can change the screen that is automatically displayed when the machine remains idle for a specified length of time: ➤ **<Function After Auto Reset>(P. 449)**

- You can change a variety of accessibility-related settings, such as the scroll speed: [▶<Accessibility>\(P. 467\)](#)

LINKS

[▶Control Panel\(P. 26\)](#)

[▶Entering Characters\(P. 157\)](#)

Entering Characters

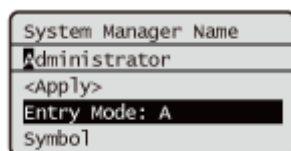
E9SJ-039

Use the numeric keys to enter text and values.



Switching the Type of Text

Press ***** to switch the type of text that is entered.



NOTE

- You can also select <Entry Mode> and press **OK** to switch the type of text.

Types of Text That Can Be Entered

Text that can be entered is listed below.

Key	A	a	12
1	@ . - _ /		1
2	ABC	abc	2
3	DEF	def	3
4	GHI	ghi	4

Basic Operations

5	JKL	jkl	5
6	MNO	mno	6
7	PQRS	pqrs	7
8	TUV	tuv	8
9	WXYZ	wxyz	9
0	(Not available)		0
#	(space) -. * # ! " , ; : ^ ` _ = / ' ? \$ @ % & + \ ~ () [] { } < >		(Not available)

NOTE

- Press **#** or select <Symbol> and press **OK** when the type of text that is entered is <A> or <a> to display enterable symbols in the screen. Use **▲** / **▼** / **◀** / **▶** to select the symbol you want to enter, and press **OK**.

Deleting Text

One character is deleted each time **C** (Clear) is pressed. Press and hold **C** (Clear) to delete all of the entered text.

Moving the Cursor (Entering a Space)

Press **◀** or **▶** to move the cursor. To enter a space, move the cursor to the end of the text, and press **▶**.

Logging into the Machine

E9SJ-03A

If Department ID Management is enabled or System Manager IDs are enabled, you must log in before using the machine. When the login screen appears, use the procedure below to enter the Department ID and PIN.

NOTE

- If <Auto Reset Time> is set, the user is automatically logged out when no operations are performed for a specified period. ➤<Auto Reset Time>(P. 449)

1 Select <Department ID> or <System Manager ID>.

2 Enter the ID and press **OK**.

3 Select <PIN>.

4 Enter the PIN and press **OK**.

5 Press **ID**.

➡ When login is successful, the machine functions become available.

- Log out after use.

LINKS

- Using the Control Panel(P. 149)
- Customizing the Display(P. 160)
- Managing Users(P. 241)
- Starting the Remote UI(P. 329)

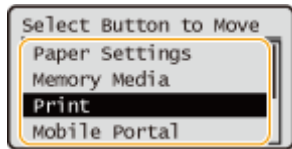
Customizing the Display

E9SJ-03C

In order to make the <Home> screen easier to use, you can customize it.

Customizing the <Home> Screen

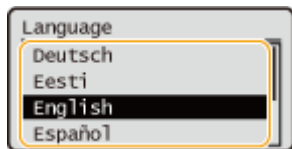
You can rearrange the displayed items and customize the screen to make it easier to select functions.



▶ Customizing the <Home> Screen(P. 161)

Changing the Displayed Language

You can change the language displayed on the screen.



▶ Switching the Displayed Language(P. 162)

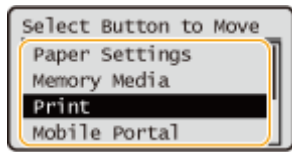
LINKS

▶ Using the Control Panel(P. 149)

Customizing the <Home> Screen

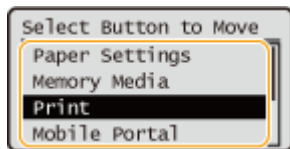
E9SJ-03E

You can freely change the display order of items to make the buttons easier to use.

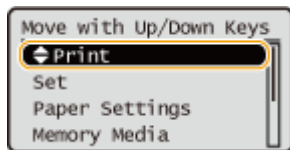


1 Select <Display Order (Home)> on the <Home> screen.  <Home> Screen(P. 150)

2 Use ▲ / ▼ to select the item to be moved, and press .



3 Use ▲ / ▼ to move to the target position, and press .



4 When the buttons are rearranged in the way you want, press  (Back).

NOTE:

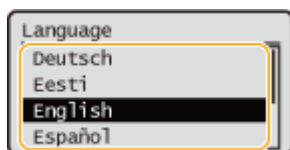
- Operating this setting requires administrator privileges.

Switching the Displayed Language

E9SJ-03F

You can change the language displayed on the screen.

- 1** Select <Set> on the <Home> screen. ▶ <Home> Screen(P. 150)
- 2** Select <Preferences> ▶ <Display Settings> ▶ <Language>.
- 3** Select a language from the list.



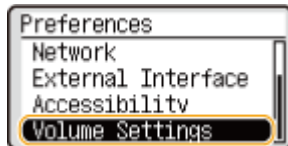
Setting Sounds

E9SJ-03H

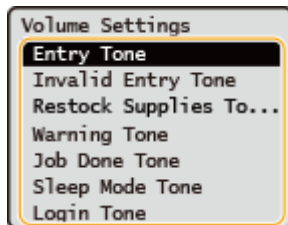
The machine produces sounds in a variety of situations, such as when control panel keys are pressed, or when a malfunction occurs. You can specify whether or not set each sound individually.

1 Select <Set> on the <Home> screen. ▶ <Home> Screen(P. 150)

2 Select <Preferences> ▶ <Volume Settings>.



3 Select a setting ▶ select <On> or <Off>.



Setting Items	Description
<Entry Tone>	Sound produced each time a key on the control panel is pressed
<Invalid Entry Tone>	Sound produced when an invalid key operation is performed, or when you enter a number outside the valid setting range
<Restock Supplies Tone>	Sound produced when the amount of toner is low
<Warning Tone>	Sound produced when a malfunction such as paper jam or operational error occurs
<Job Done Tone>	Sound produced when an operation such as printing is complete
<Sleep Mode Tone>	Sound produced when the machine enters sleep mode, or when the machine is turned OFF if you set <Quick Startup Settings for Main Power> to <On>. (Depending on the situations, the machine does not startup quickly and the tone does not sound.)
<Login Tone>	Sound produced when login is successful

Entering Sleep Mode

E9SJ-03J

The sleep mode function reduces power consumption by temporarily disabling some internal operations of the machine. If no operations will be performed on the machine for a while, such as during a lunch break, you can save power simply by pressing  (Energy Saver) on the control panel.



IMPORTANT

Press  (Energy Saver) if the machine will not be used for a long period of time, such as overnight

- Put the machine into Sleep mode as a safety precaution.

NOTE

When in sleep mode

- When the machine enters the sleep mode,  (Energy Saver) lights up yellow green.

Situations in which the machine does not enter the sleep mode

- When the machine is in operation
- When the Data indicator is lit up or blinking  **Control Panel(P. 26)**
- When the machine is performing an operation such as adjustment or cleaning
- When a paper jam occurs
- When the menu screen is displayed
- If <Energy Saver/Sleep Mode Exit Time Set.> is set to <Off> when an error occurs
- When the SSID/network key screen for Direct Connection is displayed

- When settings are being imported or exported

Exiting Sleep Mode

You can press  (Energy Saver) or any other key on the control panel to exit the sleep mode.

When You Want to Set the Auto Sleep Timer

You can use the <Auto Sleep Time> setting to automatically put the machine into sleep mode. If you want to change the amount of time that elapses before the machine enters auto sleep mode, follow the procedure below.



<Set> ► <Preferences> ► <Timer/Energy Settings> ► <Auto Sleep Time> ► ▲ or ▼ to select the amount of time that elapses before the machine automatically enters the sleep mode.

NOTE

- You can set the time range to automatically enter the sleep mode by the day of the week.  <Auto Sleep Weekly Timer> (P. 451)

Energy Consumption in the Sleep Mode

You can set the amount of energy that the machine consumes when it is in the sleep mode. Follow the procedure below to set the amount of energy consumed in the sleep mode.



<Set> ► <Preferences> ► <Timer/Energy Settings> ► <Sleep Mode Energy Use> ► select <Low> or <High>.

NOTE

- If you select <Low>, energy consumption in the Sleep mode is low, but it takes longer to recover from the Sleep mode.

When using a wireless LAN also while in sleep mode

- Set <Sleep Mode Energy Use> to <High>.  <Sleep Mode Energy Use> (P. 450)

Exiting Sleep Mode at a Specified Time

You can configure a setting so that the sleep mode is released at the specified time. If you want to set the time at which the machine recovers from the sleep mode, follow the procedure below.



<Set> ► <Preferences> ► <Timer/Energy Settings> ► <Sleep Mode Exit Time Settings> ► <On> ► ▲ or ▼ to select the amount of time that elapses before the machine automatically returns from the sleep mode.

Keeping the Control Panel in Sleep Mode when Print Jobs Are Received

You can set the machine to keep the control panel in the sleep mode when a print job is received. You can also set the machine to recover the control panel from the sleep mode when a print job is received so that the user can tell when a job has been received.



<Set> ▶ <Preferences> ▶ <Timer/Energy Settings> ▶ <Settings for Sleep Mode Exit upon Job RX>
▶ <Do Not Turn Device Control Panel On>.

NOTE

- If you select <Turn Device Control Panel On> in <Settings for Sleep Mode Exit upon Job RX>, power consumption is higher than when <Do Not Turn Device Control Panel On> is selected.

Printing

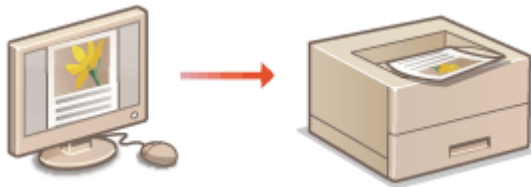
Printing	168
Printing From a Computer	170
Canceling Printing	173
Checking the Printing Status and History	175
Printing from an External Network (IPP Printing)	176
Advanced Functions for Printing	179
Printing Documents that are Forced to be Held in the Machine	180
Printing Held Documents Automatically When Logging In	182
Print Screen	183
Printing Out Secured Documents	185
Various Printing Methods	187
Directly Printing Files without Opening Them	188
Printing Using a Virtual Printer	190
Printing From Memory Media (Media Print)	192
Printing Received E-mail (E-Mail Print)	193
Printing Using the Microsoft Cloud Service (Universal Print)	194
Configuring the Universal Print User Settings	198

Printing

You can print documents and images prepared on a computer. This section introduces basic procedures and convenient printing functions.

■ Introduction of basic operations

This section describes the basic operation methods when printing from a computer.



- ▶ **Printing From a Computer(P. 170)**
- ▶ **Canceling Printing(P. 173)**
- ▶ **Checking the Printing Status and History(P. 175)**
- ▶ **Printing from an External Network (IPP Printing) (P. 176)**

■ Advanced functions for printing

This section introduces functions used when you want to print a sample set or edit the document before printing large quantities, avoid to leave or to be copied printed paper, etc.



- ▶ **Printing Documents that are Forced to be Held in the Machine(P. 180)**
- ▶ **Printing Out Secured Documents(P. 185)**

■ Printing in various environments

This section introduces printing methods for printing without the printer driver of the machine such as printing without your computer during a business trip, etc.



- ▶ **Directly Printing Files without Opening Them(P. 188)**
- ▶ **Printing Using a Virtual Printer(P. 190)**
- ▶ **Printing From Memory Media (Media Print)(P. 192)**
- ▶ **Printing Received E-mail (E-Mail Print)(P. 193)**
- ▶ **Printing Using the Microsoft Cloud Service (Universal Print) (P. 194)**

TIPS

- You can print photographs, PDF files, etc. from a mobile device such as a smart phone, tablet, etc. For more information, see [▶Linking with Mobile Devices\(P. 208\)](#) .

Printing From a Computer

E9SJ-03L

This section describes basic printing from a computer with the printer driver installed.

- ▶ **Help for Printer Drivers(P. 170)**
- ▶ **Basic Printing Operations(P. 170)**

Help for Printer Drivers

Clicking [Help] (Window) or ? (Mac OS) on the printer driver setting screen displays the Help screen. For information that is not in the User's Guide, including about driver features and how to set up those features, see Help.

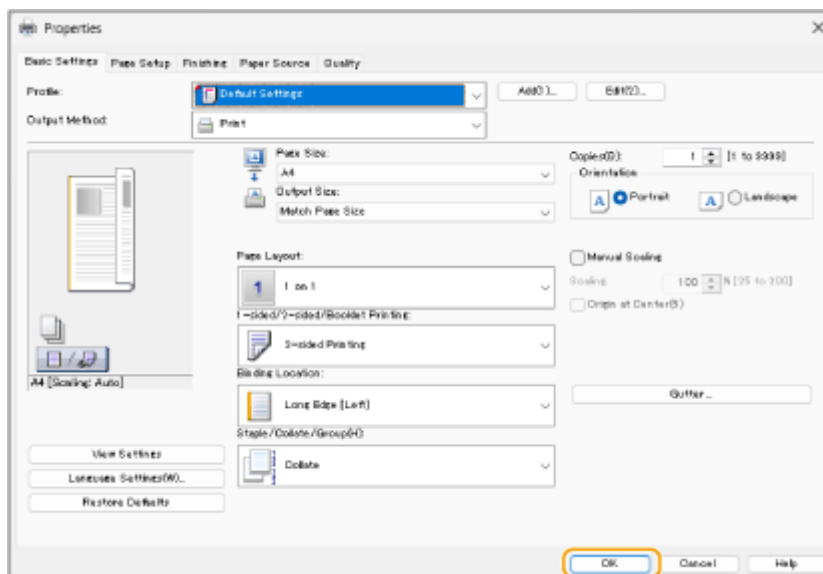
Basic Printing Operations

This section describes the basic flow when printing from a computer.

- ▶ **In case of Windows(P. 170)**
- ▶ **In case of Mac OS(P. 171)**

Windows

- 1 Open a document and display the print screen.**
- 2 Select the machine and click [Preferences] or [Properties].**
- 3 Specify the print settings as necessary and click [OK].**
 - Switch tabs as necessary to specify the desired print settings.



4 Click [Print] or [OK].

⇒ Printing starts.

- If you want to cancel, see [Canceling Printing\(P. 173\)](#) .

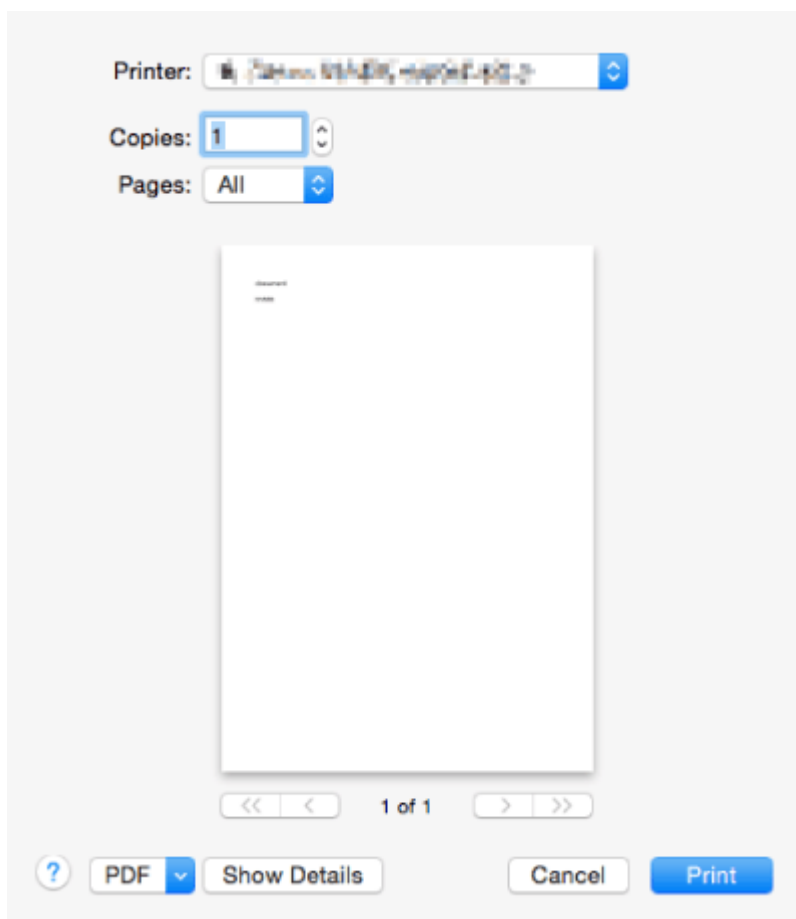
Mac OS

1 Open a document and display the print screen.

2 Select the machine.

3 Specify the print settings as necessary.

- After selecting the setting panel from the drop-down list, set for printing on each panel.



4 Click [Print].

⇒ Printing starts.

- If you want to cancel, see [Canceling Printing\(P. 173\)](#) .

LINKS

▶ **Checking the Printing Status and History(P. 175)**

Canceling Printing

E9SJ-03R

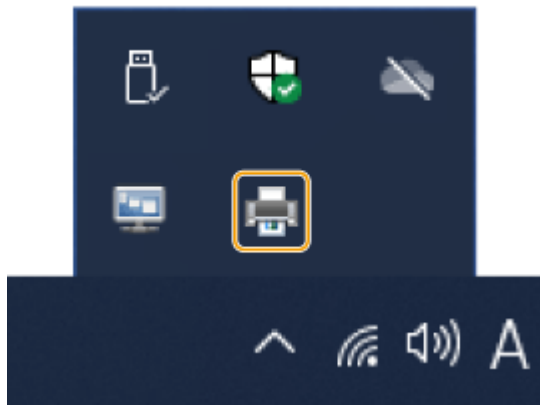
You can cancel printing before it has finished. You can also cancel a print job on the control panel of the machine. ▶
Checking the Printing Status and History(P. 175)

▶ In case of Windows(P. 173)

▶ In case of Mac OS(P. 174)

Windows

1 Double-click the printer icon displayed in the task tray of the desktop.



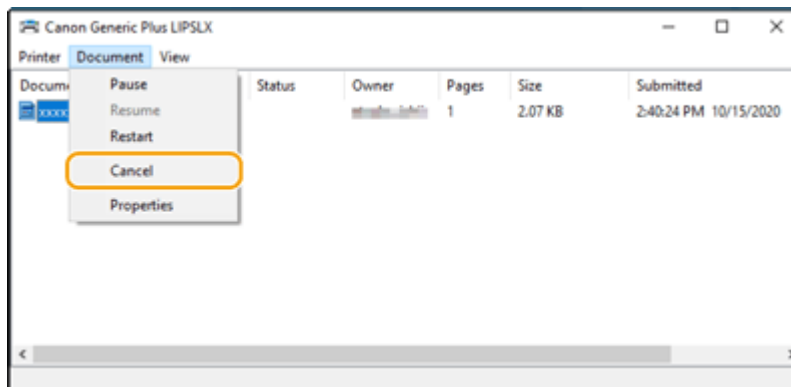
NOTE

When the printer icon is not displayed

- Open the printer folder, and click or double-click the icon for the machine.

2 Select the document to cancel and click [Document] ▶ [Cancel].

- If you cannot find the document to cancel, the document is already sent to the machine. In that case, you cannot cancel the printing on the computer.



3 Click [Yes].

⇒ Printing is canceled.

Mac OS

- 1** Click the printer icon displayed on the Dock.



- 2** Select the document to cancel and click [Delete] or .

⇒ Printing is canceled.

Checking the Printing Status and History

E9SJ-03S

You can check the wait status for print jobs and whether or not an error has occurred during printing. Operations such as printing the document ahead of other documents and temporarily suspending or canceling printing are possible as well.

NOTE

- When personal authentication management is used, you can restrict users from performing operations on the jobs of other users on the <Status Monitor> screen. [▶<Restrict Access to Other User Jobs>\(P. 487\)](#)

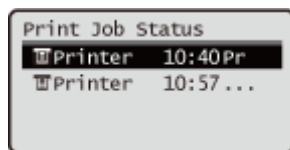
1 Press  (Status Monitor).

2 Select <Print Job>.

3 Select the print statuses and logs.

■Checking the status of printing

1 In <Job Status>, select the document to check the status of.



⇒ Display detailed information about the document.

■Checking the printing history

1 In <Job Log>, select an item ▶ select the document to check the history of.

- <OK> is displayed when a document was printed successfully, and <Error> is displayed when a document failed to be printed because it was canceled or there was some error.



⇒ Displays detailed information about the document.

LINKS

[▶Canceling Printing\(P. 173\)](#)

Printing from an External Network (IPP Printing)

E9SJ-03U

Using the IPP port enables you to print from an external network via the Internet. To use IPP printing, you must specify the IPP port in the printer driver. To use IPPS also, you must install this machine's key and certificate on your computer.  **Installing This Machine's Key and Certificate on Your Computer(P. 177)**

IMPORTANT

- To use IPP printing, you must specify the <IPP Print Settings>.  **<IPP Print Settings>(P. 455)**
- To perform the following procedure, you need to log in to your computer with the administrator account.

1 Prepare the printer driver.

- If the machine is supplied with a CD-ROM, insert the CD-ROM into the drive on the computer.
- To download the printer driver, go to the Canon website (<https://global.canon/en/support/>) and download your printer driver.

2 Select [Windows System] ▶ [Control Panel] ▶ [Hardware and Sound] ▶ [Devices and Printers].

3 Click [Add a printer].

4 Click [The printer that I want isn't listed].

5 Select [Select a shared printer by name], enter the connection destination and click [Next].

- To use IPP, enter "http://<IP address of the machine>/ipp" for the connection destination.
- To use IPPS, enter "https://<IP address of the machine>/ipp" for the connection destination.

6 Click [Have Disk...].

7 Click [Browse...].

8 Specify the folder containing the printer driver, select the INF file and click [Open].

- The INF file is stored in the [Driver] folder.

9 Proceed with the settings by following the on-screen instructions.

➡ The printer driver is installed. To use IPPS, install this machine's key and certificate on your computer.

■ Installing This Machine's Key and Certificate on Your Computer

This description shows the procedure for installing the key and certificate using the Microsoft Edge.

- 1 Start the Web browser.**
- 2 Enter "http://<IP address of the machine>/" in the address input field and press the [ENTER] key on the computer keyboard.**
- 3 Click [Not Secure] ► [Your connection to this site isn't secure] ► [Show certificate] in the URL input field.**
- 4 Click [Copy to File...] on the [Details] tab.**
- 5 Click [Next].**
- 6 Select a file format and click [Next].**
- 7 Set the save destination and certificate file name and then click [Next].**
- 8 Check the content being saved and click [Finish] ► [OK].**
 This completes certificate saving.
- 9 Click [OK].**
- 10 Close the Web browser.**
- 11 Install the certificate saved in step 8 on your computer.**

■ For DER/Base64 (with the ".cer" extension)

- 1 Double-click the saved certificate.**
- 2 Click [Install Certificate...].**
- 3 Select a save location and click [Next].**
- 4 Select [Place all certificates in the following store] then [Browse...] ► [Trusted Root Certification Authorities], and then click [OK].**
- 5 Click [Next] ► [Finish].**

■ **For PKCS#7 (with the "p7b" extension)**

- 1** Double-click the saved certificate.
- 2** Double-click the path for the folder containing the certificate with the name shown in [Logical Store Name].
- 3** Double-click the [Certificates] shown in [Object Type].
- 4** Double-click the file shown in [Issued To].
- 5** Click [Install Certificate...].
- 6** Select a save location and click [Next].
- 7** Select [Place all certificates in the following store] then [Browse...] ► [Trusted Root Certification Authorities], and then click [OK].
- 8** Click [Next] ► [Finish].

Advanced Functions for Printing

E9SJ-03W

This section introduces methods for printing with increased security.



▶ **Printing Documents that are Forced to be Held in the Machine(P. 180)**



▶ **Printing Out Secured Documents(P. 185)**

Printing Documents that are Forced to be Held in the Machine

E9SJ-03X



To avoid leaving printed material or accidental information leakage, etc., the machine may be configured so that it will not print data soon after it receives the data from a computer. **▶Configuring the Forced Hold Printing Settings(P. 321)**
In that case, you need to operate the machine to print the held data.

! IMPORTANT

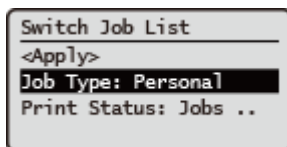
- When a certain length of time elapses before the held data is printed, the data is deleted automatically and cannot be printed.

NOTE

- The documents retained in the machine are saved even if the machine is turned OFF.
- You can change the length of time for retaining the held data. **▶<Job Storage Period>(P. 484)**

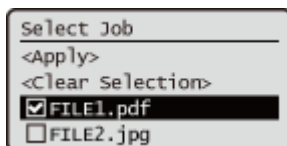
1 Select **<Print>** on the **<Home>** screen. **▶<Home> Screen(P. 150)**

2 Select the document type under **<Job Type>** on the **<Switch Job List>** screen.



3 Select **<Apply>**.

4 Select documents on the **<Select Job>** screen and press **OK**.



NOTE:

- You can select and print up to 100 documents at the same time.

5 Select **<Apply>**.

6 Select <Start Printing>.

■▶▶▶ Printing starts.

NOTE:

- When you want to cancel a print job, select the job you want to cancel under <Jobs Printed> and select <Delete Job>. You can also cancel a print job by pressing  (Stop) on the control panel and selecting the job to cancel from the print job list.
- By pressing  (Status Monitor), you can check the printing status or history. ▶ **Checking the Printing Status and History(P. 175)**

TIPS

Printing automatically when logging in

- If the auto print function is enabled, you can set the machine to print your own held documents automatically when you log in to the machine. ▶ **Printing Held Documents Automatically When Logging In(P. 182)**

Printing Held Documents Automatically When Logging In

E9SJ-03Y

You can set the machine to print your own held documents automatically when you log in to the machine.

- 1 Start the Remote UI.** ▶ **Starting the Remote UI(P. 329)**
- 2 On the portal page, click [Settings/Registration].** ▶ **Remote UI Screen(P. 331)**
- 3 Click [Printer] ▶ [Print].**
- 4 Confirm that [Force Hold] is selected.**
- 5 Select [Enable Auto Print Function When Logging In].**
- 6 Click [OK].**

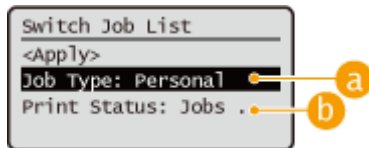
NOTE

- When a user logs in, only the documents belonging to the login user are printed automatically. The following documents that need a PIN or a password when printing are not printed automatically.
 - Encrypted secured print documents
 - Encrypted PDF
- Up to 100 documents are printed at a single occasion of a user login.

Print Screen

When you select <Print> on the <Home> screen on the control panel, the <Switch Job List> screen is displayed. On this screen, you can filter held documents according to the job type and the print status. When you select <Apply> on the <Switch Job List> screen, you can select documents on the <Select Job> screen. You can print or delete the selected documents.

■ <Switch Job List> screen



a <Job Type>

Select the type of the documents displayed on the list.

- <Personal>: Displays the documents of a log in user
- <Shared>: Displays the documents that are held under specific conditions
*The documents under <Shared> are displayed for every user and can be printed by every user.
- <Group>: Displays the documents under the same department ID as that of a login user.

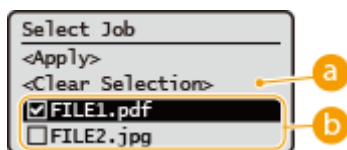
NOTE:

- <Group> is available only when using IC card authentication.

b <Print Status>

Select the job status that is displayed on the list from <Jobs to Be Printed> and <Jobs Printed>.

■ <Select Job> screen



a <Select All>/<Clear Selection>

- If you press <Select All> when no document is selected, all documents in the list are selected.
- If you press <Clear Selection> when documents are selected, the entire selection is canceled.

b List of documents

The following documents are displayed in the list.

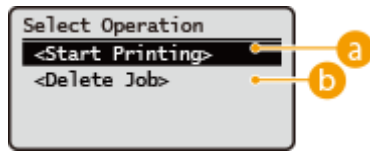
- Held
- Secured printed
- Encrypted secured printed

When you select a document, a check mark is added.

NOTE:

- Up to 100 documents can be selected at the same time.

■ <Select Operation> screen



a <Start Printing>

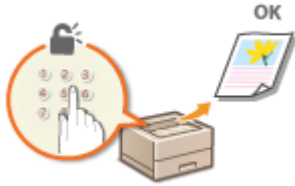
Starts printing selected documents.

b <Delete Job>

Deletes selected documents.

Printing Out Secured Documents

E9SJ-041



This section describes how to print a document from an application as a secured document.

➤ Sending a Secured Document from a Computer to the Machine(P. 185)

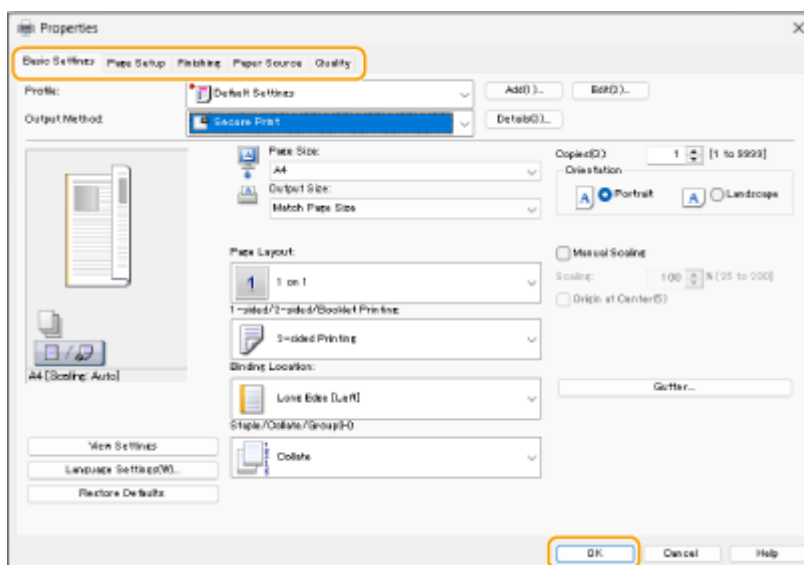
Sending a Secured Document from a Computer to the Machine

- 1** Open a document in an application and display the print dialog box.
- 2** Select the printer driver for this machine, and click [Preferences] or [Properties].
- 3** Select [Secured Print] in [Output Method].

➡ The [Information] pop-up screen is displayed. Check the message, and click [Yes] or [No].

- 4** Specify the print settings as necessary, and click [OK].

- Switch the tab according to the settings.



- 5** Click [Print] or [OK].

- ➡ After the secured document is sent to the machine, it is held in the memory of the machine waiting to be printed.

LINKS

- ▶ **Checking the Printing Status and History(P. 175)**

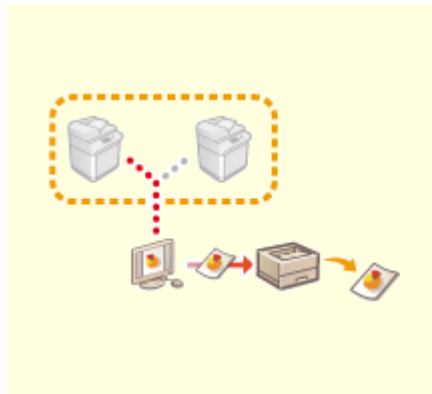
Various Printing Methods

E9SJ-042

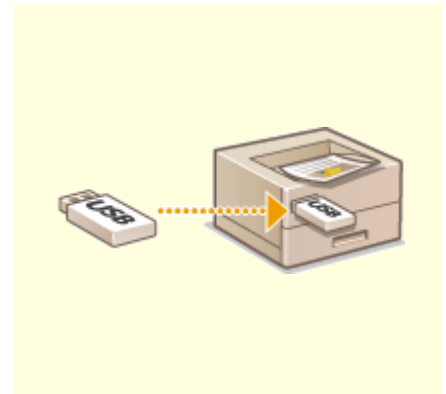
This section introduces printing method using the Remote UI, or how to print a file stored in memory media.



▶ Directly Printing Files without Opening Them(P. 188)



▶ Printing Using a Virtual Printer(P. 190)



▶ Printing From Memory Media (Media Print)(P. 192)



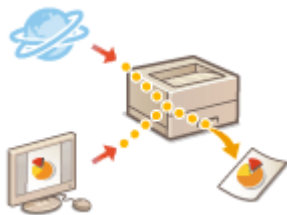
▶ Printing Received E-mail (E-Mail Print)(P. 193)



▶ Printing Using the Microsoft Cloud Service (Universal Print) (P. 194)

Directly Printing Files without Opening Them

E9SJ-043



By using remote UI, it is possible to print files saved on a computer or network directly from the machine without using the printer driver. You do not need to open files on the computer for printing.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Direct Print] on the portal page. ▶ Remote UI Screen(P. 331)
- 3 Select a file format and then a file.

NOTE:

- In [Image File], you can print JPEG or TIFF files.

4 Specify the print settings as necessary.

- If a password is set for the PDF file, press [Specify PDF File] ▶ enter the password in [Document Password]. When printing PDF files linked to the policy server, select [Specify PDF File] ▶ enter the policy server user name in [Policy Server User Name] and the policy server password in [Policy Server Password].
- To print the PDF file which is prohibited for printing, or to print PDF files that only allow low-resolution printing in high resolution, enter the master password.
- Depending on the selected paper size, PDF/XPS files may be canceled on printing.

5 Click [Start Printing].

➡ Printing starts.

IMPORTANT

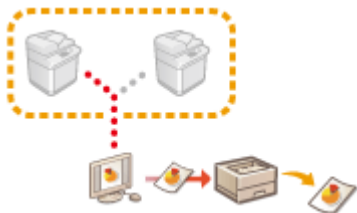
- Do not click [Start Printing] repeatedly during file transfer. Otherwise, file malfunction may occur and the file may not be transferred.
- Printing may not be performed properly depending on the data.

NOTE

- If printing with Direct Print is not possible or the printing position deviates, opening files from the application and using the printer driver may enable proper printing.

Printing Using a Virtual Printer

E9SJ-044



A virtual printer enables you to use LPD printing or FTP printing with the print settings registered as a virtual printer in advance. For example, registering settings such as the paper type, number of copies, and two-sided printing in advance eliminates the need to specify these settings for each job.

▶ **Adding a Virtual Printer(P. 190)**

▶ **Printing with a Virtual Printer(P. 191)**

! IMPORTANT

- For Secure Print and Encrypted Secure Print, the virtual printer is disabled and the job is held in the machine.

NOTE

- Set ▶ **<LPD Print Settings>(P. 454)** to <On> to perform LPD printing.
- Set ▶ **<FTP Print Settings>(P. 454)** to <On> to perform FTP printing.
- The page description language and file format that can be used with a virtual printer is PS and PDF.

Adding a Virtual Printer

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [Printer] ▶ [Virtual Printer Management].**
- 4 Click [Add Virtual Printer].**

NOTE

- Operations cannot be performed from multiple browsers at the same time.

- 5 Enter the virtual printer name and specify the required settings.**

Virtual Printer Management - Add Virtual Printer

Virtual Printer Name: (Max 64 characters)

Settings for Virtual Printer

Select	Item Name	Change Settings
☐	Paper Source	Auto
☐	Paper Type	Auto
☐	Paper Output	Auto
☐	Number of Copies	1 (1-9999)
☐	2-Sided Printing	Off
☐	Print Range	All Pages
☐	First Page	1 (1-9999)
☐	Last Page	1 (1-9999)
☐	Toner Save	Off

NOTE

- Multiple virtual printers with the same name cannot be registered.
- A maximum of 20 virtual printers can be registered.

6 Click [Add].

NOTE

- You are required to log in to the Remote UI with Administrator privileges to configure this setting. For more information, see the items in [Select Role to Set:] in [▶Registering User Information in the Local Device\(P. 246\)](#).
- This setting can be imported/exported with models that support batch importing of this setting. [▶Importing/Exporting the Setting Data\(P. 357\)](#)
- This setting is included in [Settings/Registration Basic Information] when batch exporting. [▶Importing/Exporting All Settings\(P. 359\)](#)

Printing with a Virtual Printer

For LPD printing

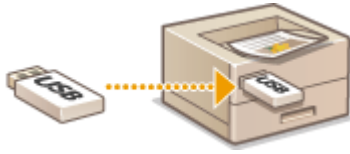
- LPR -S [IP address of the machine] -P [virtual printer name] [file name]
Example: Printing "sample.pdf" with a virtual printer named "001"
lpr -S IP address of the machine -P 001 sample.pdf

For FTP printing

- put [file name] [virtual printer name]
Example: Printing "sample.pdf" with a virtual printer named "001"
> put sample.pdf 001

Printing From Memory Media (Media Print)

E9SJ-045



It is possible to print files saved on memory media directly from the machine without using a computer. This is convenient when printing after bringing data back from an outside location or when printing data you have brought with you to a business destination.

NOTE

Using memory media

- For available memory media and information on inserting/removing memory media, see [▶Connecting a USB Memory Device\(P. 20\)](#) .
- For instructions on using memory media, see [▶Using Memory Media\(P. 202\)](#) .
- Depending on the file format, an optional product may be required. [▶System Options\(P. 610\)](#)

Printing Received E-mail (E-Mail Print)

E9SJ-046



E-Mail Print allows you to print the message and attached TIFF image files of an e-mail received from the POP3 mail server without using a computer. E-mails can be manually received as well as being automatically received at regular intervals. When the SMTP protocol is used, e-mails directly sent to the machine via no mail server are printed.

▶ Manually Receiving E-Mails(P. 193)

NOTE

- Some files are unavailable depending on the file structure.
- For information on the settings for receiving and printing e-mail with the machine, see ▶ **Configuring E-Mail Print Settings(P. 143)** .
- For information on the specification of the e-mail print, see ▶ **Printer Functions(P. 599)** .

■ Outline of E-Mail Print

General

- An e-mail message is printed with e-mail header information.
- If the text in the e-mail body field does not fit in one line, a line break is automatically inserted.

! IMPORTANT

- When the toner cartridge is nearly empty, no e-mails can be received.

Manually Receiving E-Mails

If e-mail printing from the POP3 mail server is enabled, you can manually receive and print e-mails as well. When you want to connect to the mail server before automatically receiving e-mails or the machine is configured to prevent e-mails from being automatically received, follow the procedure below to manually receive the e-mails.

1 Press  (Status Monitor).

2 Select <RX Job> ▶ <Check E-Mail RX>.

⇒ The machine is connected to the mail server. E-Mail Print is started for new e-mails in the mailbox of the mail server if any.

LINKS

- ▶ **Checking the Printing Status and History(P. 175)**
- ▶ **Printing Reports and Lists(P. 379)**

Printing Using the Microsoft Cloud Service (Universal Print)

E9SJ-047



Universal Print is a Microsoft service that enables you to print documents via the cloud. There is no need to install a printer driver to print documents from your computer. You can also print documents from a remote location as long as your computer is connected to the Internet.

Conditions of Use

To use Universal Print, you must first register as a Microsoft 365 service user and use the Microsoft Entra ID Service.

NOTE

- You cannot use Universal Print for communication using a sub line.

Required Settings

Administrator settings

Use the Remote UI to register this machine in Microsoft Entra ID. ➤ **Registering This Machine in Microsoft Entra ID(P. 195)**

User settings

Configure your computer so that Universal Print can be used. ➤ **Configuring a Printer Registered in Microsoft Entra ID on the Computer(P. 197)**

NOTE

When a proxy server is used

- To use Universal Print via a proxy server, you must also configure the proxy settings on your computer.

Associating Users and Universal Print Jobs

You can associate Universal Print jobs with users authenticated through User Authentication. You can still use Universal Print without configuring these settings. ➤ **Configuring the Universal Print User Settings(P. 198)**

Printing with Universal Print

See the Microsoft website for information on printing with Universal Print.



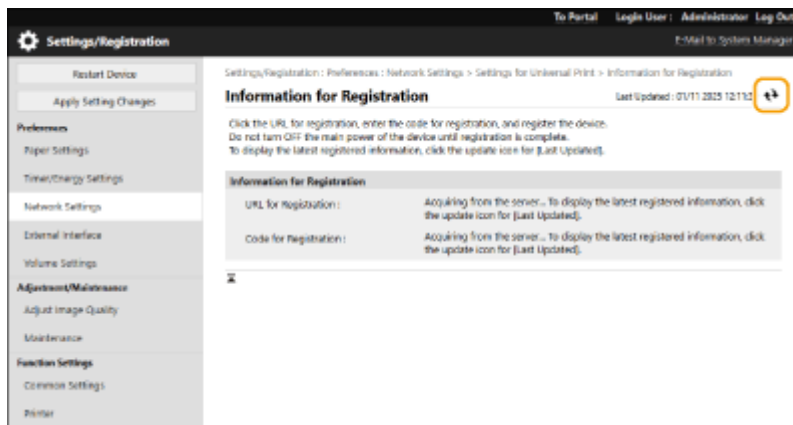
- In some operating systems, print errors or problems with the print results may occur. See Universal Print Troubleshooting on the Microsoft website for information on the compatibility of your operating system.

NOTE

- If Forced Hold printing is enabled, Universal Print jobs will run as specified in the Forced Hold printing settings. ➤ **Configuring the Forced Hold Printing Settings(P. 321)**

Registering This Machine in Microsoft Entra ID

- 1 Start the Remote UI.** ➤ **Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page.** ➤ **Remote UI Screen(P. 331)**
- 3 Click [Network Settings] ▶ [Settings for Universal Print].**
- 4 Click [Edit] for [Basic Settings].**
- 5 Select the [Use Universal Print] checkbox and enter the printer name in the [Printer Name] field.**
 - To verify the server certificate sent from the server, select the [Verify Server Certificate] checkbox.
 - To add CN (Common Name) to the items to be verified, select the [Add CN to Verification Items] checkbox.
 - Normally, you do not need to change [Application ID], [Microsoft Entra ID Authentication URL], or [Microsoft Entra ID Registration URL]. You need to change the settings only when using a specific cloud environment.
 - To return [Microsoft Entra ID Authentication URL], [Microsoft Entra ID Registration URL], and/or [Application ID] to the initial settings, click [Initial Settings] for the setting(s), or enter the following initial settings manually:
 - [Microsoft Entra ID Authentication URL]: <https://login.microsoftonline.com/organizations/oauth2/v2.0>
 - [Microsoft Entra ID Registration URL]: <https://register.print.microsoft.com/api/v1.0/register>
 - [Application ID]: f9fc375c-c7ba-4e5c-b213-23affd792cc1
- 6 Click [OK].**
- 7 Click [Register] in [Registration Status].**
- 8 Wait a few seconds, and then click [↺].**



9 Click the URL link displayed for [URL for Registration].

10 Follow the instructions on the screen to register the machine.

11 Wait a few minutes, and then click [↻] in the Remote UI screen.

➡ Once registration is completed, [Registered] appears in [Registration Status].

12 View the Universal Print management screen of Microsoft Entra ID in your web browser.

13 Select the registered machine and click [Share Printer].

- To change the name displayed on the computer, enter the new name in [Printer Share Name], and then click [Share Printer].

➡ [Printer shared.] appears at the top right of the screen.

14 Click [Members], and then click [Add].

15 Select the members and groups who will use the registered printer from the list.

- The selected members and groups will be able to use the printer.

■ To Delete a Registered Printer

1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)

3 Click [Network Settings] ▶ [Settings for Universal Print].

- 4** Click [Registration Status] for [Unregister].
- 5** Click [OK].
- 6** View the Microsoft Entra ID device management screen in your web browser.
- 7** Select the model to be deleted and click [Delete].

Configuring a Printer Registered in Microsoft Entra ID on the Computer

- 1** Click [Windows] ► [Settings] ► [Accounts].
- 2** Click [Access work or school] ► [Connect].
- 3** Follow the on-screen instructions to sign in to your Microsoft 365 account.
- 4** Click [Home] ► [Devices].
- 5** Click [Printers & scanners] ► [Add a printer or scanner].
- 6** Select a registered printer from the list.

Configuring the Universal Print User Settings

E9SJ-048

Configure these settings if you want to manage users authenticated through User Authentication and their associated Universal Print jobs. Universal Print can still be run without configuring these settings.

- **Set by the User(P. 198)**
- **Set by the Administrator(P. 198)**
- **Set by the Administrator Using a CSV File(P. 199)**

Set by the User

- 1 Start the Remote UI. ➤Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ➤Remote UI Screen(P. 331)**
- 3 Click [User Management] ► [Authentication Management].**
- 4 Enter [User Name for Universal Print:] in [Information for Universal Print].**
 - In [User Name for Universal Print:], enter the email address or phone number used in the Microsoft 365 account.

Set by the Administrator

- 1 Start the Remote UI. ➤Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ➤Remote UI Screen(P. 331)**
- 3 Click [User Management] ► [Authentication Management].**
- 4 Click [Edit] for the user to be set.**

NOTE:

If the Universal Print user is not registered

- Click [Add User] and register the user information. When registering the user information, enter the [User Name for Universal Print:] in [Information for Universal Print].

- 5 Enter [User Name for Universal Print:] in [Information for Universal Print].**

- In [User Name for Universal Print:], enter the email address or phone number used in the Microsoft 365 account.

6 Click [Update].

Set by the Administrator Using a CSV File

You can associate User Authentication users with a Microsoft 365 account by editing a CSV file.

1 Start the Remote UI. ▶Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)

3 Click [User Management] ▶ [Authentication Management] ▶ [Settings for Universal Print].

4 Click [Start Exporting].

- If there is no user information that is associated with a Microsoft 365 account, you cannot configure the settings using a CSV file. Click [Add Association...], add the associated user and then click [Start Exporting].

5 Editing the exported CSV file

- Enter a registered user name in "mcp_uid".
- In "azureaccount_name", enter the email address or phone number used in the Microsoft 365 account.

6 Click [Import] and specify the file edited in step 5.

7 Click [Start Importing].

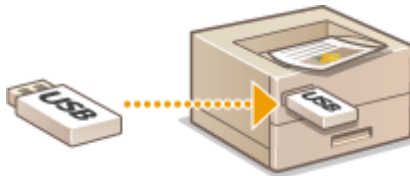
Using Memory Media Such as USB Memory

Using Memory Media Such as USB Memory	201
Using Memory Media	202

Using Memory Media Such as USB Memory

E9SJ-049

You can also use the data on a computer not connected to the network via memory media compliant with the USB standard. Preparations are required for using memory media. ▶ **Using Memory Media(P. 202)**



Using Memory Media

E9SJ-04A

You can directly insert memory media to the machine and use it.
Memory media compliant with the USB 2.0 standard is supported. FAT32/exFAT format memory media is supported.
The following devices and usage methods are not supported.

- Memory media with security functions
- Memory card readers connected via USB
- USB extension cables or USB hubs

▶ **Preparing to Use Memory Media(P. 202)**

▶ **Inserting/Removing Memory Media(P. 202)**

▶ **Printing Files on Memory Media(P. 203)**

Preparing to Use Memory Media

When using memory media, perform the following preparations in advance.

■ Enabling Memory Media for Printing



<Set> ▶ <Function Settings> ▶ <Access Files> ▶ <Memory Media Settings> ▶ <Use Print Function>
▶ <On>

If memory media is not recognized although it is connected correctly, set <Use MEAP Driver for USB Storage Device> to <Off>. ▶ **<Use MEAP Driver for USB Storage Device>(P. 465)**

NOTE

Displaying the print settings screen when memory media is inserted

- Set <Select Option When Connecting Mem. Media> to <On>. When memory media is inserted, a confirmation screen is displayed and printing can be immediately executed. ▶ **<Select Option When Connecting Mem. Media>(P. 483)**

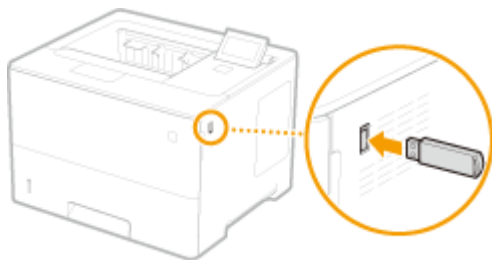
*To display the print settings screen from memory media, insert the memory media after canceling the Sleep mode. ▶ **Exiting Sleep Mode(P. 165)**

Inserting/Removing Memory Media

Inserting memory media incorrectly or in the wrong direction may cause problems with the machine or the memory media.

■ Inserting Memory Media

Insert the USB memory into the USB port on the right side of the machine with the correct orientation.



■ Removing Memory Media

Perform one of the following operations to remove the media.

- Select <Remove Memory Media> on the memory media print screen ► <Yes> for <Remove memory media?>.
- Select  (Status Monitor) ► <Device Status> ► <Remove Memory Media>.

Printing Files on Memory Media

1 Insert the memory media into the USB port of the machine.  **Inserting/Removing Memory Media(P. 202)**

2 Select <Memory Media> on the <Home> screen.  **<Home> Screen(P. 150)**

3 Select <Select File and Print>.

- Select <Select All> to select all the files.
 - If there are multiple file types, select <PDF>, <XPS>, or <JPEG/TIFF>.
- You can deselect a file by selecting the file again. To deselect all files, select <Clear Selection>.

4 Select <Apply>.

When using a print ticket to print an XPS file

When printing a file in the XPS file format, you can print according to the print ticket (print settings) embedded in the file.

1 Select <On> for <Use Print Ticket>.

2 Select <Start Printing>.

 Printing starts. Remove the memory media when printing is complete.  **Inserting/Removing Memory Media(P. 202)**

5 Specify the print settings as necessary.

Select the item to set.

<Number of Copies>

Specify the number of copies. Enter a quantity using numeric keys, and press .

<Paper>

Select the paper source that contains the paper to use for printing.

NOTE:

- The  icon indicates the multi-purpose tray.
- The number icon indicates the paper drawer position.
- For information on paper sources, see **Parts and Their Functions(P. 18)** and **Optional Equipment(P. 86)** .

<N on 1>

- <N on 1> cannot be used for JPEG files or TIFF files.

Prints data for multiple pages of image data on the same side of a sheet of paper. You can specify the number of pages to print on one side of a sheet of paper. For example, to print four pages on one side of a sheet of paper, select <4 on 1>.

<2-Sided>

You can make 2-sided printouts. Select the binding position.

<Book Type>

Prints on both sides of paper in such a way that the printed pages are opened horizontally when bound.

**<Calendar Type>**

Prints on both sides of paper in such a way that the printed pages are opened vertically when bound.

**NOTE:**

- <2-Sided> may not be available with some sizes or types of paper. **Available Paper(P. 91)**

<Resolution>

Set <1200 dpi> to print more clearly.

<Print Range>

When printing a file with two pages or more, specify the pages to print.

<Print Range (TIFF)>

- <Print Range (TIFF)> cannot be used for PDF files, XPS files, or JPEG files.

When printing a file with two pages or more, specify the pages to print.

<Fit Paper Size>

- <Fit Paper Size> cannot be used for JPEG files or TIFF files.

Set this mode to automatically enlarge/reduce when printing PDF/XPS files.

<Enlarge/Reduce>

- <Enlarge/Reduce> cannot be used for PDF files or XPS files.

Set this mode to automatically enlarge/reduce the image size according to the paper size when printing image files.

<Enlarge Print Area>

Set this mode to narrow the blank borders at each side of the page and enlarge the print area.

<Collate>

- <Collate> cannot be used for JPEG files or TIFF files.

Set this mode to sort when printing PDF/XPS files.

<Image Orientation>

- <Image Orientation> cannot be used for PDF files or XPS files.

Set this mode to automatically detect the aspect ratio of the image file and print it vertically or horizontally as required. You can also manually specify to print vertically or horizontally.

<Print Position>

- <Print Position> cannot be used for PDF files or XPS files.

You can set the print area to the center or the top left when printing an image file.

<Halftones>

Set the printing method for reproducing halftones (the intermediate areas between the light areas and dark areas of an image) with the optimal image quality.

■ For JPEG files or TIFF files

<Resolution>

Set this mode to enable fine printing so that the outlines of text data, etc. are clearer. This mode is optimal for printing data containing a lot of text or fine lines.

<Gradation>

Prints images with fine gradation, such as digital camera images, with a smooth finish.

<Error Diffusion>

This mode is suitable for printing data with text and thin lines and the curved lines of CAD data, etc.

NOTE:

- The stability of the texture and fixed toner may be reduced when <Error Diffusion> is used.

■ For PDF files or XPS files

<Error Diffusion>

This mode is suitable for printing data with text and thin lines and the curved lines of CAD data, etc.

NOTE:

- This setting is only available when <Resolution> is set to <600 dpi>.
- The stability of the texture and fixed toner may be reduced when <Error Diffusion> is used.

<Resolution/Gradation>

Select a method used to reproduce halftones, if <Error Diffusion> is set to <Off>. This option can be specified for each image type in any one document.

6 Select <Start Printing>.

⇒ The selected file is printed.

- If you want to cancel printing, select <Cancel> ► <Yes>.

7 Correctly remove the memory media. ▶ Inserting/Removing Memory Media(P. 202)

Incorrectly removing the memory media may cause problems with the machine or the memory media.

Linking with Mobile Devices

Linking with Mobile Devices	208
Connecting with Mobile Devices	209
Connecting Directly	210
Utilizing the Machine through Applications	214
Using AirPrint	217
Printing with AirPrint	221
If AirPrint Cannot Be Used	225
Printing with Default Print Service (Android)	226

Linking with Mobile Devices

E9SJ-04C

Linking the machine with mobile devices such as smart phones and tablets enables you to easily print using applications. In addition, you can operate the machine from mobile devices via remote control to confirm printing status and change the settings of the machine.



- ▶ **Connecting with Mobile Devices(P. 209)**
- ▶ **Utilizing the Machine through Applications(P. 214)**
- ▶ **Using AirPrint(P. 217)**
- ▶ **Printing with Default Print Service (Android)(P. 226)**

IMPORTANT

- Depending on your mobile device, the machine may not operate correctly.

Connecting with Mobile Devices

E9SJ-04E

There are two methods to connect the mobile devices with the machine, "Connecting via a Wireless LAN Router" and "Direct connection." Select a connection method in accordance with the communication environment and the device you are using.

Perform communication with mobile devices from <Mobile Portal> (**▶<Home> Screen(P. 150)**). You can confirm the information of connected mobile devices, etc., from here.

■ Connecting via a Wireless LAN Router

For information on how to connect a mobile device to your wireless LAN router, see the manuals provided with the devices, or contact the manufacturer.

Connect with the machine using either a wired LAN or wireless LAN router. **▶Setting up the Network Environment(P. 106)**



NOTE

- If you connect a mobile device to the machine via a wireless LAN router, you can confirm the information of the machine on the <Device Name/IP Address> screen by selecting <Mobile Portal> (**▶<Home> Screen(P. 150)**) **▶<Display Device Name/IP Address>**.
- If <Use Direct Connection> is set to <On>, you can confirm the information of the machine on the <Device Name/IP Address> screen by selecting <Mobile Portal> (**▶<Home> Screen(P. 150)**) **▶LAN Connection▶<Display Device Name/IP Address>**.

■ Connecting Directly

Directly connect a mobile device to the machine wirelessly without using wireless LAN. It is possible to immediately connect to the machine wirelessly even outside of a wireless LAN environment. **▶Connecting Directly(P. 210)**



Connecting Directly

E9SJ-04F

Even in an environment without a wireless LAN router, you can still directly connect your mobile device to the machine via "Access Point Mode" or "Wi-Fi Direct," which enable connections between the device and the machine without the need to configure complicated settings.



- ▶ **Preparing to Connect Directly(P. 210)**
- ▶ **Checking the Network Connection Type of the Machine(P. 211)**
- ▶ **Connecting Directly (Access Point Mode)(P. 211)**
- ▶ **Connecting Directly (Wi-Fi Direct)(P. 212)**

Preparing to Connect Directly

Establish a connection by using Access Point Mode in the following order.



Check the network settings of the machine.

- Select <Set> ▶ <Preferences> ▶ <Network> ▶ <TCP/IP Settings> ▶ <IPv4 Settings> ▶ set <Use IPv4> to <On>.



Prepare the mobile device.

- Configure the mobile device to enable Wi-Fi connection.



Prepare the machine for connection.

- Select <Set> ▶ <Preferences> ▶ <Network> ▶ <Direct Connection Settings> ▶ set <Use Direct Connection> to <On>.
- Select <Set> ▶ <Preferences> ▶ <Network> ▶ <Direct Connection Settings> ▶ select the type of direct connection to use in <Direct Connection Type>.
- Press <Mobile Portal> (▶<Home> Screen(P. 150)) ▶ <Direct Connection> ▶ <Connect>.
- When the connection type is set to a wireless LAN (including a sub line), a direct connection cannot be established. Change <Main Line> and <Sub Line> to a setting other than <Wireless LAN>. ▶<Select Interface>(P. 460)

NOTE

- For details on using Canon PRINT, see the related manuals. (<https://global.canon/gomp/>)
- If the message <Cannot be used with current settings. Contact the system manager.> is displayed on the top of the control panel and <Connect> cannot be selected, confirm that <Use Direct Connection> is set to <On>. If <Use Direct Connection> is set to <On> but <Connect> cannot be pressed, change the IP address in <Direct Connection IP Address Settings>. ▶<Use Direct Connection>(P. 461) ▶<Direct Connection IP Address Settings>(P. 462)
- When using the Access Point Mode, if the machine is started with <Keep Enabled If SSID/Net. Key Specified> set to <On>, direct connections are possible without selecting <Mobile Portal> ▶<Connect>. ▶<Keep Enabled If SSID/Net. Key Specified>(P. 462)

Checking the Network Connection Type of the Machine

If the machine is not connected to a network (wired or wireless LAN), use the control panel to check that the network connection mode is set to wired LAN (including a sub line).

If the machine is connected to a network, you do not have to check this.

Administrator or NetworkAdmin privileges are required to check the network connection type settings.

1 <Set> ▶ <Preferences> ▶ <Network> ▶ <Select Interface>

2 Check that <Main Line> is set to <Wired LAN>, and check that <Sub Line> is set to <Off> or <Wired LAN>.

- If the connection type is set to wired LAN, you can establish a direct connection even if the machine is not connected to a network. ▶<Selecting the Network Connection Method>(P. 108)

When <Main Line> or <Sub Line> Is Set to <Wireless LAN>

When Using Access Point Mode

When the machine is not connected to a wireless LAN, a direct connection cannot be established. Change <Main Line> and <Sub Line> to a setting other than <Wireless LAN>, or connect the machine to a wireless LAN. ▶

Connecting to a Wireless LAN(P. 112)

When Using Wi-Fi Direct

When the connection type is set to a wireless LAN (including a sub line), a direct connection cannot be established. Change <Main Line> and <Sub Line> to a setting other than <Wireless LAN>.

Connecting Directly (Access Point Mode)

IMPORTANT

- It may take some time for connection between the machine and the mobile device to be established.

■ Connecting Manually

1 Select <Mobile Portal> on the <Home> screen. ▶<Home> Screen(P. 150)

- If there is a mobile device already connected, proceed to step 3.

2 Select <Connect>.

3 Configure the connection settings on your mobile device using the SSID and network key information shown on the screen of the machine.

4 After completing the desired operations, select Disconnect.

Connecting Directly (Wi-Fi Direct)

■ Connecting to the Machine from a Mobile Device

1 Start a direct connection on the mobile device.

- Open the Wi-Fi Direct screen from the Wi-Fi settings screen of the mobile device, and tap the machine from the list of Wi-Fi Direct devices that have been detected.
 - ⇒ A message indicating that a connection request has been received from the mobile device is displayed on the screen of the machine.

2 Select <Yes> on the screen of the machine.

- ⇒ A connection between the machine and the mobile device is started.

3 After completing the desired operations, select Disconnect.

■ Connecting to a Mobile Device from the Machine

1 Select the name of the device to directly connect to from the list displayed on the screen, and select Connect.

- ⇒ A screen for selecting whether to allow a connection to the mobile device is displayed.

2 Tap [Yes] on the screen of the mobile device.

- ⇒ A connection between the machine and the mobile device is started.

3 After completing the desired operations, select Disconnect.

TIPS

- To check the connected mobile devices, select <Connection Information> on the <Direct Connection> screen.

IMPORTANT

- While connecting via direct connection, you may not be able to connect to the Internet depending on the mobile device you are using.
- The connection standby status ends if a wireless connection is not performed from the mobile device within five minutes of the device name being displayed.
- If the status without data transmission between a mobile device and the machine continues during communication by direct connection, the communication may end.
- Power saving performance of sleep mode degrades while connecting via direct connection.
- If the machine is used with a wireless LAN, you need to keep the machine connected to the wireless LAN when using direct connection. When the machine is not connected to a wireless LAN or the connection process is not complete yet, the direct connection process cannot begin. If the connection between the machine and the wireless LAN is lost during communication through direct connection, the communication may end.
- When you finish the desired operation, be sure to terminate the connection between the machine and the mobile device. If they remain connected, power saving performance of sleep mode degrades.
- If you use the direct connection, do not set the IP address manually on the mobile device. Doing so may prevent proper communication after using the direct connection.

Utilizing the Machine through Applications

E9SJ-04H

Print by using applications from a mobile device connected to the machine. Various applications including those exclusive to Canon are supported. Use properly in accordance with your device, the application, and the situation.

■ Canon PRINT

An application for printing, etc. from mobile devices that support iOS/Android. No operations on the machine are necessary to perform printing. For information on supported operating systems, detailed setting methods, and operational procedures, see the Help of the application or the Canon website (<https://global.canon/gomp/>).

IMPORTANT

- Canon PRINT can be downloaded free of charge, but the customer is responsible for any fees regarding internet connection.

■ Printing with Canon Print

You can easily print from the menu of applications that support the Android print subsystem. For more information on supported operating systems and detailed settings and procedures, see the Canon website (<https://global.canon/psmp/>).

■ Printing with Mopria®

The machine also supports Mopria®. Using Mopria® enables you to print from mobile devices that support Android using common operations and settings, even if manufacturers and models differ. For example, if you are using printers supporting Mopria® made by multiple manufacturers or a printer supporting Mopria® that is located in a place you are visiting, you can print without installing an application exclusive for each manufacturer or model. For more information on supporting models or operation environments, see <http://www.mopria.org>.



Confirming Mopria® settings



Log in to the Remote UI with Administrator privileges (▶ **Starting the Remote UI(P. 329)**)
 ▶ [Settings/Registration] ▶ [Network Settings] ▶ [Mopria Settings] ▶ select the [Use Mopria] check box ▶ [OK]

■ Printing with IPP Everywhere

This machine also supports IPP Everywhere. If your Chromebook supports IPP Everywhere, you can print directly from your Chromebook using IPP Everywhere.

Confirming IPP Everywhere



Log in to the Remote UI with Administrator privileges (▶ **Starting the Remote UI(P. 329)**)
 ▶ [Settings/Registration] ▶ [Network Settings] ▶ [IPP Everywhere Settings] ▶ select the [Use IPP Everywhere] check box ▶ [OK]

! IMPORTANT

- If you select [Use IPP Everywhere], the following settings in <TCP/IP Settings> are set to <On>.
 - <Use HTTP>
 - <IPP Print Settings>
 - <Use IPv4 mDNS>
 - <Use IPv6 mDNS>

■ Printing from Windows Phone (Windows 10 Mobile and Later)

You can perform printing from a Windows Phone without downloading a dedicated application or installing a driver. Make sure that the <Use WSD Print>, <Use WSD Browsing>, and <Multicast Discovery Settings> are enabled.

▶ **<WSD Settings>(P. 454)**

▶ **<Multicast Discovery Settings>(P. 455)**

■ Printing from Chrome OS

You can perform printing from Chrome OS without downloading a dedicated application or installing a driver. To print with the machine, it is necessary to enable Mopria®.

Confirming Mopria® settings



Log in to the Remote UI with Administrator privileges (▶ **Starting the Remote UI(P. 329)**)
 ▶ [Settings/Registration] ▶ [Network Settings] ▶ [Mopria Settings] ▶ select the [Use Mopria] check box ▶ [OK]

Printing

1 Before printing, make sure that the machine is turned ON and connected to a Chromebook.

- For information on checking the connection status, see ▶ **Setting up the Network Environment(P. 106)** .
- See the Chromebook Help page (<https://support.google.com/chromebook/answer/7225252>) for more information on printing.

NOTE

- You can also connect the machine to a Chromebook using a USB cable. See the Chromebook website (<https://support.google.com/chromebook/answer/7225252>) for information on the connection procedure.

IMPORTANT

- Printing from Chrome OS may not be supported, depending on your country or region.

Using AirPrint

E9SJ-04J

This section describes the settings required to use AirPrint and the procedure for printing from Apple devices.



AirPrint Settings

- ▶ **Configuring AirPrint Settings(P. 217)**
- ▶ **Displaying the Screen for AirPrint(P. 219)**

Functions of the AirPrint

- ▶ **Printing with AirPrint(P. 221)**

Troubleshooting

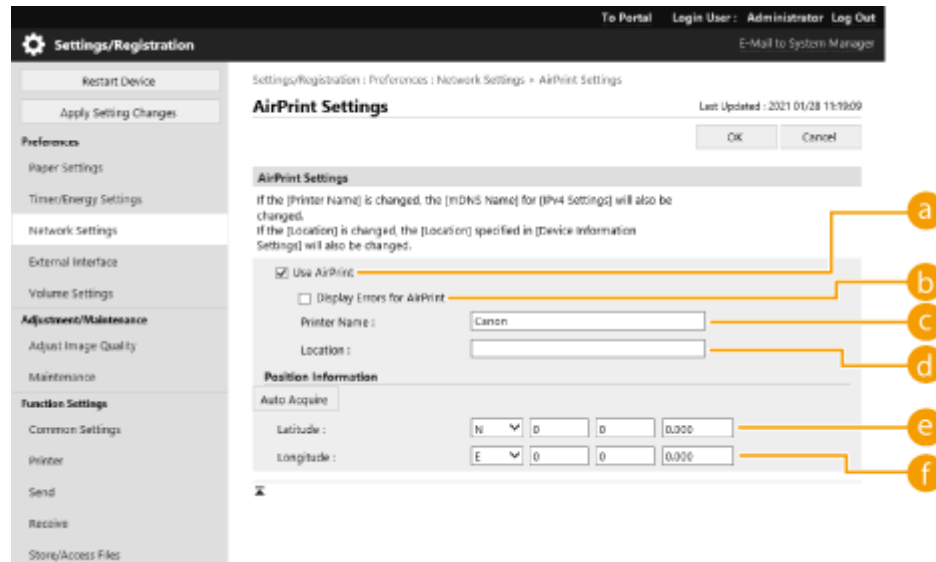
- ▶ **If AirPrint Cannot Be Used(P. 225)**

Configuring AirPrint Settings

You can register information, including the name of the machine and installation location, that is used for identifying the machine. The settings required for using AirPrint can be configured remotely using the Remote UI.

■ Configuring Settings Using the Remote UI

- 1 Start the Remote UI and log on in System Manager Mode. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration].**
 - If you are using a mobile device, such as an iPad, iPhone, or iPod touch, read "click" as "tap" in this section.
- 3 Click [Network Settings] ▶ [AirPrint Settings].**
- 4 Specify the required settings, and click [OK].**



a [Use AirPrint]

Select the check box to enable AirPrint. To disable AirPrint, clear the check box.

b [Display Errors for AirPrint]

If you are printing with AirPrint and there is an issue with the print file and the file does not print correctly, you can use this setting to choose whether error screens appear on the control panel.

c [Printer Name]

Enter the name of the machine. If an mDNS name has already been registered in [mDNS Settings] ([Network Settings] in [Preferences] (Settings/Registration)), the registered name is displayed.

d [Location]

Enter the location of the machine. If a location has already been registered in [Device Information Settings] ([Device Management] in [Management Settings] (Settings/Registration)), the registered name is displayed.

e [Latitude]

Enter the latitude of the location where the machine is installed.

f [Longitude]

Enter the longitude of the location where the machine is installed.

5 Restart the machine.

- Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

■ Configuring Settings from the Control Panel

1 Select <Set> on the <Home> screen. ▶ <Home> Screen(P. 150)

2 Select <Preferences> ▶ <Network> ▶ <Use AirPrint>.

- The Administrator PIN must be entered in order to configure this setting.

3 Select <On> .

IMPORTANT

If you select [Use AirPrint], the following settings in <TCP/IP Settings> are set to <On>.

- Use HTTP
- IPP Print Settings
- Use IPv4 mDNS
- Use IPv6 mDNS

NOTE

- If you change [Printer Name] that you have once specified, you may be unable to print any more from the Mac that has been able to be used for printing so far. This phenomenon occurs because <mDNS Name> ( **Making DNS Settings(P. 128)**) of IPv4 is also changed automatically. In this case, add the machine to the Mac again.
- When AirPrint is in-use, <Use IPv4 Name for mDNS> is fixed to <On> for the mDNS name of IPv6.
- Entering the printer name makes it easier to identify multiple printers that support AirPrint.

Displaying the Screen for AirPrint

You can display the screen for AirPrint, on which you can not only access the AirPrint Settings but also view information about consumables, such as paper and toner cartridge. Further, you can configure security function settings.

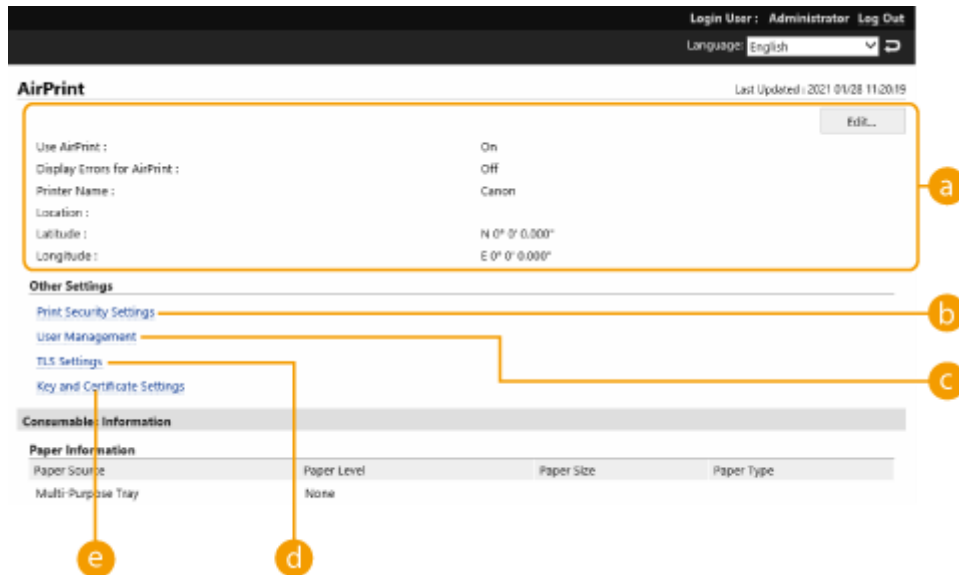
■ Displaying from a Mac

- 1 Click [System Preferences] in the Dock on the desktop ► [Printers & Scanners].
- 2 Select the machine, and click [Options & Supplies].
- 3 Click [Show Printer Webpage].
- 4 Logging in to the Remote UI

- To change the AirPrint settings, it is necessary to log in as an administrator.

■ Configuring the Screen for AirPrint

If you log in with administrator privileges, you can also change the AirPrint settings from the page for AirPrint.



a [AirPrint]

Enables you to check the values entered in the AirPrint settings, such as the name and location of the machine. You can click [Edit] to change the settings.

b [Print Security Settings]

Specify the settings required to print using TLS and authentication.

If <IPP Print Settings> is already set, the existing settings are displayed. The values registered in [Print Security Settings] change according to the values in <IPP Print Settings>.

c [User Management]

You can add/edit users to authenticate. ► **Managing Users(P. 241)**

d [TLS Settings]

Enables you to change the key and certificate used for TLS. ► **Configuring the Key and Certificate for TLS(P. 303)**

e [Key and Certificate Settings]

Enables you to generate and install a key and certificate, or request a certificate to be issued. ► **Configuring the Key and Certificate for TLS(P. 303)**

■ Checking Consumables and the Device Version

You can check information regarding the paper sources of the machine, the remaining amount of toner, and the device version.

Trademarks

Apple, Bonjour, iPad, iPhone, iPod touch, Mac, macOS, OS X, and Safari are trademarks of Apple Inc. AirPrint and the AirPrint logo are trademarks of Apple Inc.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

Printing with AirPrint

You can print from an iPad, iPhone, iPod touch, or Mac without using a printer driver.



- ▶ **Printing from an iPad, iPhone, or iPod touch(P. 221)**
- ▶ **Printing from a Mac(P. 222)**
- ▶ **Registering IPP Printing Presets(P. 223)**

System Requirements

One of the following Apple devices is required to print with AirPrint.

- iPad (all models)
- iPhone (3GS or later)
- iPod touch (3rd generation or later)
- Mac (OS X 10.7 or later)*1

*1 OS X 10.9 or later when using a USB connection

Network Environment

One of the following environments is required.

- An environment where an Apple device and the machine are connected to the same LAN
- An environment where an Apple device and the machine are connected directly
- An environment where a Mac is connected to the machine via USB

Printing from an iPad, iPhone, or iPod touch

1 Make sure that the machine is turned ON and connected to the Apple device.

- For how to make sure of this, see ▶ **Setting up the Network Environment(P. 106)** .
- For information on the Direct Connection, see ▶ **Connecting Directly(P. 210)** .

2 From the application on your Apple device, tap to display the menu options.

3 Tap [Print].

4 Select this machine from [Printer].

► The printers connected to the network are displayed here. Select this machine in this step.

! IMPORTANT

- The screen for selecting the machine in [Printer] is not displayed for applications that do not support AirPrint. In this case, printing cannot be performed.

5 Specify the print settings as necessary.

NOTE

- The available settings and paper sizes differ depending on the application you are using.
- You can recall registered print settings (presets). For information on registering print settings as presets, see [▶Registering IPP Printing Presets\(P. 223\)](#) .

6 Tap [Print].

⇒ Printing starts.

NOTE

Checking the print status

- During printing, press the Home button of the Apple device twice ▶ tap [Print].

NOTE

- You can specify whether to display an error screen on the control panel if printing cannot be performed as expected due to a problem with the print data. For details, see [▶<Display Errors for AirPrint>\(P. 459\)](#) .
- When the machine is configured not to print data sent from a computer straight away, the AirPrint data is also put on hold on the machine. In this case, you need to operate the machine to perform printing. [▶ Printing Documents that are Forced to be Held in the Machine\(P. 180\)](#)

Printing from a Mac

1 Make sure that the machine is turned ON and connected to the Mac.

- For how to make sure of this, see [▶Setting up the Network Environment\(P. 106\)](#) .

2 From your Mac, add the machine in [System Preferences] ▶ [Printers & Scanners].

3 Open a document in an application and display the print dialog box.

- How to display the print dialog box differs for each application. For more information, see the instruction manual for the application you are using.

4 Select the machine in the print dialog box.

⇒ The printers added to the Mac are displayed. Select the machine in this step.

5 Specify the print settings as necessary.

- 6 Click [Print].**

NOTE

- ## Registering IPP Printing Presets

1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the Portal page. ▶ Remote UI Screen(P. 331)

3 Click [Printer] ► [Preset Management for IPP Printing].

4 Click [Add Presets].

5 Enter the required information, and click [Add].

223

a [Preset Name]

Enter the name of the preset.

b [Enable Presets]

Select this check box to enable the registered preset.

c [Prioritize Preset Settings]

Select this check box to prioritize the settings of the registered preset.

d [Number of Copies]

Select this check box to register the number of copies to print in the preset.

e [2-Sided Printing]

Select this check box to register the two-sided printing setting in the preset. You can select [Off], [On (For Long Edge Binding)], or [On (For Short Edge Binding)].

f [Barcode Adjustment Mode]

Select this check box to register the barcode adjustment mode setting in the preset. You can select [Off] or [Mode 1] to [Mode 5].

NOTE:

- Print density will be lighter when you select stronger improvement.

g [Toner Save]

Select this check box to register the toner save setting in the preset. You can select [Off] or [On].

NOTE

- Settings not configured in the preset follow the device settings when the job is executed.

If AirPrint Cannot Be Used

E9SJ-04L

If AirPrint cannot be used, try taking the following solutions.

- Make sure that the machine is turned ON. If the machine is turned ON, first turn it OFF, then wait for at least 10 seconds and then turn it back ON to check if the problem is solved.
- Make sure that no error messages are displayed on the machine.
- Make sure that Apple devices and the machine are connected to the same LAN. If the machine is turned ON, it may take several minutes before the machine is ready for communication.
- Make sure that Bonjour on your Apple device is enabled.
- To use AirPrint with Department ID Management enabled, select [Allow Printer Jobs with Unknown IDs]. **▶Using Department IDs to Manage Printing via Computer(P. 282)**
- For printing, make sure that the paper is loaded in the machine and the machine has sufficient toner levels remaining. **▶Displaying the Screen for AirPrint(P. 219)**

Printing with Default Print Service (Android)

E9SJ-04R

If your Android terminal supports Default Print Service, you can print from the Default Print Service of your Android terminal.

To print with the machine using Default Print Service, it is necessary to enable Mopria®.

Confirming Mopria® settings



Log in to the Remote UI with Administrator privileges (▶ **Starting the Remote UI(P. 329)**)
▶ [Settings/Registration] ▶ [Network Settings] ▶ [Mopria Settings] ▶ select the [Use Mopria] check box ▶ [OK]

NOTE

- In order to use the Canon machine/printer from the Default Print Service of your Android terminal, you must first configure the following settings on your Android terminal.
 - Enable Default Print Service.
 - Disable or uninstall Mopria®.
 - Disable or uninstall Canon Print Service.

Managing the Machine

Managing the Machine	229
Applying a Security Policy to the Machine	231
Using a Password to Protect the Security Policy Settings	232
Configuring the Security Policy Settings	234
Security Policy Setting Items	236
Managing Users	241
Configuring the Personal Authentication Management Settings	243
Registering User Information in the Local Device	246
Importing/Exporting User Data	251
Adding and Editing User Information in a CSV File	254
Associating IPP Printing Information with Users	259
Registering Server Information	262
Configuring the Authentication Functions	270
Using Personal Authentication to Manage Printing via a Computer	274
Using Other Convenient Personal Authentication Management Functions	275
Setting the Department ID Management	276
Changing the System Manager ID and PIN	277
Configuring the Department ID Management Settings	279
Using Department IDs to Manage Printing via Computer	282
Setting an Authentication/Password Policy	283
Configuring the Network Security Settings	286
Restricting Communication by Using Firewalls	288
Specifying IP Addresses in Firewall Settings	289
Specifying MAC Addresses in Firewall Settings	292
Configuring the Firewall in IP Addresses of the Sub Line	295
Configuring the Firewall in MAC Addresses of the Sub Line	298
Setting a Proxy	301
Configuring the Key and Certificate for TLS	303
Generating the Key and Certificate for Network Communication	307
Configuring the IPSec Settings	310
Configuring the IEEE 802.1X Authentication Settings	317
Restricting the Machine's Functions	320
Restricting Printing from a Computer	321
Restricting the Use of Memory Media	325
Restricting Use of the Control Panel	326

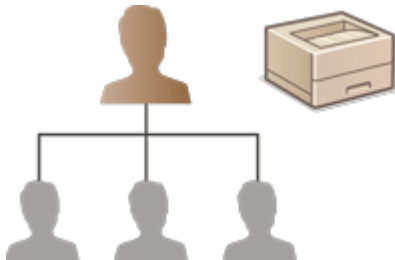
Managing the Machine from a Computer (Remote UI)	327
Starting the Remote UI	329
Checking the Status and Logs	334
Turning OFF/Restarting the Machine	336
Registering a Key and Certificate for Network Communication	337
Configuring the Expiration Check Method for Received Certificates	340
Generating a Key and Certificate Signing Request (CSR)	343
Retrieving/Updating a Certificate from an SCEP Server	346
Managing the Logs	352
Importing/Exporting the Setting Data	357
Importing/Exporting All Settings	359
Updating the Firmware	363
Updating the Firmware (Distribution)	365
Setting Scheduled Updates	368
Displaying Messages from the Administrator	370
Setting the Website for Purchasing Consumables	371
Installing System Options	373
Managing Storage Device Data	375
Initializing Settings	376
Checking the Number of Pages for Print	378
Printing Reports and Lists	379
Paper Type Management Settings	380

Managing the Machine

E9SJ-04S

To reduce the various risks associated with using this machine, such as the leakage of personal information or unauthorized use by third parties, constant and effective security measures are required. Designate an administrator to handle important machine settings, such as the user management and security settings, to ensure that the machine is used safely.

■ Configuring the Basic Management System



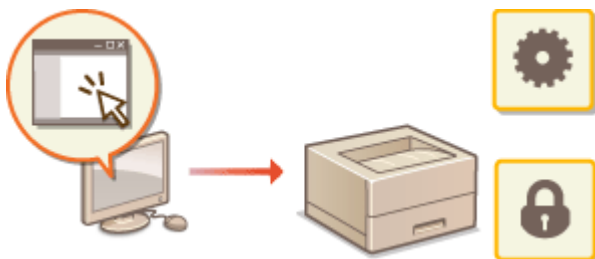
- ▶ Applying a Security Policy to the Machine(P. 231)
- ▶ Managing Users(P. 241)
- ▶ Configuring the Network Security Settings(P. 286)

■ Limiting Risks from Negligence, Operation Errors, and Misuse



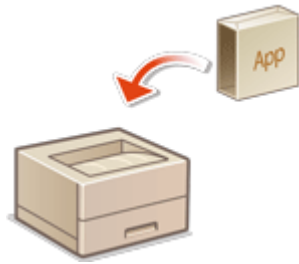
- ▶ Restricting the Machine's Functions(P. 320)

■ Ensuring Effective Management



- ▶ Managing the Machine from a Computer (Remote UI)(P. 327)

■ Managing the System Configuration and Settings



- ▶ **Installing System Options(P. 373)**
- ▶ **Initializing Settings(P. 376)**

■ Others



- ▶ **Checking the Number of Pages for Print(P. 378)**
- ▶ **Printing Reports and Lists(P. 379)**
- ▶ **Paper Type Management Settings(P. 380)**

Applying a Security Policy to the Machine

E9SJ-04U

It is a common practice for organizations to adopt a security policy that defines basic information security objectives and standards, which requires information devices such as computers and printers/multifunctional printers to be operated accordingly. On this machine, multiple settings related to security policy can be managed in batch via the Remote UI, and a dedicated password can be set up so that only the information security administrator is able to modify the settings. Before configuring these settings, make sure that the Remote UI is set up to use TLS. **▶Starting the Remote UI(P. 329)**



- ▶Using a Password to Protect the Security Policy Settings(P. 232)
- ▶Configuring the Security Policy Settings(P. 234)
- ▶Security Policy Setting Items(P. 236)

! IMPORTANT

- The purpose of the security policy settings is to manage all functions and settings related to information security, and not to actually prevent information leakage itself.

Using a Password to Protect the Security Policy Settings

E9SJ-04W

It is recommended that you use a password to protect the machine settings related to security policy. By setting a password, the privilege for modifying the security policy settings can be restricted only to the information security administrators who know the password.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [Security Settings] ▶ [Security Policy Settings].
 ➡ The [Confirm Security Policy] page is displayed.
- 4 Click [Password Settings].
- 5 Enter a password and click [OK].

- Use alphanumeric characters or symbols for the password.
- Make sure that the password is entered correctly, and enter the new password again in [Confirm:].

NOTE:

To change the password

- Enter the current password in [Current Password:] and the new password in [New Password:], then enter the new password again in [Confirm:] and click [OK].

To remove the password

- Enter the current password in [Current Password:], and click [OK] without entering any value for [New Password:] or [Confirm:] (leave them blank). If an input character limit has been configured in [Password Settings Policy], a value must be entered for this setting. Cancel the limit before removing the password.

▶ Security Policy Setting Items(P. 236)

! IMPORTANT

- Make sure that you do not forget your password. If you forget your password, contact your dealer or service representative.

NOTE

- To set/change the password, it is necessary to log in to the Remote UI with Administrator privileges.
- If a password is set, it will be required for authentication in order to initialize the machine. After authentication is performed and the machine is initialized, the password will be deleted.  **Initializing Settings(P. 376)**

Configuring the Security Policy Settings

E9SJ-04X

Machine settings related to information security can be applied and managed in batch. It is recommended that the information security administrator in charge of managing your security policy apply the security policy to the machine in accordance with the policy of your organization. To configure the security policy, log in to the Remote UI with Administrator privileges.

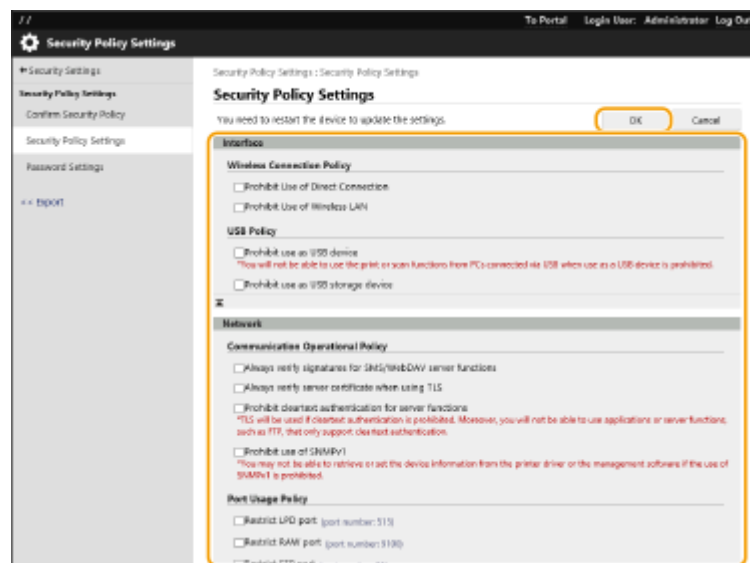
- 1 Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)
- 2 Click [Settings/Registration] on the portal page. [▶Remote UI Screen\(P. 331\)](#)
- 3 Click [Security Settings] ▶ [Security Policy Settings].
- 4 Click [Security Policy Settings].

⇒ The setting precautions are displayed. Make sure to read and understand the contents.

NOTE:

- If no password has been configured ([▶Using a Password to Protect the Security Policy Settings\(P. 232\)](#)), read the contents and click [OK] to proceed to step 6.

- 5 Enter the password and click [Log In].
- 6 Configure the necessary items and click [OK].



- For information on the settings, see [▶Security Policy Setting Items\(P. 236\)](#) .

! IMPORTANT:

- The settings related to items indicated with a check mark here cannot be changed using <Set> or the Remote UI.

- For any machine settings that were changed when the security policy settings were applied, you cannot simply clear the check box to restore the previously set value. To change the settings, use <Set> or the Remote UI.

7 Click [OK].

NOTE:

- If a security policy has been configured, a message indicating that functions and operations are restricted is displayed when the [Settings/Registration] screen is displayed on the control panel or the Remote UI.

■Applying the Security Policy Settings to Another Device

You can import and export the machine's security policy settings. By applying the same policy to multiple devices*, you can manage all of the devices in your organization using identical settings. ▶**Importing/Exporting the Setting Data(P. 357)**

* Only Canon devices that are compatible with security policy settings

NOTE

- The security policy settings can only be imported if the security policy setting password on the exporting machine matches that of the importing machine, or if no password has been set for the importing machine. If no password has been set for the importing machine, the password configured for the exporting machine is set to the importing machine.

Security Policy Setting Items

E9SJ-04Y

The setting items related to the security policy of the machine are described below. Select the check boxes for the items that you want to apply on the setting screen.

■ [Interface]

[Wireless Connection Policy]

Prevent unauthorized access by prohibiting wireless connections.

[Prohibit Use of Direct Connection]	<Use Direct Connection> and <Keep Enabled If SSID/Net. Key Specified> are set to <Off>. It is not possible to access the machine from mobile devices.	☒ Connecting Directly (P. 210) ☒ <Network> (P. 452)
[Prohibit Use of Wireless LAN]	If <Wireless LAN> is set for <Main Line> or <Sub Line> in <Select Interface>, it changes to <Wired LAN>. Wireless connections can no longer be made via a wireless LAN router or access point.	☒ <Select Interface> (P. 460)

[USB Policy]

Prevent unauthorized access and data breaches by prohibiting USB connection.

[Prohibit use as USB device]	<Use as USB Device> is set to <Off>. It is not possible to connect to a computer via USB.	☒ <Use as USB Device> (P. 465)
[Prohibit use as USB storage device]	<Use USB Storage Device> is set to <Off>. It is not possible to use USB storage devices.	☒ <Use USB Storage Device> (P. 465)

■ [Network]

[Communication Operational Policy]

Increase the security of communications by requiring the verification of signatures and certificates.

[Always verify signatures for SMB/ WebDAV server functions]	There are no setting items that the security policy is applied to for the machine.	-
[Always verify server certificate when using TLS]	The following settings are set to <On>, and a check mark is added to <CN>. • <Confirm TLS Certificate for POP RX> • <Confirm TLS Certificate Using MEAP App> During TLS communication, verification will be performed for digital certificates with common names.	☒ <Confirm TLS Certificate for POP RX> (P. 481) ☒ <Confirm TLS Certificate Using MEAP App> (P. 489)
[Prohibit cleartext authentication for server functions]	• <Use FTP Printing> in <FTP Print Settings> is set to <Off>. • <SMTP RX> in <E-mail Settings> ► <Communication Settings> ► <Allow TLS> is set to <Always Use TLS>. • [Authentication Method] in [Network Settings] ► [Dedicated Port Authentication Method] is set to [Mode 2]. When using the machine as a server, plain text authentication and functions that use plain text authentication are not available.	☒ <FTP Print Settings> (P. 454) ☒ <Communication Settings> (P. 481) ☒ <Dedicated Port Authentication Method> (P. 457)

[Prohibit use of SNMPv1]	In <SNMP Settings>, <Use SNMPv1> is set to <Off>. It is not possible to use SNMPv1 when obtaining device information from the computer.	 <SNMP Settings>(P. 457)
--------------------------	---	---

NOTE

- This setting does not apply to communication with IEEE 802.1X networks, even if the check box is selected for [Always verify server certificate when using TLS].
- If [Prohibit cleartext authentication for server functions] is selected and your device management software or driver version is old, it may not be possible to connect to the machine. Ensure that you are using the latest versions.

[Port Usage Policy]

Prevent external breaches by closing unused ports.

[Restrict LPD port (port number: 515)]	<LPD Print Settings> is set to <Off>. It is not possible to perform LPD printing.	 <LPD Print Settings>(P. 454)
[Restrict RAW port (port number: 9100)]	<RAW Print Settings> is set to <Off>. It is not possible to perform RAW printing.	 <RAW Print Settings>(P. 454)
[Restrict FTP port (port number: 21)]	In <FTP Print Settings>, <Use FTP Printing> is set to <Off>. It is not possible to perform FTP printing.	 <FTP Print Settings>(P. 454)
[Restrict WSD port (port number: 3702, 60000)]	In <WSD Settings>, <Use WSD Print> and <Use WSD Browsing> are all set to <Off>. It is not possible to use WSD functions.	 <WSD Settings>(P. 454)
[Restrict BMLinkS port (port number: 1900)]	There are no setting items that the security policy is applied to for the machine.	-
[Restrict IPP port (port number: 631)]	The <IPP Print Settings> and <Use Mopria> options are all set to <Off>. It is not possible to print using IPP or Mopria®.	 <IPP Print Settings>(P. 455)  <Use Mopria>(P. 459)
[Restrict SMB port (port number: 139, 445)]	There are no setting items that the security policy is applied to for the machine.	-
[Restrict SMTP port (port number: 25)]	[SMTP RX] in [Network Settings - E-Mail Settings]  [SMTP/POP Settings] is deselected and cannot be set. SMTP reception is not possible.	 <Configuring E-Mail Print Settings>(P. 143)
[Restrict dedicated port (port number: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547)]	[Use Dedicated Port] is deselected and cannot be set. It is not possible to use dedicated ports.	 <Dedicated Port Settings>(P. 457)
[Restrict Remote Operator's Software port (port number: 5900)]	<Remote Operation Settings> is set to <Off>. It is not possible to use remote operation functions.	 <Remote Operation Settings>(P. 490)
[Restrict SIP (IP Fax) port (port number: 5004, 5005, 5060, 5061, 49152)]	There are no setting items that the security policy is applied to for the machine.	-
[Restrict mDNS port (port number: 5353)]	The following settings are set to <Off>. • <Use IPv4 mDNS> and <Use IPv6 mDNS> in <mDNS Settings>. • <Use Mopria>	 <mDNS Settings>(P. 454)  <Use Mopria>(P. 459)

	It is not possible to search the network or perform automatic settings using mDNS. It is also not possible to print using Mopria®.	
[Restrict SLP port (port number: 427)]	In <Multicast Discovery Settings>, <Response> is set to <Off>. It is not possible to search the network or perform automatic settings using SLP.	➤<Multicast Discovery Settings>(P. 455)
[Restrict SNMP port (port number: 161)]	In <SNMP Settings>, the <Use SNMPv1> and <Use SNMPv3> options are set to <Off>. It is not possible to obtain device information from the computer or configure settings using SNMP.	➤<SNMP Settings>(P. 457)

■ [Authentication]

[Authentication Operational Policy]

Prevent unregistered users from performing unauthorized operations by implementing secure user authentication.

[Prohibit guest users to use device]	<Set Administrator PIN> is set to <On>. It becomes [Standard Authentication Mode] if [Guest Authentication Mode] is set for [Authentication Mode:] in [Remote UI Authentication]. In addition, [Guest Authentication Mode] can no longer be selected for [Authentication Mode:] in [Remote UI Authentication]. Unregistered users cannot access settings that require Administrator privileges, and print jobs from computers are canceled.	➤<Set Administrator PIN>(P. 486) ➤Configuring detailed settings for authentication functions(P. 271)
[Force setting of auto logout]	<Auto Reset Time> is enabled. The user is automatically logged out if no operations are performed for a specified period of time. Select [Time Until Logout:] on the Remote UI setting screen.	➤<Auto Reset Time>(P. 449)

[Password Operational Policy]

Impose strict limits for password operations.

[Prohibit caching of password for external servers]	[Prohibit Caching of Authentication Password for Access to External Servers] is selected and [Save authentication information for login users] is deselected. Users will always be required to enter a password when accessing an external server. The authentication information of the login user is no longer retained.	➤Setting a Password Policy(P. 284) ➤Registering Server Information(P. 262)
[Display warning when default password is in use]	[Display Warning When Default Password Is in Use] is selected. A warning message will be displayed whenever the machine's factory default password is used.	➤Setting a Password Policy(P. 284)
[Prohibit use of default password for remote access]	[Allow Use of Default Password for Remote Access] is deselected. It is not possible to use the factory default password when accessing the machine from a computer.	➤Setting a Password Policy(P. 284)

[Password Settings Policy]

Prevent third parties from easily guessing passwords by setting a minimum level of complexity and a period of validity for user authentication passwords.

Managing the Machine

[Set minimum number of characters for password]	[Set Minimum Number of Characters for Password] is selected. It is not possible to set a password with fewer characters than the number specified for [Minimum Number of Characters].	➤ Setting a Password Policy(P. 284)
[Set password validity period]	[No Expiry for Password] is deselected. [Set Password Validity Period] is selected. Specify the password expiration period in [Validity Period:].	➤ Registering User Information in the Local Device(P. 246) ➤ Setting a Password Policy(P. 284)
[Prohibit use of 3 or more identical consecutive characters]	[Prohibit Use of 3 or More Identical Consecutive Characters] is selected. It is not possible to set a password that includes the same character repeated three or more times consecutively.	➤ Setting a Password Policy(P. 284)
[Force use of at least 1 uppercase character]	[Force Use of at Least 1 Uppercase Character] is selected. Passwords are required to include at least one uppercase alphabetic character.	➤ Setting a Password Policy(P. 284)
[Force use of at least 1 lowercase character]	[Force Use of at Least 1 Lowercase Character] is selected. Passwords are required to include at least one lowercase alphabetic character.	➤ Setting a Password Policy(P. 284)
[Force use of at least 1 digit]	[Force Use of at Least 1 Digit] is selected. Passwords are required to include at least one numeric character.	➤ Setting a Password Policy(P. 284)
[Force use of at least 1 symbol]	[Force Use of at Least 1 Symbol] is selected. Passwords are required to include at least one symbol.	➤ Setting a Password Policy(P. 284)

[Lockout Policy]

Block users from logging in for a specified period of time after a certain number of consecutive invalid login attempts.

[Enable lockout]	[Enable Lockout] in [Authentication Function Settings] is selected. Specify the values for [Lockout Threshold] and [Lockout Period].	➤ Setting a Lockout Policy(P. 283)
------------------	--	---

■ [Key/Certificate]

Protect important data by preventing the use of weak encryption, or by saving encrypted user passwords and keys in a designated hardware component.

[Prohibit use of weak encryption]	[Prohibit Use of Weak Encryption] is selected. It is not possible to use weak encryption. When the check box is selected, [Prohibit use of key/certificate with weak encryption] can be selected.	➤ Setting the Security Strength and Encryption Method(P. 305)
[Prohibit use of key/certificate with weak encryption]	[Prohibit Use of Key/Certificate with Weak Encryption] in [Prohibit Use of Weak Encryption] is selected. It is not possible to use a key or certificate with weak encryption.	➤ Setting the Security Strength and Encryption Method(P. 305)
[Use TPM to store password and key]	There are no setting items that the security policy is applied to for the machine.	-

■ [Log]

You can periodically survey how the machine is used, by requiring logs to be recorded.

[Force recording of audit log]	The following settings are set to <On>. • <Display Job Log> • <Save Audit Log> • <Retrieve Network Authentication Log> • <Rtrv Log w/ Mngt Sftwr> in <Display Job Log> is set to <Allow>. Audit logs are always recorded.	▶<Display Job Log>(P. 487) ▶<Save Audit Log>(P. 487) ▶<Retrieve Network Authentication Log>(P. 487)
[Force SNTP settings]	In <SNTP Settings>, <Use SNTP> is set to <On>. Time synchronization via SNTP is required. Enter a value for [NTP Server Address] on the Remote UI setting screen.	▶<SNTP Settings>(P. 454)

■ [Job]

[Printing Policy]

Prevent information leakage from occurring when printing.

[Prohibit immediate printing of received jobs]	[Force Hold] is selected. Only [Hold as Shared Job] in [Condition Settings] can be set for [Action]. Printing does not occur immediately, even when printing operations are performed.	▶<Configuring the Forced Hold Printing Settings>(P. 321)
--	--	---

[Sending/Receiving Policy]

Limit the sending operations for destinations, and limit how received data is processed.

[Allow sending only to registered addresses]	There are no setting items that the security policy is applied to for the machine.	-
[Force confirmation of fax number]	There are no setting items that the security policy is applied to for the machine.	-
[Prohibit auto forwarding]	There are no setting items that the security policy is applied to for the machine.	-

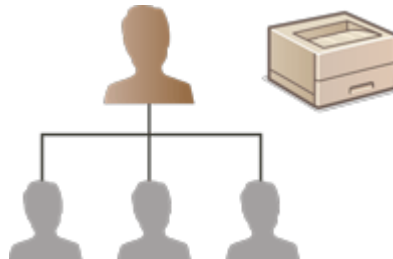
■ [Storage]

Delete unnecessary data in the memory of the machine to prevent information leaks.

[Force complete deletion of data]	There are no setting items that the security policy is applied to for the machine.	-
-----------------------------------	--	---

Managing Users

You can ensure a higher level of security and efficiency by utilizing a user authentication application (login service) to manage the users of the machine ([▶Login Service\(P. 241\)](#)). It is recommended that the administrator manage all users in accordance with your operating environment and required security measures. [▶User Management Functions\(P. 241\)](#)



[▶Configuring the Personal Authentication Management Settings\(P. 243\)](#)

[▶Using Other Convenient Personal Authentication Management Functions\(P. 275\)](#)

Login Service

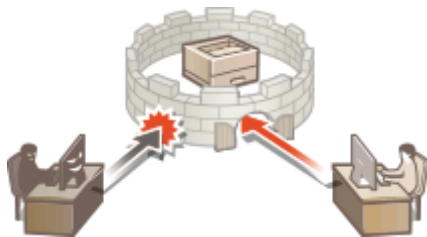
A user authentication application (login service) called "User Authentication" is used as the primary method of managing the users of the machine. With the User Authentication login service, personal authentication can be performed for users based on the user name and password registered for each user. The user information is checked either on the database inside the machine or on an external authentication server. With the ability to precisely define which functions are available to each user, you can improve security by limiting access to certain functions. It may also be possible to use Department ID Management to manage groups, depending on the device used for authentication.

User Management Functions

User management can provide the advantages described below. To protect important data and reduce costs, you can limit access to the machine and define the range of operations that are available to users.

Preventing Unauthorized Use by Third Parties

Because machine usage is limited to approved users, information leakage due to unauthorized use by third parties is prevented, even if the machine is located in a busy area that is open to outside parties.



Setting the Privilege Levels

With personal authentication management, you can define the range of available operations by specifying the role (privilege level) for each user. Roles include the "Administrator" role, with full access privileges, and the "GeneralUser" role that cannot use items that require Administrator privileges.



Setting Usage Restrictions

Personal authentication management enables a user with Administrator privileges to manage the range of operations that are available to users.



Managing Groups of Users

Users can be assigned to groups based on Department ID (Department ID Management), enabling you to check the total number of printed pages for each Department ID. You can also set specific limits for each Department ID, such as a maximum of 500 printed pages. This function can help boost cost awareness and provide hints on how to improve your operations.



NOTE

Associating User Accounts with Keychains for Smooth Operations

- When authentication information different from the authentication information used when logging in is required, the authentication information has to be entered once, but does not need to be entered again once authentication is successful. This authentication information is called a keychain. Since keychains are associated with user accounts, authentication information does not need to be entered again, even if the power of the machine is turned OFF.

Associating User Accounts with Department IDs to Restrict the Number of Prints

- User Authentication user accounts can be associated with Department IDs. By specifying print restrictions for Department IDs in advance, you can apply restrictions on the number of prints for each department that a user belongs to. For information on associating user accounts with Department IDs, see [▶Registering User Information in the Local Device\(P. 246\)](#) . For information on specifying restrictions according to department, see [▶Configuring the Department ID Management Settings\(P. 279\)](#) .

Configuring the Personal Authentication Management Settings

E9SJ-051

The User Authentication login service performs personal authentication based on the information registered for each user, enabling you to limit the users who can access the machine. User information registration (authentication) can be performed on this machine and on an external server. You can configure the authentication system to use only this machine as the authentication device, or you can additionally specify an Active Directory, Microsoft Entra ID or LDAP authentication server on the network as an authentication device to utilize the existing user information registered on the server ([▶Authentication Device\(P. 243\)](#)). For the user login method, you can enter authentication information ([▶Login Method\(P. 243\)](#)). Before configuring the user authentication settings, decide the authentication device and login method. [▶Configuring Personal Authentication Management with User Authentication\(P. 244\)](#)



- ▶[Registering User Information in the Local Device\(P. 246\)](#)
- ▶[Importing/Exporting User Data\(P. 251\)](#)
- ▶[Registering Server Information\(P. 262\)](#)
- ▶[Configuring the Authentication Functions\(P. 270\)](#)
- ▶[Using Personal Authentication to Manage Printing via a Computer\(P. 274\)](#)

Authentication Device

The authentication devices described below can be used for personal authentication management. Each type of authentication device requires a different environment and settings. Confirm your system environment before configuring. [▶System Specifications\(P. 598\)](#)

Local Device (This Machine)

User information is managed on the database inside the machine. User information is registered and edited via the Remote UI. When the local device is configured as a standalone authentication device, Department ID Management can also be performed at the same time. [▶Registering User Information in the Local Device\(P. 246\)](#)

Active Directory/Microsoft Entra ID/LDAP Server

In addition to the local devices, you can use a Windows Server with Active Directory installed, a cloud server using Microsoft Entra ID, or an LDAP server as an external authentication server. One advantage of using this type of device is that the users registered on the server can be added as general users without any changes. To provide administrator privileges to a user, the user must be assigned to a specific administrator group on the Active Directory, Microsoft Entra ID or LDAP server. To specify the additional authentication device, you must register the information of the server used for authentication. [▶Registering Server Information\(P. 262\)](#)

Login Method

The user login methods described below are available for personal authentication management.

Keyboard Authentication (Remote UI Only)

With this method, users log in by entering a user name and password. This method is available regardless of the authentication device that is used.

NOTE

- Users cannot log in from the control panel of the machine with a user name and password.

Configuring Personal Authentication Management with User Authentication

Configure the personal authentication management settings in the order described below.



Check the basic configuration.

- Is the machine properly connected to the computer? ▶ **Setting up the Network Environment(P. 106)**
- If you are using an authentication server, have the DNS settings been configured for the machine?
- If you are using an authentication server, have the date and time been properly set? ▶ **Setting the Date/Time(P. 105)**



Check the login service.

- Log in to the Remote UI with Administrator privileges, click [Settings/Registration] ▶ [User Management] ▶ [Authentication Management] ▶ [Authentication Service Information], and check that the login service is indicated as User Authentication.



Configure the authentication server settings.

- Register user information on the local device and specify the authentication server.
 - ▶ **Registering User Information in the Local Device(P. 246)**
 - ▶ **Registering Server Information(P. 262)**



4



Select the user authentication system.

- ▶ **Configuring the Authentication Functions(P. 270)**
- ▶ **Using Personal Authentication to Manage Printing via a Computer(P. 274)**

! IMPORTANT

- Make sure to log out after you finish using the Remote UI. If you close the Remote UI without logging out, it may take a long time to log in next time.

Registering User Information in the Local Device

E9SJ-052



To perform personal authentication management, you must first register user information in the database of the machine.

- ▶ Registering User Information(P. 246)
- ▶ Enabling Two-Factor Authentication(P. 249)

Registering User Information

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [User Management] ▶ [Authentication Management].**

NOTE:

Disabling "Administrator"

- A user with "Administrator" as the user name is registered by default as the user with administrator privileges. This "Administrator" user cannot be deleted but it can be disabled after adding another user with "Administrator" privileges. If the "Administrator" user is disabled, you cannot change settings that only the "Administrator" user can configure, on the control panel of the machine.

- 4 Click [Add User].**

NOTE:

To edit user information

- Click [Edit] for the user information that you want to edit, make the necessary changes, and click [Update].

To delete user information

- Select the check box for the user information that you want to delete, and click [Delete] ▶ [OK].

- 5 Enter the necessary information.**

a [User Name:] / [Password:] / [Confirm:]

Enter the user name and password. For confirmation, enter the password again in [Confirm:]. Single-byte or double-byte characters can be used for the user name.

NOTE:

- When a detailed password policy is set, enter a password that complies with the password policy. ▶ **Setting a Password Policy(P. 284)**

b [No Expiry for Password]

Select the check box to set the password of the user to register to have no expiration date. This setting can be specified when [Set password validity period] is set to [Off] in [Password Settings Policy] in [Authentication] in [Security Policy Settings].

c [Change Password at Next Login]

Select this check box to force registered users to change their passwords the first time they log in. Once a user has changed their password, the check box is cleared automatically.

d [Displayed As:]

Enter the name of the user. The display name is displayed as the user name for forced hold printing.

e [E-Mail Address:]

Enter the e-mail address that the user is using on devices such as computers.

NOTE:

- It is also possible for general users to change their own password.
- Selecting the [Allow e-mail address settings] check box enables general users to specify e-mail addresses. ▶ **Configuring the User Login Methods and Authentication Devices(P. 270)**

6 Specify other required settings.

The screenshot shows a settings window with several sections. Labels a through f point to the following elements:

- a**: Text input field for 'User Name or E-Mail Address for IPP Print'.
- b**: Text input field for 'User Name for Universal Print'.
- c**: 'Department ID' dropdown menu.
- d**: 'Select Role to Set' dropdown menu.
- e**: 'Set expiration for the user account' checkbox.
- f**: 'Disable the user account' checkbox.

a [User Name or E-Mail Address for IPP Print]

To associate IPP Printing with the user, specify the e-mail address used for IPP printing.

* You can configure the setting when the setting in [Settings/Registration] ► [Network Settings] ► [IPP Print Settings] is enabled.

* Users registered in the local device can configure the settings themselves, or an administrator can configure batch settings by using a CSV file. ► **Associating IPP Printing Information with Users(P. 259)**

b [User Name for Universal Print:]

If [Settings/Registration] ► [Network Settings] ► [Settings for Universal Print] is enabled, you can enter the email address or phone number used in the Microsoft 365 account of the user with which Universal Print jobs are associated.

c [Department ID:]

When using Department ID Management, you must click [Department ID Settings...] and select the Department ID from the list to assign to the user. First, register the necessary Department IDs in [Register New Department...] on the list screen. If the Department ID that you specify here is later deleted, make sure to change this setting. ► **Configuring the Department ID Management Settings(P. 279)**

d [Select Role to Set:]

The user privileges (roles) listed below can be selected. The available setting items vary depending on the privileges (► **Settings/Registration(P. 386)**).

[Administrator]	Allows all operations as an administrator of the machine.
[GeneralUser]	Allows general user privileges.

e [Set expiration for the user account]

When setting a period of validity for the account, select the check box and enter a value for [Expiration].

f [Disable the user account]

Select the check box to temporarily disable the account.

7 Click [Add].

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ► **Importing/Exporting the Setting Data(P. 357)**

- This setting is included in [Settings/Registration Basic Information] when batch exporting. **▶Importing/Exporting All Settings(P. 359)**

TIPS

Check for unregistered Department IDs

- If you click [Check Unregistered Department ID...] on the screen displayed in step 4, you can find out Department IDs that are not registered in the machine by checking Department IDs assigned to the users against Department IDs registered in the machine.

Batch settings for Department IDs

- If you click [Batch Settings for Department ID...] on the screen displayed in step 4, you can create new Department IDs and apply settings for all users.
- If the user name is comprised of numbers and is seven digits or fewer, the same number is assigned to the same user as the Department ID. If the password of the same user is registered as a number that is seven digits or fewer, it is also set as the PIN for that Department ID.
- If the user name and password do not meet the above conditions, a Department ID is automatically assigned starting from 0000001, and 0 (none) is set for the PIN.

Registering the Department ID as the User Name

- If you click [Add User Using Department ID...] on the screen in step 4, a new user with the same name as the Department ID is registered. When keyboard authentication is used, authentication can be performed using numeric key entry only.

Enabling Two-Factor Authentication

You can use two-factor authentication to increase the security of logging into the Remote UI by requiring a one-time password in addition to the password set in " **▶Registering User Information(P. 246)** ."

NOTE

- To obtain a one-time password, a mobile app (Microsoft Authenticator or Google Authenticator) must be installed to a mobile device such as a smartphone or tablet. The time of the mobile device must also match that of the machine.
- Two-factor authentication can only be enabled for the user account that is logged in.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [User Management] ▶ [Authentication Management].**
 - For a user with Administrator privileges, click [Edit] on the [User Management] screen.
- 4 Select [Use Two-Factor Authentication], and click [Update].**

5 Start the mobile app and use it to scan the QR code displayed on the [Enable Two-Factor Authentication] screen of the Remote UI.

NOTE:

- If you cannot scan the QR code, enter the key displayed in [Manual Entry Key:].

6 On the [One-Time Password:] screen, enter the one-time password displayed in the mobile app ► click [Verify].

! IMPORTANT

When account information has been lost or deleted

- A QR code or key can be used to register or restore the account information from any mobile device. It is recommended that you take a photo or screenshot of the QR code or key displayed on the computer screen, in case the mobile device is lost or the account information registered in the mobile app is accidentally deleted.
- Store the photo or screenshot of the QR code or key carefully so that others cannot see it.

NOTE

- If the mobile device is lost or the account information registered to the mobile app is deleted and you do not have a photo or screenshot of the QR code or key, you will be unable to obtain a one-time password and therefore unable to log in to the Remote UI. In this case, ask a user with Administrator privileges to deselect [Use Two-Factor Authentication] so that you can log into the Remote UI.

LINKS

► **Registering Server Information(P. 262)**

► **Configuring the Authentication Functions(P. 270)**

► **Using Personal Authentication to Manage Printing via a Computer(P. 274)**

Importing/Exporting User Data

E9SJ-053

You can save user information stored in the machine to a computer (export), as well as load user information from other machines into the machine you are using (import). This is useful when you want to register multiple users at once.

▶ **Exporting User Data(P. 251)**

▶ **Manually Importing User Data(P. 251)**

NOTE

- For information on editing a CSV file for importing, see ▶ **Adding and Editing User Information in a CSV File(P. 254)** .
- If duplicates of data exist in a CSV file for importing, the version of the data that was read first will be prioritized and registered.
- It is recommended that you export the registered/edited user data to make a backup copy.

Exporting User Data

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [User Management] ▶ [Authentication Management].**
- 4 Click [Export].**
- 5 Select the file format, and click [Start Export].**
 - User information created in the file format that can be used with User Authentication is exported. The file extension is "csv."
- 6 Follow the instructions on the screen to specify the location to store the file.**

⇒ The csv file is stored.

Manually Importing User Data

You can manually specify data for importing and update user information.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**

2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)

3 Click [User Management] ▶ [Authentication Management].

4 Click [Import] ▶ [Manual Import Settings...]

5 Specify the required settings.

a [File Path:]

Specify the path of the file for importing.

b [File Format:]

Select the file format for importing.

- <User Authentication Format>:

Imports user information created in the file format that can be used with User Authentication. The file extension is "csv."

c [Import Method:]

Select whether to import only updated or added user data, or all user data.

NOTE:

- If you select [Perform full import] and a user with the same user name is already registered, the user information is overwritten.
- When performing a complete import, any users not listed in the imported files are deleted from the machine. However, "-----" and "Administrator", which are registered by default, will remain even if they are not listed in the imported files.

d [Application Timing:]

Select [Apply immediately] or [Specify the date and time]. If you select [Specify the date and time], enter the desired date and time or the time only.

NOTE:

- If the user information cannot be reflected at the specified time because the machine is turned OFF or is completely in the Sleep mode, the information is reflected when the machine recovers.

6 Click [Start Import]

NOTE:

- If the Department ID (dept_id) and PIN (dept_pin) are written in the imported CSV file, [Check Unregistered Department ID] will be displayed after importing is complete. Perform Department ID registration.

Adding and Editing User Information in a CSV File

E9SJ-054

This section describes the content of each column in a CSV file used for importing or exporting. Refer to this section when editing CSV files.

However, if "No" is written in the "Change Required" section for a particular column, do not change the content of that column.

Column Name	Change Required	Valid Characters	Invalid Characters	Compatibility With Remote UI Screen	Notes
uid	Yes	1 to 32 characters	Control characters, single-byte spaces, and the following characters: \\ / : * ? < > [] ; , = + @ "		- Must be input when importing. "@" may be available depending on a setting. ▶Configuring the User Login Methods and Authentication Devices(P. 270)
password	Yes	0 to 32 characters within the ISO885915 character set	Control characters		- Output as "*****" (* x 8) when exporting. - When updating the password, "*****" will be deleted and overwritten by the new password. However, when importing changes, even if you leave the field unspecified (blank), it will not be overwritten as empty (blank), but will instead retain the existing value. - If this item is omitted when importing changes, the existing user will carry over the original password.
pin	No	-	-	-	Not used with this machine.
cn	Yes	0 to 32 characters	Control characters		N/A
cn;lang-ja;phonetic	Yes	0 to 32 characters	Control characters	See "Notes."	Displayed as "phonetic" if the display language is set to "Japanese."
mail	Yes	Combination of 0 to 256 alphanumeric characters and symbols	Control characters		N/A
avatorImgPath	No	-	-	-	Not used with this machine.
dept_id	Yes	A number up to seven digits	Non-single-byte numeric characters		N/A

Managing the Machine

Column Name	Change Required	Valid Characters	Invalid Characters	Compatibility With Remote UI Screen	Notes
dept_pin	Yes	A number up to seven digits	Non-single-byte numeric characters		N/A
roleName	Yes	0 to 32 characters	Control characters, single-byte spaces, and the following characters: \\ : * ? < > [] ; , = + @ " &		If this item is omitted, or if a name is specified that is not registered in role management, it will be changed to the initial role setting.
accountExpires	Yes	See "Notes."	See "Notes."		YYYYMMDD format. "235959" is automatically added as the time after importing.
accountDisabled	Yes	1 or 0	Any character besides "1" (disable) or "0" (enable)		N/A
group	No	-	-	-	Not used with this machine.
createDate	Yes	See "Notes."	See "Notes."	- (N/A)	- Output in the "YYYYMMDDhhmmssmmm" format when exporting. (The "T" is added in order to prevent corruption of the text.) - When importing, input the information in one of the following formats. - YYYYMMDDhhmmssmmm - YYYYMMDDhhmmssmmm - YYYYMMDD - YYYYMMDD - If you omit this item, the date and time of importing is used for the date and time of registration for new users. For existing users, the original registration date and time are carried over.
lastLoginDate	Yes	See "Notes."	See "Notes."	- (N/A)	- The date and time that the user last logged in are stored. - Output in the "YYYYMMDDhhmmssmmm" format when exporting. (The "T" is added in order to prevent corruption of the text.)

Column Name	Change Required	Valid Characters	Invalid Characters	Compatibility With Remote UI Screen	Notes
					- When importing, input the information in one of the following formats. - YYYYMMDDhhmmssmmm - YYYYMMDDhhmmssmmm - YYYYMMDD - YYYYMMDD - Used for determining whether a user has logged in and whether to perform automatic user deletion. - If you omit this item, the date and time that the user last logged in are blank for new users. For existing users, date and time that the user last logged in are carried over.
dc	No	0 to 32 characters	Control characters	- (N/A)	Cannot be changed. It will be automatically assigned for the following users. Users registered following server authentication
uuid	No	-	-	-	Cannot be changed. Automatically assigned during user registration.
sdl_digest	No	-	-	-	Cannot be changed. Automatically generated when registering/changing password.
uac_advbox_digest1	No	-	-	-	Cannot be changed. Automatically generated when registering/changing password.
uac_advbox_digest2	No	-	-	-	Cannot be changed. Automatically generated when registering/changing password.
pin_digest	No	-	-	-	Cannot be changed. Automatically generated when registering/changing PIN.
server_user_flg	No	-	-	-	Cannot be changed. This is an identification flag for the user registered after completing server authentication.
server_user_gp_key	No	-	-	-	Cannot be changed. This is the group to which the user who is registered after completing server authentication belongs.
server_user_gp_value	No	-	-	-	Cannot be changed. This is the group to which the user who is registered after completing server authentication belongs.

Column Name	Change Required	Valid Characters	Invalid Characters	Compatibility With Remote UI Screen	Notes
non_expire_password	Yes	1 or 0	Any character besides "1" (enable) or "0" (disable)	j	If this item is not entered, "0" (disabled) is reflected.
next_password_change_required	Yes	1 or 0	Any character besides "1" (enable) or "0" (disable)	k	If this item is not entered, "0" (disabled) is reflected.
CharSet	-	-	-	-	For UTF8, "CharSet:UTF8" will be written in the column line.

NOTE

- The line at the beginning of the file is the column line.
- Items names may not appear in sequence.
- The encodings supported by CSV files are UTF-8, SJIS, BIG5, GB2312, and Korean.
- Text strings in exported CSV files are surrounded by "[" and "]" if any of the following conditions apply. When editing a CSV file and adding new text strings that meet the following conditions, surround any such text strings with "[" and "]".
 - Numbers starting with "0"
 - Numbers greater than 12 digits

- Text strings surrounded by "[" and "]"

Associating IPP Printing Information with Users

E9SJ-055

You can associate users registered to the local device with user information that uses IPP printing and manage that user information.

* You can still operate IPP printing without configuring these settings.

▶ **Configuring the User Information (User)**(P. 259)

▶ **Configuring the User Information (Administrator)**(P. 259)

▶ **Configuring Batch Settings Using a CSV File (Administrator)**(P. 260)

Configuring the User Information (User)

Configure this setting using Remote UI from a computer. You cannot use the control panel to configure the setting.

- 1 Log in to Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 On the Portal page of Remote UI, click [Settings/Registration]. ▶ Remote UI Screen(P. 331)**
- 3 Click [User Management] ▶ [Authentication Management].**
 ➡ The [Change User Information] screen is displayed.
- 4 Configure the user information in [IPP Print Information].**
 - Enter a user name or e-mail address used for IPP printing in [User Name or E-Mail Address for IPP Print].
- 5 Click [Update].**
 ➡ The settings are applied.
- 6 Log out from Remote UI.**

Configuring the User Information (Administrator)

Configure this setting using Remote UI from a computer. You cannot use the control panel to configure the setting. Administrator privileges are required.

- 1 Log in to Remote UI as an administrator. ▶ Starting the Remote UI(P. 329)**
- 2 On the Portal page of Remote UI, click [Settings/Registration]. ▶ Remote UI Screen(P. 331)**

3 Click [User Management] ► [Authentication Management].

► The [User Management] screen is displayed.

4 Click [Edit] for the user whose information you want to configure.

► The [Edit User Information] screen is displayed.

- If the user is not registered, click [Add User] instead of [Edit], and specify [IPP Print Information] when registering the new user information. ► **Registering User Information in the Local Device(P. 246)**

5 Specify the user information in [IPP Print Information].

- Enter a user name or e-mail address used for IPP printing in [User Name or E-Mail Address for IPP Print].

6 Click [Update].

► The settings are applied.

7 Log out from Remote UI.

Configuring Batch Settings Using a CSV File (Administrator)

You can edit a CSV file to associate users registered to the local device with user information that uses IPP printing.

Configure this setting using Remote UI from a computer. You cannot use the control panel to configure the setting. Administrator privileges are required.

1 Log in to Remote UI as an administrator. ► **Starting the Remote UI(P. 329)**

2 On the Portal page of Remote UI, click [Settings/Registration]. ► **Remote UI Screen(P. 331)**

3 Click [User Management] ► [Authentication Management] ► [IPP Print Settings].

► The [IPP Print Settings] screen is displayed.

4 Click [Start Export] and save the CSV file to the computer.

- If no user information associated with IPP printing has been registered, click [Add Association] to add a user associated with IPP printing, and then click [Start Export].

5 Edit the exported CSV file.

- Enter the name of the user registered to the local device in "uid."
- Enter a user name or e-mail address used for IPP printing in "ipp_user_name."

6 Click [Import].

⇒ The [Import Associations] screen is displayed.

7 In [File Path], click [Choose File] to specify the edited CSV file.

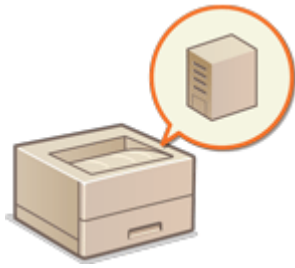
8 Click [Start Import].

⇒ The file is imported.

9 After the import is completed, log out from Remote UI.

Registering Server Information

E9SJ-056



To specify an Active Directory, Microsoft Entra ID or LDAP server as an additional authentication device, you must register the information of the server used for authentication. Conduct a connection test as necessary.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [User Management] ▶ [Authentication Management].
- 4 Click [Server Settings] ▶ [Edit...].
- 5 Set the authentication server and domain information.

a [Use Active Directory]

Select the check box when using Active Directory.

b [Set Domain List:]

Select whether the Active Directory information of the login destination is retrieved automatically or entered manually. To enter it manually, select [Set Manually] and add the domain of the login destination in [Active Directory Management...].

c [Use access mode within sites]

Select the check box if there are multiple Active Directory servers and you want to assign access priority to the Active Directory located in the same site as the machine. Change the settings for [Timing of Site Information Retrieval:] and [Site Access Range:] as necessary.

! IMPORTANT:

- Even when [Only site to which device belongs] in [Site Access Range:] is set, the machine may access sites outside the site it belongs to when performing domain controller access during the startup process. However, access to domain controllers in the same site as the machine is prioritized. As an exception, if domain controllers in the same site cannot be accessed but domain controllers outside the site can be accessed, priority is given to accessing domain controllers outside the site.

d [Number of Caches for Service Ticket:]

Specify the number of service tickets that the machine can hold. A service ticket is an Active Directory function that acts as a record of a previous login, which reduces the amount of time it takes for the same user to log in next time.

e [Use LDAP server]

Select the check box when using an LDAP server.

f [Use Microsoft Entra ID]

Select the check box when using Microsoft Entra ID.

g [Period Until Timeout]

Specify the time limit for attempting to connect to the authentication server and the time limit for waiting for a response. When [Save authentication information for login users] is enabled, if you cannot log in within the time limit specified here, login is attempted using the authentication information saved in the cache.

h [Default Domain of Login Destination:]

Specify the domain that has connection priority.

■ Manually specifying the Active Directory domain

- 1 Select the check box for [Use Active Directory] and select [Set Manually] for [Set Domain List:].
- 2 Click [Active Directory Management...] ► [OK].
- 3 Click [Add Domain...].
- 4 Enter the necessary information.

The screenshot shows the 'Add Domain' form in the Authentication Management interface. The form is titled 'Add Domain' and has buttons for 'Test Connection', 'Add', and 'Cancel'. The fields are as follows:

- a** Domain Name: [Text input field]
- b** NetBIOS Name: [Text input field] (Maximum 15 Characters)
- c** Primary Host Name or IP Address: [Text input field] (Maximum 64 Characters)
- c** Secondary Host Name or IP Address: [Text input field] (Maximum 64 Characters)
- d** User Name: [Text input field] (Maximum 20 Characters)
- d** Password: [Text input field]
- e** Starting Point for Search: [Text input field]
- f** Attributes to Set for Login Account:
 - Login Name: [Text input field] (Maximum 64 Characters)
 - Displayed As: [Text input field] (Maximum 64 Characters)
 - E-Mail Address: [Text input field] (Maximum 254 Characters)

a [Domain Name:]

Enter the domain name of the Active Directory that is the login destination (**Example:** company.domain.com).

b [NetBIOS Name]

Enter the NetBIOS domain name (**Example:** company).

c [Primary Host Name or IP Address:] / [Secondary Host Name or IP Address:]

Enter the host name of the Active Directory server or the IPv4 address. When using a secondary server, specify the name in [Secondary Host Name or IP Address:].

- Example:**

Using a host name: ad-server1

Using an IPv4 address: 192.168.18.138

d [User Name:] / [Password:]

Enter the user name and password to use for accessing and searching the Active Directory server.

e [Starting Point for Search:]

Specify the location to access and search in the Active Directory Server.

f [Login Name:] / [Displayed As] / [E-Mail Address:]

Specify the data fields (attribute names) for the login name, display name, and e-mail address of each user account on the Active Directory server (**Example:** sAMAccountName, cn, mail).

- Click [Test Connection] to confirm that connection is possible, and then click [Add].

NOTE:

To edit server information

- Click [Edit] for the server information that you want to edit, make the necessary changes, and click [Update].

■Registering LDAP server information

- Select the check box for [Use LDAP server] and click [LDAP Server Management...] ► [OK].

2 Click [Add Server...].

3 Enter the LDAP server information.

The screenshot shows the 'Add LDAP Server' form in the Authentication Management interface. The form is titled 'Add LDAP Server' and includes the following fields, each labeled with a letter in a yellow circle:

- a** Server Name: (Maximum 28 Characters)
- b** Primary Address: (Maximum 48 Characters)
- c** Port: (336) (1-65535)
- d** Secondary Address: (Maximum 48 Characters)
- e** Port: (336) (1-65535)
- f** Comments: (Maximum 64 Characters)
- g** Use TLS: (checked)
- h** Use authentication information: (checked)
- g** User Name: (Maximum 128 Characters)
- g** Password: (Maximum 28 Characters)
- h** Starting Point for Search: (Maximum 128 Characters)

a [Server Name]

Enter the name for the LDAP server. The name "localhost" cannot be used. The server name may not include spaces.

b [Primary Address]

Enter the IP address or host name of the LDAP server (**Example:** ldap.example.com). The loopback address (127.0.0.1) cannot be used.

c [Port:]

Enter the port number used for communicating with the LDAP server. Use the same setting that is configured on the server. If you do not enter a number, it is automatically set to "636" when the check box is selected for [Use TLS], or it is set to "389" when the check box is cleared.

d [Secondary Address:] / [Port:]

When using a secondary server in your environment, enter the IP address and the port number.

e [Comments]

Enter a description or note as necessary.

f [Use TLS]

Select the check box when using TLS encryption for communications with the LDAP server.

g [Use authentication information]

Clear the check box to allow anonymous access to the LDAP server, only if the LDAP server is set to allow anonymous access. When using the user name and password for authentication, select the check box and enter values for [User Name:] and [Password:].

NOTE:

- If this check box is selected, when you want to change the settings in [Primary Address] or [Secondary Address:] of an LDAP server, entering the password specified in [Password:] in [Use authentication information] is required.

h [Starting Point for Search:]

Specify the location (level) to search for user information when LDAP server authentication is performed.

4 Specify how to set the attribute names and domain name.

a [User Name (Keyboard Authentication):]

Specify the LDAP data field (attribute name) for the user name on the LDAP server (**Example:** uid).

b [Login Name:] / [Display Name:] / [E-Mail Address:]

Specify the LDAP data fields (attribute names) for the login name, display name, and e-mail address of each user account on the LDAP server (**Example:** uid, cn, mail).

c [Specify the domain name] / [Specify the attribute name for domain name acquisition]

Select how to set the domain name of the login destination. To specify the domain name directly, select [Specify the domain name] and enter the domain name. To specify an LDAP data field (attribute name) from which to acquire the domain name on the LDAP server, select [Specify the attribute name for domain name acquisition] and enter the attribute name (**Example:** dc).

- 5 Click [Test Connection] to confirm that connection is possible, and then click [Add].

NOTE:

To edit server information

- Click [Edit] for the server information that you want to edit, make the necessary changes, and click [Update].

■ Specifying the domain of Microsoft Entra ID

NOTE:

If you want to specify Microsoft Entra ID as an authentication server, you need to register a user on the Microsoft 365 Service and use the Microsoft Entra ID Service. ➤ **Registering Application on Microsoft Entra ID(P. 595)**

- 1 Select the check box for [Use Microsoft Entra ID] and click [Domain Settings] ► [OK].
- 2 Enter the necessary information.

The screenshot shows the 'Microsoft Entra ID Domain Settings' page in the Authentication Management console. The page is divided into several sections, each with a corresponding lettered callout (a-i) pointing to its input field:

- a** [Login Destination Name:] Input field for the login destination name.
- b** [Domain Name:] Input field for the domain name.
- c** [Application ID:] Input field for the application ID.
- d** [Secret:] Input field for the secret.
- e** [Key and Certificate:] Input field for the key and certificate.
- f** [Microsoft Entra ID Authentication URL] / [Microsoft Entra ID API URL] Input fields for the authentication and API URLs.
- g** [Login Name:] / [Display Name:] / [E-Mail Address:] Input fields for the login name, display name, and email address.
- h** [Domain Name to Set for Login Account:] Input field for the domain name to set for login account.
- i** [Autocomplete for Entering User Names When Using Keyboard Authentication] Input field for the domain name to autocomplete.

a [Login Destination Name:]

Enter the display name for the login destination.

- **Default value:** Microsoft Entra ID

b [Domain Name:]

Enter the domain name of Microsoft Entra ID that is the login destination.

c [Application ID:]

Enter the application ID (client).

d [Secret:]

Enter the secret issued on Microsoft Entra ID. When you use [Key and Certificate], it is not necessary to enter here.

e [Key and Certificate]

Click [Key and Certificate] when you use a key and a certificate. By clicking [Export Certificate], you can export the certificate that is registered to Microsoft Entra ID.

f [Microsoft Entra ID Authentication URL] / [Microsoft Entra ID API URL]

Enter the URL. Depending on your cloud environment, it may be necessary to modify the URL.

Click [Restore Initial Settings] to restore the URL of [Microsoft Entra ID Authentication URL] / [Microsoft Entra ID API URL] to the default value.

- **Default value:**

[Microsoft Entra ID Authentication URL]: <https://login.microsoftonline.com>

[Microsoft Entra ID API URL]: <https://graph.microsoft.com>

g [Login Name:] / [Display Name:] / [E-Mail Address:]

Enter the data field (attribute) names to which a login name, display name, and e-mail address of each user account are registered on an Microsoft Entra ID server.

- **Default value:** WindowsLogonName, displayName, mail
- **Example:** userPrincipalName, displayName, mail

h [Domain Name:]

Under most circumstances, you do not need to change the setting.

- **Default value:** AzureAD

i [Domain Name to Autocomplete:]

Enter the domain name that is entered automatically. You do not have to enter the domain name after @ by yourself.

- 3 Click [Test Connection], confirm that the connection is established, and click [Update].

6 Enter the user information and set the privileges.

The screenshot shows a configuration window with the following sections:

- Default Domain:** A dropdown menu for 'Default Domain of Login Destinations'.
- Cache for User Information:** A checkbox for 'Save authentication information for login users' and a 'Retention Period' field set to 30 days.
- Role Association:** A dropdown for 'User Attribute to Browse' set to 'memberOf' and a checkbox for 'Retrieve role name to apply from (User Attribute to Browse)'.
- Conditions:** A table with columns: Condition, Search Criteria, Character String, and Role. The first row is pre-filled with 'Administrator', 'Exact Match', 'Canon Peripheral Admins', and 'Administrator'.

a [Save authentication information for login users]

Select the check box to save the authentication information of users who log in via the control panel. After the settings are configured, the saved authentication information can be used for login, even if the machine is unable to connect to the server. Change the [Retention Period:] setting as necessary.

b [User Attribute to Browse:]

Enter the data field (attribute name) on the referenced server that is used to determine user privileges (roles). Normally, you can use the preset value of "memberOf", which indicates the group that the user belongs to.

c [Retrieve role name to apply from [User Attribute to Browse]]

Select the check box to use the character string registered in the data field on the server specified in [User Attribute to Browse:] for the role name. Before configuring, check the role names that can be selected on the machine, and register them on the server.

d [Conditions]

You can set the conditions that determine user privileges. The conditions below are applied in the order that they are listed.

[Search Criteria]	Select the search criteria for [Character String].
-------------------	--

[Character String]	Enter the character string that is registered to the attribute specified in [User Attribute to Browse:]. To set the privileges based on the group that user belongs to, enter the group name.
[Role]	Select the privileges that apply to users who match the criteria.

NOTE:**The [Conditions] settings when using Active Directory servers**

- "Canon Peripheral Admins" is set in advance as the Administrator user group. Assign different privileges to the other groups created on the server.

7 Click [Update].**8 Restart the machine. ▶Restarting the Machine(P. 336)****NOTE****DNS Settings**

The following settings are required if the port number used for Kerberos on the Active Directory side is changed.

- Information for the Kerberos service of Active Directory must be registered as an SRV record as follows:
 - Service: "_kerberos"
 - Protocol: "_udp"
 - Port number: The port number used by the Kerberos service of the Active Directory domain (zone)
 - Host offering this service: Host name of the domain controller that is actually providing the Kerberos service of the Active Directory domain (zone)

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

LINKS

- ▶ **Registering User Information in the Local Device(P. 246)**
- ▶ **Configuring the Authentication Functions(P. 270)**
- ▶ **Using Personal Authentication to Manage Printing via a Computer(P. 274)**

Configuring the Authentication Functions

E9SJ-057

You can configure the user login methods, authentication devices, and other authentication functions based on your system environment and needs.

Configuring the User Login Methods and Authentication Devices

Specify the user login methods (▶ **Login Method(P. 243)**) and authentication devices (▶ **Authentication Device(P. 243)**). Note that the authentication devices need to be set up before configuring the settings below.

- ▶ **Registering User Information in the Local Device(P. 246)**
- ▶ **Registering Server Information(P. 262)**

1 Start the Remote UI. ▶ **Starting the Remote UI(P. 329)**

2 Click [Settings/Registration] on the portal page. ▶ **Remote UI Screen(P. 331)**

3 Click [User Management] ▶ [Authentication Management].

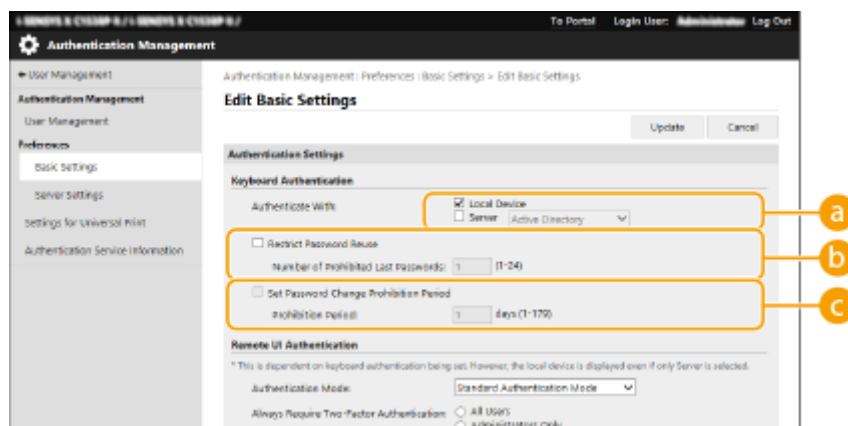
4 Click [Basic Settings] ▶ [Edit...].

5 Specify the required settings.

- Select the login methods that you want to use, and specify detailed settings such as authentication device settings.

■ Using keyboard authentication

Configure the settings below when using keyboard authentication.



a [Authenticate With:]

Select the user authentication device.

- Select the check box for [Local Device] if you are using the database inside this machine to manage user information.
- When using an external authentication server, select [Server] and specify the type of server.

b [Restrict Password Reuse]

Select this check box to prohibit the re-use of a password that has already been used. The password history count should also be configured to match this setting.

c [Set Password Change Prohibition Period]

Select this check box to specify the period for which password changes are prohibited. Specify the expiry period also.

■ Configuring detailed settings for authentication functions

You can configure detailed settings for the personal authentication functions.

The screenshot shows the 'Remote UI Authentication' settings page. The settings are organized into sections: 'Authentication Mode', 'Always Require Two-Factor Authentication', 'Other Authentication', 'User Recognition Settings', 'Department ID Settings for Users', 'Set Default Role', 'Setting Changes by Users Without Administrator Privileges', 'Device Settings', 'Auto Delete Users', and 'Communication Mode for Kerberos Authentication Settings'. Callouts a through l point to specific settings: a points to 'Authentication Mode' (set to 'Standard Authentication Mode'), b points to 'Always Require Two-Factor Authentication' (set to 'OFF'), c points to 'Web Service Authentication Method' (set to 'Use OAuth2/OIDC/MEDS'), d points to 'Match Case for User Name' (unchecked), e points to 'Allow Use of @ in User Name' (unchecked), f points to 'Automatically set the department ID at user registration' (unchecked), g points to 'Automatically Delete Department ID at User Deletion' (unchecked), h points to 'Default Role When Registering User' (set to 'General User'), i points to 'Allow e-mail address settings' (unchecked), j points to 'Functions to Restrict' (set to 'Permit job without user authentication'), k points to 'Auto Delete Users' (set to 'Delete users that have not logged in for the specified period'), and l points to 'Communication Mode for Kerberos Authentication Settings' (set to 'Use UDP').

a [Authentication Mode:]

Select the authentication mode to use for Remote UI login. When [Guest Authentication Mode] is selected, unregistered users can also log in by clicking [Log In (Guest)]. Select [Administrator Authentication Mode] to only allow users with Administrator privileges to log in.

b [Always Require Two-Factor Authentication:]

You can compel users logging in to the Remote UI to use two-factor authentication. Select [All Users] or [Administrators Only] as the users to which this applies.

c [Web Service Authentication Method:]

Select the local device authentication method to use for communications with Web service applications.

d [Match Case for User Name]

If this function is set, you can set whether user names are case-sensitive.

NOTE:

- It is recommended that this is set together with [Function Settings] ► [Printer] ► [Print] ► [Match Case for User Name].

e [Allow Use of @ in User Name]

Select whether to allow "@" to be used in user names.

f [Automatically set the department ID at user registration]

Select the check box to automatically allocate a Department ID when you register/edit a user via the Remote UI. A new Department ID will not be allocated if one has already been allocated. This setting can only be specified from the Remote UI.

NOTE:

- If the user name is comprised of numbers and is seven digits or fewer, the same number is assigned to the same user as the Department ID. If the password of the same user is registered as a number that is seven digits or fewer, it is also set as the PIN for that Department ID.
- If the user name and password do not meet the above conditions, a Department ID is automatically assigned starting from 0000001, and 0 (none) is set for the PIN.
- In the following cases, the Department ID is not registered automatically.
 - If a user is registered from the control panel of the machine
 - If 1,000 Department IDs are already registered
 - If 1,001 or more users are already registered

g [Automatically Delete Department ID at User Deletion]

If this check box is selected, when a user is deleted, the department ID assigned to the user is automatically deleted. Counter information assigned to the corresponding department ID is also deleted. If multiple users are registered to the department ID, it is not automatically deleted.

h [Default Role When Registering User:]

Select the role to apply to users in situations such as when no privileges are set.

i [Allow e-mail address settings]

Select the check box to enable users without Administrator privileges to specify their own e-mail addresses in their user accounts.

1 [Functions to Restrict:]

Select the check boxes for functions that cannot be used when personal authentication management is enabled.

k [Delete users that have not logged in for the specified period]

Select the check box to delete users registered in the local device who have not logged in to the machine for a specified period of time. Make sure to also specify the number of days before automatic deletion and the time it is executed.

NOTE:

- If you set [Auto Delete After:] to [0], all accounts other than the administrator are deleted at the time set in [Auto Delete Time:].
- If the accounts cannot be deleted at the specified time because the machine is turned OFF or is completely in sleep mode, the accounts are deleted the next time that the machine starts.
- If a user has never logged in before, the date and time that the user was registered is displayed as the time that the user last logged in.

1 [Communication Mode for Kerberos Authentication:]

Select the communication method used for Kerberos authentication.

6 Click [Update].**7 Restart the machine. ▶Restarting the Machine(P. 336)****NOTE****Batch importing/batch exporting**

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

LINKS

▶ **Registering User Information in the Local Device(P. 246)**

▶ **Registering Server Information(P. 262)**

- ▶ **Using Personal Authentication to Manage Printing via a Computer(P. 274)**

Using Personal Authentication to Manage Printing via a Computer

E9SJ-058

You can apply personal authentication management to printing via a computer. This can provide greater security, as the machine does not accept these operations unless the user is identified.



Start the Remote UI ► [Settings/Registration] ► [User Management] ► [Authentication Management] ► [Basic Settings] ► [Edit...] ► [Functions to Restrict:] ► select [Remote job without user authentication].

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ► **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ► **Importing/Exporting All Settings(P. 359)**

LINKS

- **Registering User Information in the Local Device(P. 246)**
- **Registering Server Information(P. 262)**
- **Configuring the Authentication Functions(P. 270)**

Using Other Convenient Personal Authentication Management Functions

E9SJ-059

Personal authentication management provides a variety of advantages in addition to user authentication. This section describes some of the other convenient functions that use personal authentication to expand the capabilities of printers/multifunctional printers, such as managing user groups.

Department ID Management

Users registered in the machine can be organized into groups such as the departments that they belong to, and managed based on their Department ID. This function lets you check the total number of pages used for each Department ID, or set maximum limits on the number of pages that each department can use for printing, which can help reduce costs. ▶ **Setting the Department ID Management(P. 276)**



Setting the Department ID Management

E9SJ-05A

Users can be organized into groups such as the departments that they belong to, and managed based on their Department ID. First, create all of the Department IDs that are to be managed, and assign users to each one (▶ **Registering User Information in the Local Device(P. 246)**). After assigning users to Department IDs, enable Department ID Management. To perform the same type of management for printing from a computer, configure the additional required settings. Administrator privileges are required in order to configure these settings.



- ▶ **Changing the System Manager ID and PIN(P. 277)**
- ▶ **Configuring the Department ID Management Settings(P. 279)**
- ▶ **Using Department IDs to Manage Printing via Computer(P. 282)**

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Department ID Management Settings] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

Changing the System Manager ID and PIN

E9SJ-05C

When Department ID Management is enabled, Department IDs must be set for users before they can log in. The System Manager ID and System Manager PIN are both set to "7654321" by default, but it is recommended to change them for security reasons. Follow the procedure below to change them.

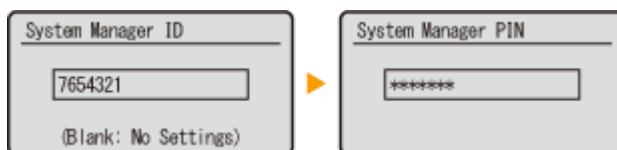
! IMPORTANT

- Make sure that you do not forget the System Manager PIN. If you forget the System Manager PIN, contact your dealer or service representative.

NOTE

- This setting is not a default User Authentication administrator setting. To specify this setting for a user with administrator privileges in User Authentication, set [Select Role to Set:] to "Administrator". **▶ Registering User Information in the Local Device(P. 246)**

- 1** Select <Set> on the <Home> screen. **▶ <Home> Screen(P. 150)**
- 2** Select <Management Settings> ▶ <User Management> ▶ <System Manager Information Settings>.
- 3** Select <System Manager ID and PIN>.
- 4** Set the System Manager ID and System Manager PIN.
 - Set <System Manager ID> ▶ <System Manager PIN>.



NOTE:

- You cannot register a System Manager ID or PIN consisting only of 0s, such as "00" or "0000000".
- Even if you enter fewer than seven digits, zeros are added to the start of the number, and a seven digit number is set.
- You can also make entering seven digits a requirement for the System Manager ID and System Manager PIN. For more information, contact your dealer or service representative.

■ Setting the administrator information

- 1** Select <System Manager Name>/<E-Mail Address>/<Contact Information>/<Comment>.
- 2** Enter the information and select <Apply>.

- For information on entering text, see [▶Entering Characters\(P. 157\)](#) .

LINKS

- ▶[Configuring the Department ID Management Settings\(P. 279\)](#)
- ▶[Registering User Information in the Local Device\(P. 246\)](#)

Configuring the Department ID Management Settings

E9SJ-05E

You can organize and manage users in groups based on Department ID. Follow the procedure below to configure Department ID Management and enable the machine to count the number of pages used for printing.

▶ **Enabling Department ID Management(P. 279)**

▶ **Registering Department IDs and PINs(P. 280)**

! IMPORTANT

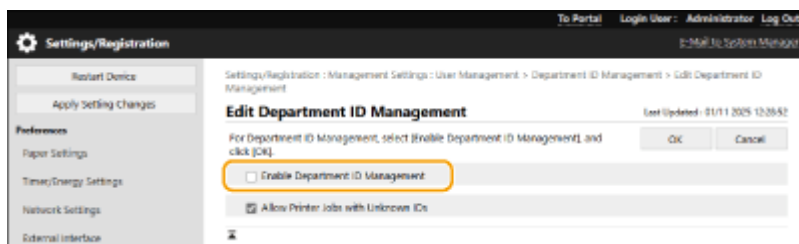
- Make sure that Department IDs have been set for the users registered in the machine. ▶ **Registering User Information in the Local Device(P. 246)**
- Department ID Management is only valid for users who are registered to the local device.
- If you login as a user with Administrator privileges, a System Manager ID and PIN are automatically assigned, and managed as Department ID.

NOTE

- For information on the number of Department IDs that you can register, see ▶ **Management Functions(P. 602)** .

Enabling Department ID Management

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [User Management] ▶ [Department ID Management].**
- 4 Click [Edit].**
- 5 Select [Enable Department ID Management].**



6 Click [OK].

Registering Department IDs and PINs

1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)

3 Click [User Management] ▶ [Department ID Management].

4 Click [Register New Department].

NOTE:

To edit Department ID settings

- Click the department ID to edit to display the edit screen.

To delete Department ID settings

- Click [Delete] for the department ID to delete ▶ [OK].

5 Enter the required information, and click [OK].

a [Department ID]

Enter a number of 7 digits or less for the Department ID.

b [PIN]

Enter the PIN (seven digits maximum). Enter the PIN again in [Confirm]. If you do not want to set a PIN, leave it blank.

c [Page Limit]

You can restrict the number of pages that a registered department can print. Select the target types and enter the page totals.

NOTE:

- You cannot register a Department ID or PIN consisting only of 0s, such as "00" or "0000000".
- Even if you enter fewer than seven digits, zeros are added to the start of the number, and a seven digit number is set.
- You can also make entering seven digits a requirement for Department IDs and PINs. For more information, contact your dealer or service representative.

NOTE

To check the page counts

- If you want to check the total number of pages used by each Department ID for printing, check [Department ID Page Totals] on the screen displayed in step 4. The page counts do not include blank pages or sample prints used for checking items such as gradation adjustment.

Logging In Using a Department ID and PIN

- By registering a user with the same name as a department ID, login operations can be performed using a registered department ID and PIN.  **Registering User Information in the Local Device(P. 246)**

LINKS

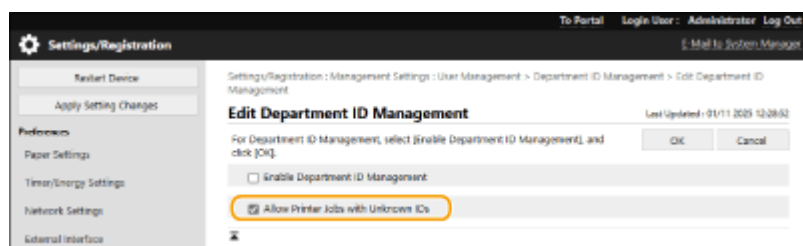
-  **Using Department IDs to Manage Printing via Computer(P. 282)**

Using Department IDs to Manage Printing via Computer

E9SJ-05F

You can use Department ID Management to manage printing operations performed via a computer. Use this function when you would like to improve security or monitor the number of pages that are printed.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [User Management] ▶ [Department ID Management].**
- 4 Click [Edit].**
- 5 Deselect the operations to restrict.**



- When deselected, department ID entry is required when executing the corresponding type of job.
- Select this check box to accept print jobs from printer drivers that do not support Department ID Management.

- 6 Click [OK].**

Setting an Authentication/Password Policy

E9SJ-05H

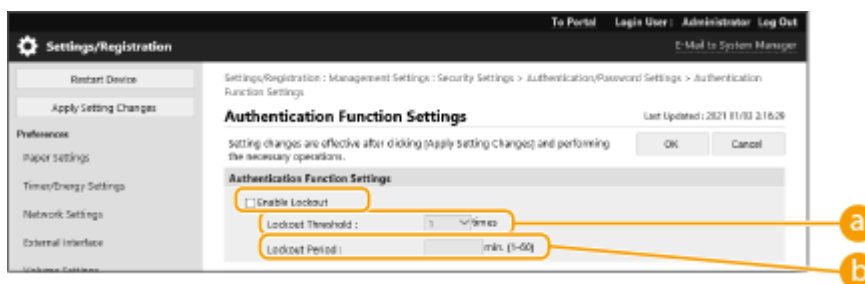
You can set a policy regarding lockout (the state where users temporarily cannot log into the machine) and password operation/entry.

- ▶ **Setting a Lockout Policy(P. 283)**
- ▶ **Setting a Password Policy(P. 284)**

Setting a Lockout Policy

You can set a policy for temporarily preventing a user that fails user authentication from logging in. However, this policy does not apply to authentication that uses information such as department IDs and PINs.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Security Settings] ▶ [Authentication/Password Settings].**
- 4 Click [Edit] in [Authentication Function Settings].**
- 5 Select [Enable Lockout] and configure the detailed settings.**



- a [Lockout Threshold]**
Set the login failure count for lockout. The user becomes unable to log in when the set count is reached.
- b [Lockout Period]**
Set the time until the lockout is canceled.

NOTE:

- When logging in to the machine from an operating system such as Windows or an application that uses FTP, IPP, or SNMPv3, lockout may occur before the set count.

- 6 Click [OK].**

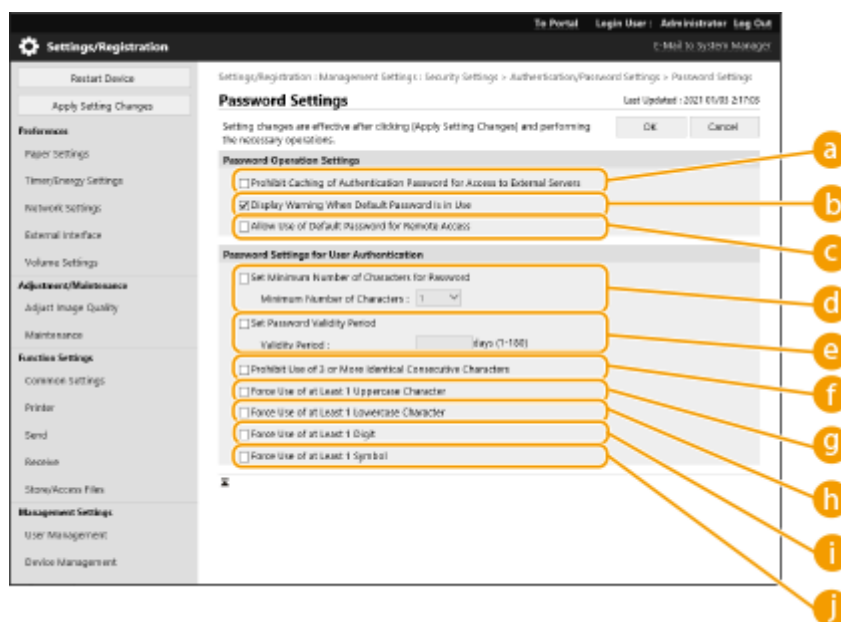
NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. **▶ Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. **▶ Importing/Exporting All Settings(P. 359)**

Setting a Password Policy

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [Security Settings] ▶ [Authentication/Password Settings].**
- 4 Click [Edit] in [Password Settings].**
- 5 Set the password operation and user authentication policy.**



a [Prohibit Caching of Authentication Password for Access to External Servers]

Select this check box to prevent passwords entered during login from being saved in the cache.

b [Display Warning When Default Password Is in Use]

Select this check box to display the screen for changing the password when the Administrator logs in to the machine using the default user name and password.

NOTE:

- If the password has expired, the screen for changing the password appears, regardless of this setting.
- c [Allow Use of Default Password for Remote Access]**
Select this check box to allow the default password to be used when logging in from the Remote UI.
- d [Set Minimum Number of Characters for Password]**

You can set the minimum number of characters required when registering a password to prevent the simplification of passwords. When a password length is set, a user cannot be registered with a blank password.

e [Set Password Validity Period]

To periodically prompt users to change their password, select this check box and specify a period in [Validity Period].

f [Prohibit Use of 3 or More Identical Consecutive Characters]

Select this check box to restrict passwords so that the same character cannot be used consecutively three or more times.

g [Force Use of at Least 1 Uppercase Character]

Select this check box to restrict passwords so that only passwords which include at least one uppercase character can be registered.

h [Force Use of at Least 1 Lowercase Character]

Select this check box to restrict passwords so that only passwords which include at least one lowercase character can be registered.

i [Force Use of at Least 1 Digit]

Select this check box to restrict passwords so that only passwords which include at least one number can be registered.

j [Force Use of at Least 1 Symbol]

Select this check box to restrict passwords so that only passwords which include at least one symbol can be registered.

6 Click [OK].

NOTE

- The settings in **d** to **j** do not apply to Department ID Management and PINs. They are valid for passwords that are registered/edited after the restrictions are set. When a password that is already registered exceeds the restrictions for these settings, a screen prompting to change the password is displayed when user authentication is performed.

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. **▶ Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. **▶ Importing/Exporting All Settings(P. 359)**

Configuring the Network Security Settings

E9SJ-05J

Authorized users may incur unanticipated losses from attacks by malicious third parties, such as sniffing, spoofing, and tampering of data as it flows over a network. To protect your important and valuable information from these attacks, the machine supports the following features to enhance security and secrecy.

Firewall Settings

Unauthorized access by third parties, as well as network attacks and breaches, can be blocked by only allowing communication with devices that have a specific IP address. [Restricting Communication by Using Firewalls\(P. 288\)](#)



Proxy Settings

When the client devices are connected to an external network, communication is established through the proxy server. When the proxy server is used, websites can be browsed more safely, therefore, security can be expected to be enhanced. [Setting a Proxy\(P. 301\)](#)



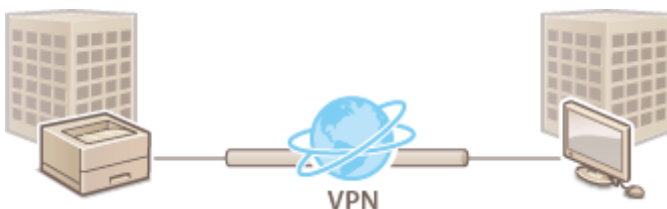
TLS Encrypted Communication

TLS is a protocol for encryption for data sent over a network and is often used for communication via a Web browser or an e-mail application. TLS encrypted communication enables secure network communication when accessing the machine using the Remote UI. [Configuring the Key and Certificate for TLS\(P. 303\)](#)



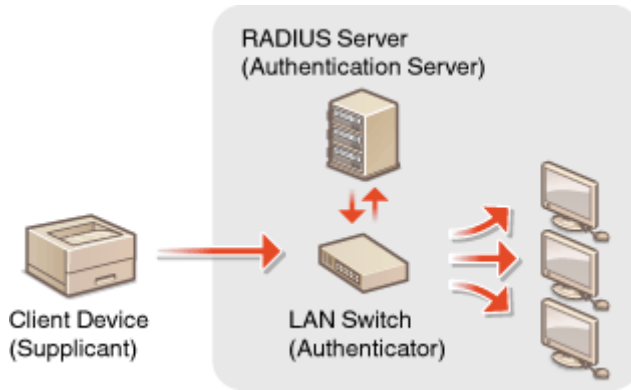
IPSec Communication

While TLS only encrypts data used on a specific application, such as a Web browser or an e-mail application, IPSec encrypts the whole (or payloads of) IP packets. This enables IPSec to offer a more versatile security system than TLS. [Configuring the IPSec Settings\(P. 310\)](#)



IEEE 802.1X Authentication

If a device tries to connect and start communicating on an 802.1X network, the device must go through user authentication in order to prove that the connection is made by an authorized user. Authentication information is sent to and checked by a RADIUS server, which permits or rejects communication to the network depending on the authentication result. If authentication fails, a LAN switch (or an access point) blocks access from the outside of the network. The machine can connect to an 802.1X network as a client device. ➤ **Configuring the IEEE 802.1X Authentication Settings(P. 317)**



Restricting Communication by Using Firewalls

E9SJ-05K

By configuring packet filtering to only allow communication with devices that have a specific IP address or MAC address, you can reduce the risk of unauthorized access by outside third parties. Administrator privileges are required in order to configure these settings.



- ▶ **Specifying IP Addresses in Firewall Settings(P. 289)**
- ▶ **Specifying MAC Addresses in Firewall Settings(P. 292)**
- ▶ **Configuring the Firewall in IP Addresses of the Sub Line(P. 295)**
- ▶ **Configuring the Firewall in MAC Addresses of the Sub Line(P. 298)**

Specifying IP Addresses in Firewall Settings

E9SJ-05L

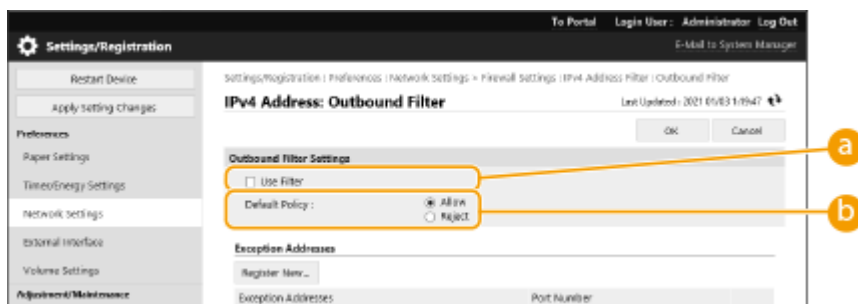
You can set whether to allow or reject communication with a device that has a specific IP address. After configuring the IP addresses in the firewall settings, you can check the results in the log of blocked communication requests. You can also set whether to allow or reject ICMP communications such as PING commands, etc., after specifying firewall settings.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Network Settings] ▶ [Outbound Filter] or [Inbound Filter] for [IPv4 Address Filter]/[IPv6 Address Filter].**

- Select the filter that matches the target IP address. To restrict data sent from the machine to a computer, select [Outbound Filter]. To restrict data received from a computer, select [Inbound Filter].

4 Specify the settings for packet filtering.

- Select the default policy to allow or reject the communication of other devices with the machine, and then specify IP addresses for exceptions.



a [Use Filter]

Select the check box to restrict communication. Clear the check box to disable the restriction.

b [Default Policy]

Select the precondition to allow or reject the communication of other devices with the machine.

[Reject]	Select to pass communication packets only when they are sent to or received from devices whose IP addresses are entered in [Exception Addresses]. Communications with other devices are prohibited.
[Allow]	Select to block communication packets when they are sent to or received from devices whose IP addresses are entered in [Exception Addresses]. Communications with other devices are permitted.

5 Click [Register New].

6 Specify exception addresses.

- Enter the IP address (or range of IP addresses) in [Address to Register].

! IMPORTANT:

- If the IP address is incorrectly entered, you may be unable to access the machine from the Remote UI. In this case, set <Use Filter> to <Off> for <Outbound Filter>/<Inbound Filter> in <IPv4 Address Filter> or <IPv6 Address Filter> from the control panel.
 - If IP addresses are incorrectly entered, you may be unable to access the machine from the Remote UI, in which case you need to set <IPv4 Address Filter> or <IPv6 Address Filter> to <Off>.
- ▶<Network>(P. 452)

NOTE:

Entry form for IP addresses

	Description	Example
Entering a single address	IPv4: Delimit numbers with periods.	192.168.0.10
	IPv6: Delimit alphanumeric characters with colons.	fe80::10
Specifying a range of addresses	Insert a hyphen between the addresses.	192.168.0.10-192.168.0.20
Specifying a range of addresses with a prefix	Enter the address, followed by a slash and a number indicating the prefix length.	192.168.0.32/27 fe80::1234/64

When [Reject] is selected for an outbound filter

- Outgoing multicast and broadcast packets cannot be filtered.

7 Specify the port number as required.

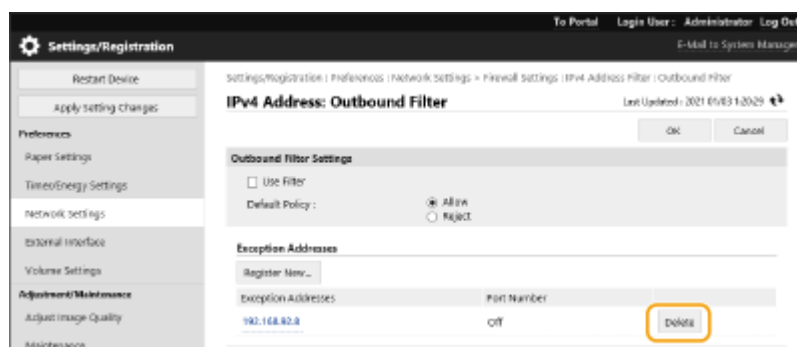
- The exception address setting only applies to communication received from the specified IP address using the designated port number. Enter the port number, and click [Add]. You can register up to 50 ports per one exception address for both IPv4/IPv6.

8 Click [OK].

NOTE:

Deleting an IP address from exceptions

- Click [Delete] for the exception address to delete.

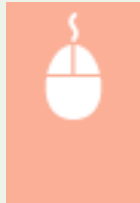


NOTE

Checking the blocked communication requests in the log

- The latest 100 communications blocked by the firewall can be checked in [Settings/Registration] ► [Network Settings] ► [IP Address Block Log]. The history of blocked communications can be exported from the Remote UI in the CSV format. ► **Exporting a Log as a File(P. 354)**
- If [Default Policy] is set to [Reject], the history of communication blocked by the firewall is not displayed in [IP Address Block Log].

To allow or reject ICMP sending and receiving



Click [Settings/Registration] ► [Network Settings] ► [IPv4 Address Filter]/[IPv6 Address Filter] ► [ICMP Sending/Receiving Settings] ► select or deselect [Always Allow Sending/Receiving Using ICMP].

Using the control panel

- You can also enable or disable IP address filtering from <Set> in the <Home> screen. ► **<Network>(P. 452)**

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ► **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ► **Importing/Exporting All Settings(P. 359)**

LINKS

- **Specifying MAC Addresses in Firewall Settings(P. 292)**

Specifying MAC Addresses in Firewall Settings

E9SJ-05R

You can limit communication to only devices with specified MAC addresses, or block devices with specified MAC addresses but permit other communications.

When the machine is connected to two different networks at the same time, set up a firewall in MAC address for the main line, as described in this section. To set up a firewall in MAC address for the sub line, see [▶Configuring the Firewall in MAC Addresses of the Sub Line\(P. 298\)](#) .

! IMPORTANT

- This function is unavailable when the machine is connected to a sub line.

1 Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)

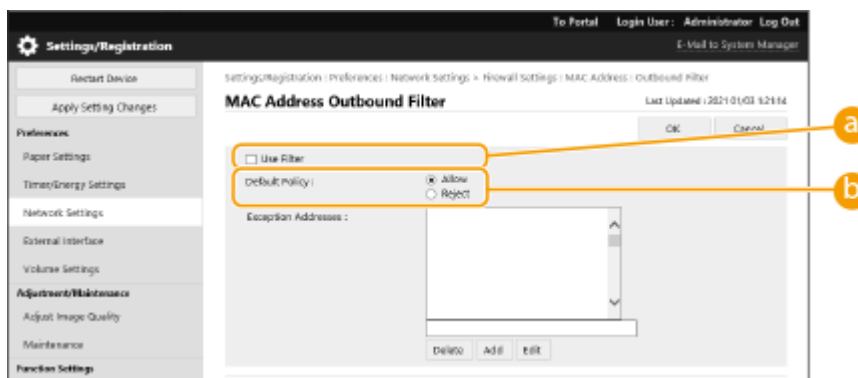
2 Click [Settings/Registration] on the portal page. [▶Remote UI Screen\(P. 331\)](#)

3 Click [Network Settings] ▶ [Outbound Filter] or [Inbound Filter] for [MAC Address Filter].

- To restrict data sent from the machine to a computer, select [Outbound Filter]. To restrict data received from a computer, select [Inbound Filter].

4 Specify the settings for packet filtering.

- Select the precondition (default policy) to allow or reject the communication of other devices with the machine, and then specify MAC addresses for exceptions.



a [Use Filter]

Select the check box to restrict communication. Clear the check box to disable the restriction.

b [Default Policy]

Select the precondition to allow or reject other devices to communicate with the machine.

[Reject]	Select to pass communication packets only when they are sent to or received from devices whose MAC addresses are entered in [Exception Addresses]. Communications with other devices are prohibited.
----------	--

[Allow]	Select to block communication packets when they are sent to or received from devices whose MAC addresses are entered in [Exception Addresses]. Communications with other devices are permitted.
---------	---

5 Specify exception addresses.

- Enter the MAC address in the [Exception Addresses] text box and click [Add].
- You do not need to delimit the address with hyphens or colons.

! IMPORTANT:

- If the MAC address is incorrectly entered, you may be unable to access the machine from the Remote UI. In this case, set <Use Filter> to <Off> for <Outbound Filter>/<Inbound Filter> in <MAC Address Filter> from the control panel.
- If MAC addresses are incorrectly entered, you may become unable to access the machine from the Remote UI, in which case you need to set <MAC Address Filter> to <Off>. ▶<Network>(P. 452)

NOTE:

When [Reject] is selected for an outbound filter

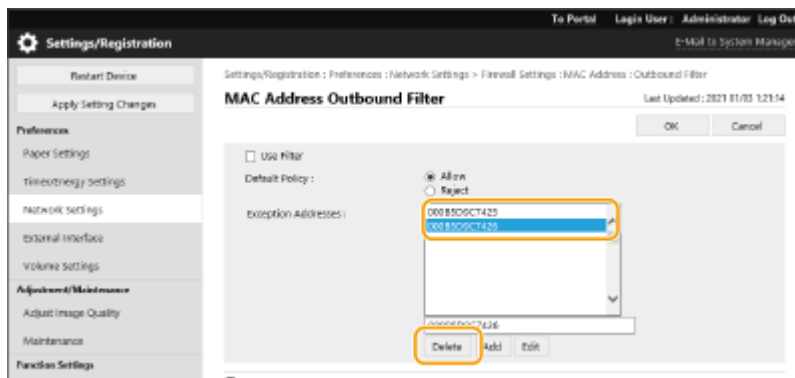
- Outgoing multicast and broadcast packets cannot be filtered.

6 Click [OK].

NOTE:

Deleting a MAC address from exceptions

- Select a MAC address and click [Delete].



NOTE

Using the control panel

- You can also enable or disable MAC address filtering from <Set> in the <Home> screen. ▶<Network>(P. 452)

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶**Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶**Importing/Exporting All Settings(P. 359)**

LINKS

➤ **Specifying IP Addresses in Firewall Settings(P. 289)**

Configuring the Firewall in IP Addresses of the Sub Line

E9SJ-05S

You can set whether to allow communication only with devices that have the specified IP address for communication with the sub line.

NOTE

- Only IPv4 addresses can be registered for the sub line.
- For information on the exception addresses and exception port numbers that can be used for communication and are registered by default, see [▶Management Functions\(P. 602\)](#) .

1 Start the Remote UI. ▶Starting the Remote UI(P. 329)

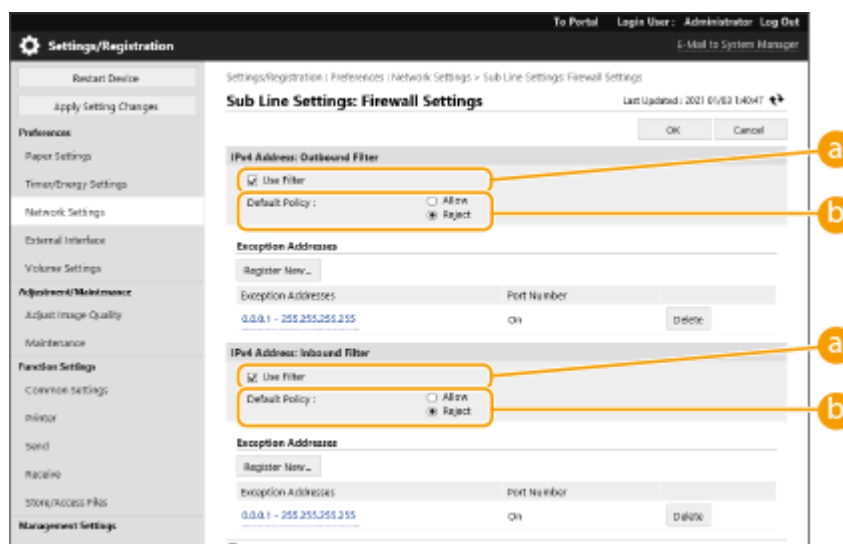
2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)

3 Click [Network Settings] ▶ [Firewall Settings] under [Sub Line Settings].

- Select the filter that matches the target IP address. To restrict data sent from the machine to a computer, select [IPv4 Address: Outbound Filter]. To restrict data received from a computer, select [IPv4 Address: Inbound Filter].

4 Specify the settings for packet filtering.

- Select the default policy to allow or reject the communication of other devices with the machine, and then specify IP addresses for exceptions.



a [Use Filter]

Select the check box to restrict communication. Clear the check box to disable the restriction.

b [Default Policy]

Select the precondition to allow or reject the communication of other devices with the machine.

[Reject]	Select to pass communication packets only when they are sent to or received from devices whose IP addresses are entered in [Exception Addresses]. Communications with other devices are prohibited.
[Allow]	Select to block communication packets when they are sent to or received from devices whose IP addresses are entered in [Exception Addresses]. Communications with other devices are permitted.

5 Click [Register New].

6 Specify exception addresses.

- Enter the IP address (or range of IP addresses) in [Address to Register].

IMPORTANT:

- If the IP address is incorrectly entered, you may be unable to access the machine from the Remote UI. In this case, set <Use Filter> to <Off> for <IPv4 Address Filter>/<Outbound Filter>/<Inbound Filter> from the control panel.

 <Network>(P. 452)

NOTE:

Entry form for IP addresses

	Description	Example
Entering a single address	Delimit numbers with periods.	192.168.0.10
Specifying a range of addresses	Insert a hyphen between the addresses.	192.168.0.10-192.168.0.20
Specifying a range of addresses with a prefix	Enter the address, followed by a slash and a number indicating the prefix length.	192.168.0.32/27

When [Reject] is selected for an outbound filter

- Outgoing multicast and broadcast packets cannot be filtered.

7 Specify the port number as required.

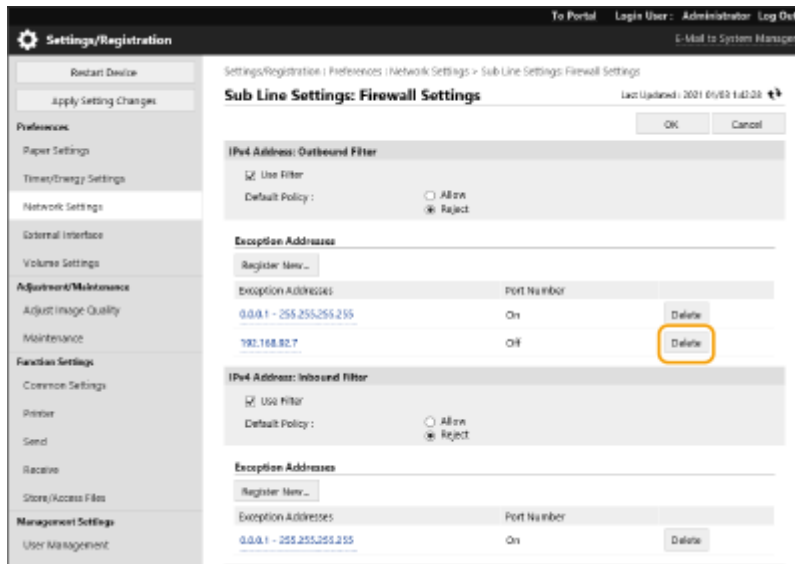
- The exception address setting only applies to communication received from the specified IP address using the designated port number. Enter the port number, and click [Add]. You can register up to 50 ports per one exception address.

8 Click [OK].

NOTE:

Deleting an IP address from exceptions

- Click [Delete] for the exception address to delete..



NOTE

Checking the blocked communication requests in the log

- The latest 100 communications blocked by the firewall can be checked in [Settings/Registration] ► [Network Settings] ► [IP Address Block Log]. The history of blocked communications can be exported from the Remote UI in the CSV format. ► **Exporting a Log as a File(P. 354)**
- If [Default Policy] is set to [Reject], the history of communication blocked by the firewall is not displayed in [IP Address Block Log].

Using the control panel

- You can also enable or disable IP address filtering from <Set> in the <Home> screen. ► **<Network>(P. 452)**

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ► **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ► **Importing/Exporting All Settings(P. 359)**

Configuring the Firewall in MAC Addresses of the Sub Line

You can limit communication to only devices with specified MAC addresses, or block devices with specified MAC addresses but permit other communications.

When the machine is connected to two different networks at the same time, set up a firewall in MAC address for the Sub Line.

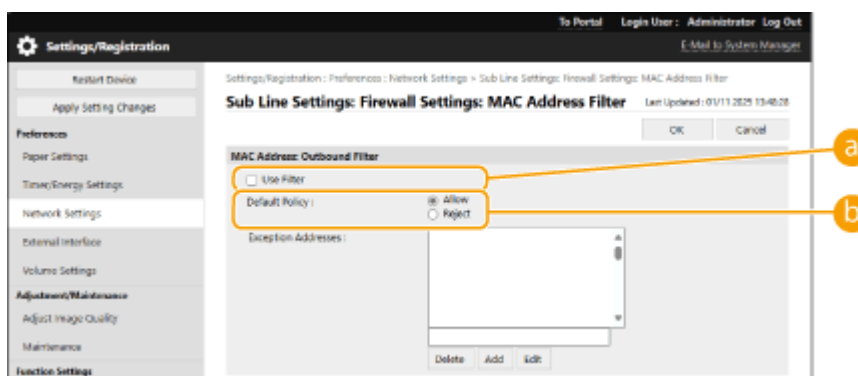
! IMPORTANT

- This function is unavailable when the machine is connected to a wireless LAN.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Network Settings] ▶ [Sub Line Settings] ▶ [Firewall Settings] ▶ [Outbound Filter] or [Inbound Filter] for [MAC Address Filter].**
 - To restrict data sent from the machine to a computer, select [Outbound Filter]. To restrict data received from a computer, select [Inbound Filter].

4 Specify the settings for packet filtering.

- Select the precondition (default policy) to allow or reject the communication of other devices with the machine, and then specify MAC addresses for exceptions.



a [Use Filter]

Select the check box to restrict communication. Clear the check box to disable the restriction.

b [Default Policy]

Select the precondition to allow or reject other devices to communicate with the machine.

[Reject]	Select to pass communication packets only when they are sent to or received from devices whose MAC addresses are entered in [Exception Addresses]. Communications with other devices are prohibited.
----------	--

[Allow]	Select to block communication packets when they are sent to or received from devices whose MAC addresses are entered in [Exception Addresses]. Communications with other devices are permitted.
---------	---

5 Specify exception addresses.

- Enter the MAC address in the [Exception Addresses] text box and click [Add].
- You do not need to delimit the address with hyphens or colons.

! IMPORTANT:

- If the MAC address is incorrectly entered, you may be unable to access the machine from the Remote UI. In this case, set <Use Filter> to <Off> for <Outbound Filter>/<Inbound Filter> in <MAC Address Filter> from the control panel.
- If MAC addresses are incorrectly entered, you may become unable to access the machine from the Remote UI, in which case you need to set <MAC Address Filter> to <Off>. ▶<Network>(P. 452)

NOTE:

When [Reject] is selected for an outbound filter

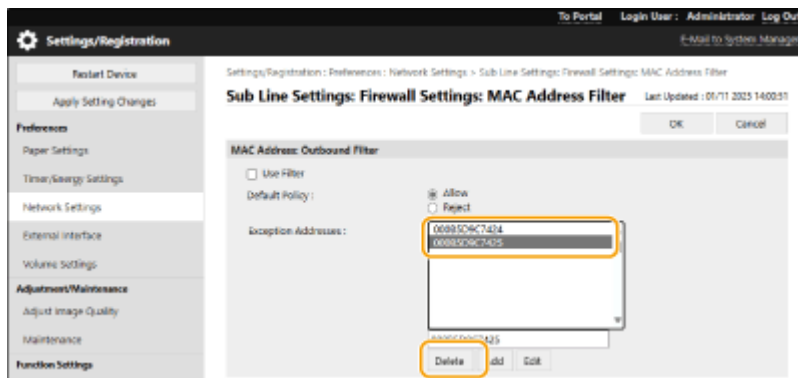
- Outgoing multicast and broadcast packets cannot be filtered.

6 Click [OK].

NOTE:

Deleting a MAC address from exceptions

- Select a MAC address and click [Delete].



NOTE

Using the control panel

- You can also enable or disable MAC address filtering from <Set> in the <Home> screen. ▶<Network>(P. 452)

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶**Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶**Importing/Exporting All Settings(P. 359)**

LINKS

➤ **Specifying IP Addresses in Firewall Settings(P. 289)**

Setting a Proxy

A proxy (or HTTP proxy server) refers to a computer or software that carries out HTTP communication for other devices, especially when communicating with resources outside the network, such as when browsing Web sites. The client devices connect to the outside network through the proxy server, and do not communicate directly to the resources outside. Setting a proxy not only facilitates management of traffic between in-house and outside networks but also blocks unauthorized access and consolidates anti-virus protection for enhanced security. Administrator privileges are required in order to configure these settings.



- 1** Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2** Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3** Click [Network Settings] ▶ [Proxy Settings].
- 4** Select the [Use Proxy] check box and specify the required settings.

a [HTTP Proxy Server Address]

Enter the address of the proxy server. Specify the IP address or host name depending on the environment.

b [HTTP Proxy Server Port Number]

Change the port number as necessary.

c [Use Proxy within Same Domain]

Select the check box to also use the specified proxy server for communication with devices in the same domain.

NOTE:

- This setting is only displayed for the proxy settings screen of the main line.

d [Use Proxy Authentication]

To use the authentication function of a proxy server, select this check box and enter the user name for authentication in [User Name] and the new password to set in [Password] using alphanumeric characters.

- 5** Click [OK].

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. 
Importing/Exporting the Setting Data(P. 357)
- This setting is included in [Settings/Registration Basic Information] when batch exporting.  **Importing/
Exporting All Settings(P. 359)**

Configuring the Key and Certificate for TLS

E9SJ-05X

You can use TLS encrypted communication to prevent sniffing, spoofing, and tampering of data that is exchanged between the machine and other devices such as computers. When configuring the settings for TLS encrypted communication, you must specify a key and certificate (server certificate) to use for encryption. You can use the key and certificate that are preinstalled in the machine, or you can generate your own or acquire them from a certification authority. Administrator privileges are required in order to configure these settings.



▶ **Setting TLS(P. 303)**

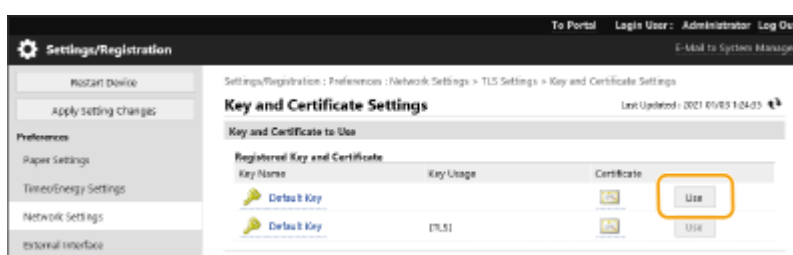
▶ **Setting the Security Strength and Encryption Method(P. 305)**

NOTE

- If you want to use a key and certificate that you generate yourself, generate the key and certificate before performing the procedure below. ▶ **Generating the Key and Certificate for Network Communication(P. 307)**
- If you want to use a key and certificate that you acquire from a certification authority (CA), register the key and certificate before performing the procedure below. ▶ **Registering a Key and Certificate(P. 337)**

Setting TLS

- 1 Start the Remote UI. ▶ **Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ **Remote UI Screen(P. 331)**
- 3 Click [Network Settings] ▶ [TLS Settings].
- 4 Click [Key and Certificate].
- 5 Click [Use] for the key and certificate to use for TLS encrypted communication.

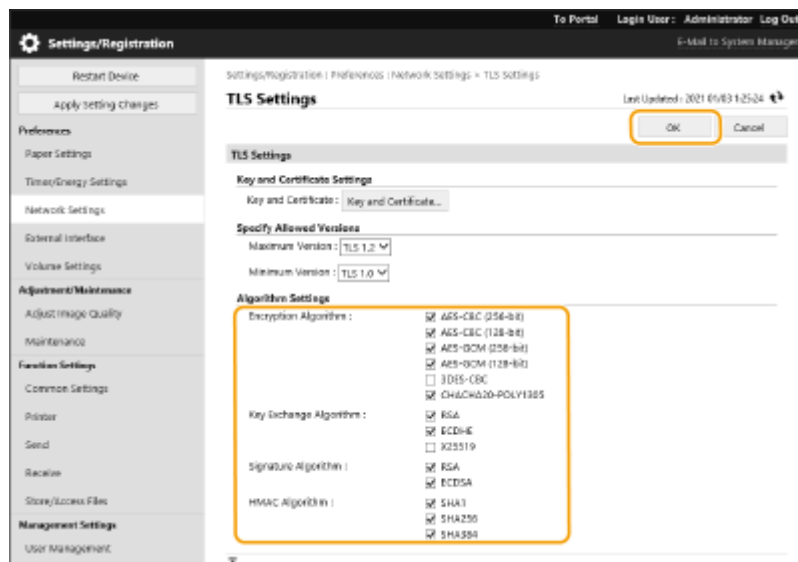


- If you want to use the preinstalled key and certificate, select [Default Key].

6 Click [Network Settings] ► [TLS Settings].

7 Specify [Maximum Version] and [Minimum Version].

8 Select the algorithm to use, and click [OK].



The following combinations of TLS version and algorithm are available.

✓: Available
-: Unavailable

Algorithm	TLS Version			
	[TLS 1.3]	[TLS 1.2]	[TLS 1.1]	[TLS 1.0]
[Encryption Algorithm]				
[AES-CBC (256-bit)]	-	✓	✓	✓
[AES-GCM (256-bit)]	✓	✓	-	-
[3DES-CBC]	-	✓	✓	✓
[AES-CBC (128-bit)]	-	✓	✓	✓
[AES-GCM (128-bit)]	✓	✓	-	-
[CHACHA20-POLY1305]	✓	-	-	-
[Key Exchange Algorithm]				
[RSA]	-	✓	✓	✓
[ECDHE]	✓	✓	✓	✓
[X25519]	✓	-	-	-
[Signature Algorithm]				

[RSA]	✓	✓	✓	✓
[ECDSA]	✓	✓	✓	✓
[HMAC Algorithm]				
[SHA1]	-	✓	✓	✓
[SHA256]	✓	✓	-	-
[SHA384]	✓	✓	-	-

NOTE

- [Format Encryption Method to FIPS 140] cannot be used when [CHACHA20-POLY1305] or [X25519] is selected.

Starting the Remote UI with TLS

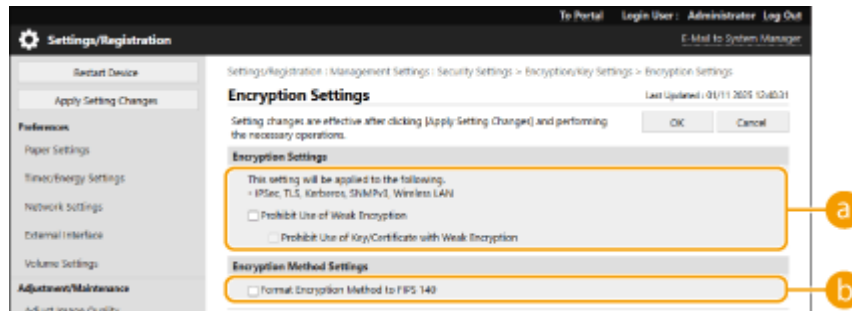
- If you try to start the Remote UI when TLS is enabled, a security alert may be displayed regarding the security certificate. In this case, check that the correct URL is entered in the address field, and then proceed to display the Remote UI screen. [▶Starting the Remote UI\(P. 329\)](#)

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. [▶Importing/Exporting the Setting Data\(P. 357\)](#)
- This setting is included in [Settings/Registration Basic Information] when batch exporting. [▶Importing/Exporting All Settings\(P. 359\)](#)

Setting the Security Strength and Encryption Method

- 1** Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)
- 2** Click [Settings/Registration] on the portal page. [▶Remote UI Screen\(P. 331\)](#)
- 3** Click [Security Settings] ▶ [Encryption/Key Settings].
- 4** Click [Edit] in [Encryption Settings].
- 5** Configure the encryption settings and encryption method, and click [OK].



a [Prohibit Use of Weak Encryption]

Select this check box to prohibit the use of weak encryption with a key length of 1024 bits or less. To prohibit the use of keys and certificates that use weak encryption, select [Prohibit Use of Key/Certificate with Weak Encryption].

b [Format Encryption Method to FIPS 140]

Select this check box to make functions using encryption comply with FIPS 140.

NOTE

- If you select [Format Encryption Method to FIPS 140], you can make the TLS communication encryption method comply with the United States government-approved FIPS (Federal Information Processing Standards) 140, but the following limitations apply.
 - An error will occur if you specify a certificate for TLS that uses an algorithm not recognized by FIPS (lower than RSA2048bit).
 - A communication error will occur if the communication destination does not support FIPS-recognized encryption algorithms.
 - [CHACHA20-POLY1305] and [X25519] can no longer be used.

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. **Importing/Exporting All Settings(P. 359)**

LINKS

- Generating the Key and Certificate for Network Communication(P. 307)**
- Generating a Key and Certificate Signing Request (CSR)(P. 343)**
- Registering a Key and Certificate for Network Communication(P. 337)**
- Starting the Remote UI(P. 329)**
- Configuring E-Mail Print Settings(P. 143)**

Generating the Key and Certificate for Network Communication

E9SJ-05Y



The machine can generate the key and certificate (server certificate) used for TLS encrypted communication. If you want to start using TLS encrypted communication immediately, it is convenient to use the key and certificate that are preinstalled in the machine. If necessary, have an administrator generate a key and certificate. Note, however, that TLS encrypted communication is not enabled simply by generating a key and certificate. ▶ **Configuring the Key and Certificate for TLS(P. 303)**

NOTE

- If you want to use a server certificate with a CA signature, you can generate the key along with a CSR, instead of the certificate. ▶ **Generating a Key and CSR(P. 343)**

- 1 Start the Remote UI.** ▶ **Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page.** ▶ **Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Key and Certificate Settings].**
- 4 Click [Generate Key].**

NOTE:

Deleting a registered key and certificate

- Select the key and certificate to delete → click [Delete] ▶ [OK].
- A key and certificate cannot be deleted if it is currently used for some purpose, such as when "TLS" or "IEEE 802.1X" is displayed under [Key Usage]. In this case, disable the function or replace the other key and certificate before deleting it.

- 5 Click [Network Communication].**
- 6 Specify settings for the key and certificate.**

a [Key Name]

Enter alphanumeric characters for naming the key. Set a name that will be easy for you to find later in a list.

b [Signature Algorithm]

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length ([▶Management Functions\(P. 602\)](#)). A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms.

c [Key Algorithm]

Select [RSA] or [ECDSA] as the key generation algorithm. Select the key length if you selected [RSA] and the key type if you selected [ECDSA]. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If [SHA384] or [SHA512] is selected for [Signature Algorithm], the key length cannot be set to [512-bit] when [RSA] is selected for [Key Algorithm].

d [Validity Start Date (YYYY/MM/DD)]/[Validity End Date (YYYY/MM/DD)]

Enter the start date and end date of the validity period for the certificate. [Validity End Date (YYYY/MM/DD)] cannot be set to a date before the date in [Validity Start Date (YYYY/MM/DD)].

e [Country/Region]

Click the [Select Country/Region Name] radio button and select the country/region from the drop-down list. You can also click the [Enter Internet Country Code] radio button and enter a country code, such as "US" for the United States.

f [State]/[City]

Enter alphanumeric characters for the location as necessary.

g [Organization]/[Organization Unit]

Enter alphanumeric characters for the organization name as necessary.

h [Common Name]

Enter alphanumeric characters for the common name of the certificate as necessary. "Common Name" is often abbreviated as "CN."

i [Issued To (Alternate Name)]

Enter the IP address or domain to be set for the Subject Alternative Name (SAN), as needed.

- If you are not configuring the [Issued To (Alternate Name)] setting, select the [Do Not Set] checkbox.
- Only IPv4 addresses can be set in [IP Address].

7 Click [OK].

- Generating a key and certificate may take some time.

- After the key and certificate is generated, it is automatically registered to the machine.

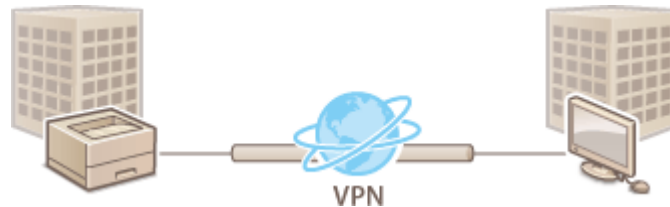
LINKS

- ▶ **Registering a Key and Certificate for Network Communication(P. 337)**
- ▶ **Configuring the Key and Certificate for TLS(P. 303)**
- ▶ **Configuring the IPSec Settings(P. 310)**

Configuring the IPsec Settings

E9SJ-060

By using IPsec, you can prevent third parties from intercepting or tampering with IP packets transported over the IP network. Because IPsec adds security functions to IP, a basic protocol suite used for the Internet, it can provide security that is independent of applications or network configuration. To perform IPsec communication with this machine, you must configure settings such as the application parameters and the algorithm for authentication and encryption. Administrator privileges are required in order to configure these settings.



▶ **Enabling IPsec(P. 311)**

▶ **Registering a Policy(P. 311)**

! IMPORTANT

Communication mode

- This machine only supports transport mode for IPsec communication. As a result, authentication and encryption is only applied to the data portions of IP packets.

Key exchange protocol

This machine supports Internet Key Exchange version 1 (IKEv1) for exchanging keys based on the Internet Security Association and Key Management Protocol (ISAKMP). For the authentication method, set either the pre-shared key method or the digital signature method.

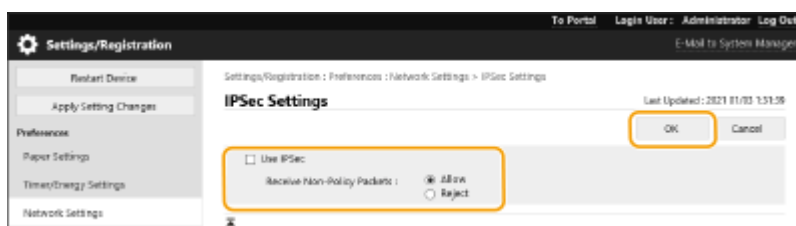
- When setting the pre-shared key method, you need to decide on a passphrase (pre-shared key) in advance, which is used between the machine and the IPsec communication peer.
- When setting the digital signature method, use a CA certificate and a PKCS#12 format key and certificate to perform mutual authentication between the machine and the IPsec communication peer. For more information on registering new CA certificates or keys/certificates, see ▶ **Registering a Key and Certificate for Network Communication(P. 337)** . Note that SNTP must be configured for the machine before it uses this method. ▶ **Making SNTP Settings(P. 138)**

NOTE

- Regardless of the setting of [Format Encryption Method to FIPS 140] for IPsec communication, an encryption module which has already obtained FIPS140 certification will be used.
- In order to make IPsec communication comply with FIPS 140, you must set the key length of both DH and RSA for IPsec communication to 2048-bit or longer in the network environment that the machine belongs to.
- Only the key length for DH can be specified from the machine.
- Take note when configuring your environment, as there are no settings for RSA in the machine.
- You can register up to 10 security policies.

Enabling IPsec

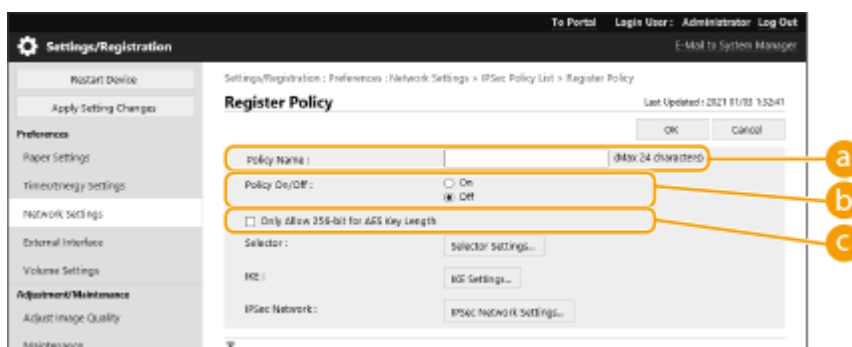
- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [Network Settings] ▶ [IPsec Settings].
- 4 Select [Use IPsec], and click [OK].



- To only receive packets that correspond to the security policy, select [Reject] for [Receive Non-Policy Packets].

Registering a Policy

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [Network Settings] ▶ [IPsec Policy List].
- 4 Click [Register New IPsec Policy].
- 5 Set a policy.



a [Policy Name]

Enter a name for identifying the policy.

b [Policy On/Off]

Select [On] to enable the registered policy.

c [Only Allow 256-bit for AES Key Length]

Select this check box to restrict the key length of the AES encryption method to 256 bit and meet CC authentication standards.

6 Configure the IPsec application parameters.

1 Click [Selector Settings].

2 Specify the IP address to apply the IPsec policy to.

- Specify the IP address of this machine in [Local Address], and specify the IP address of the communication peer in [Remote Address].

The screenshot shows the 'Selector' configuration window. It has a left sidebar with 'Settings/Registration' and a main area with 'Selector' settings. The 'Local Address Settings' and 'Remote Address Settings' sections are highlighted with orange boxes. In both sections, the 'All IP Addresses' radio button is selected. The 'IPv4 Manual Settings' option is also visible, and the 'Single Address' dropdown is set to 'Single Address'. The 'First Address' and 'Last Address' fields are empty. The 'Profile Length' is set to 0. The 'OK' and 'Cancel' buttons are at the top right.

[All IP Addresses]	IPsec is applied to all sent and received IP packets.
[IPv4 Address]	IPsec is applied to IP packets sent to and received from the IPv4 address of this machine.
[IPv6 Address]	IPsec is applied to IP packets sent to and received from the IPv6 address of this machine.
[All IPv4 Addresses]	IPsec is applied to IP packets sent to and received from the IPv4 address of the communication peer.
[All IPv6 Addresses]	IPsec is applied to IP packets sent to and received from the IPv6 address of the communication peer.
[IPv4 Manual Settings]	Specify the IPv4 address to apply IPsec to.

	• Select [Single Address] to enter an individual IPv4 address. • Select [Range Address] to specify a range of IPv4 addresses. Enter a separate address for [First Address] and [Last Address]. • Select [Subnet Settings] to specify a range of IPv4 addresses using a subnet mask. Enter separate values for [First Address] and [Subnet Settings].
[IPv6 Manual Settings]	Specify the IPv6 address to apply IPsec to. • Select [Single Address] to enter an individual IPv6 address. • Select [Range Address] to specify a range of IPv6 addresses. Enter a separate address for [First Address] and [Last Address]. • Select [Prefix Address] to specify a range of IPv6 addresses using a prefix. Enter separate values for [First Address] and [Prefix Length].

3 Specify the port to apply IPsec to.

- Select [Specify by Port Number] to use port numbers when specifying the ports that IPsec applies to. Select [All Ports] to apply IPsec to all port numbers. To apply IPsec to a specific port number [Single Port] and enter the port number. Specify the port of this machine in [Local Port], and specify the port of the communication peer in [Remote Port].
- To specify the ports to apply IPsec to by service name, select [Specify by Service Name] and select the services to use.

4 Click [OK].

7 Configure the authentication and encryption settings.

1 Click [IKE Settings].

2 Configure the necessary settings.

a [IKE Mode]

Select the operation mode for the key exchange protocol. Security is enhanced if you select [Main] because the IKE session itself is encrypted, but the speed of the session is slower than with [Aggressive], which does not encrypt the entire session.

b [Validity]

Set the expiration period of the generated IKE SA.

c [Authentication Method]

Select one of the authentication methods described below.

[Pre-Shared Key Method]	Set the same passphrase (pre-shared key) that is set for the communication peer. Select [Shared Key Settings], enter the character string to use as the shared key, and select [OK].
[Digital Signature Method]	Set the key and certificate to use for mutual authentication with the communication peer. Click [Key and Certificate], and click [Use] for the key to use.

d [Authentication/Encryption Algorithm]

Select either [Auto] or [Manual Settings] to set how to specify the authentication and encryption algorithm for IKE phase 1. If you select [Auto] an algorithm that can be used by both this machine and the communication peer is set automatically. If you want to specify a particular algorithm, select [Manual Settings] and configure the settings below.

[Authentication]	Select the hash algorithm.
[Encryption]	Select the encryption algorithm.
[DH Group]	Select the group for the Diffie-Hellman key exchange method to set the key strength.

3 Click [OK].

NOTE

- When [IKE Mode] is set to [Main] on the [IKE] screen and [Authentication Method] is set to [Pre-Shared Key Method], the following restrictions apply when registering multiple security policies.
 - Pre-shared key method key:** when specifying multiple remote IP addresses to which a security policy is to be applied, all shared keys for that security policy are identical (this does not apply when a single address is specified).
 - Priority:** when specifying multiple remote IP addresses to which a security policy is to be applied, the priority of that security policy is below security policies for which a single address is specified.

8 Configure the IPSec communication settings.

- 1 Click [IPSec Network Settings].
- 2 Configure the necessary settings.



a [Validity]

Set the expiration period of the generated IPsec SA. Make sure to set either [Time] or [Size]. If you set both, the setting with the value that is reached first is applied.

b [PFS]

If you select [Use PFS], the secrecy of the encryption key is increased but communication speed is slower. In addition, the Perfect Forward Secrecy (PFS) function must be enabled on the communication peer device.

c [Authentication/Encryption Algorithm]

Select either [Auto] or [Manual Settings] to set how to specify the authentication and encryption algorithm for IKE phase 2. If you select [Auto], the ESP authentication and encryption algorithm is set automatically. If you want to specify a particular authentication method, select [Manual Settings] and select one of the authentication methods below.

[ESP]	Authentication and encryption are both performed. Select the algorithm for [ESP Authentication] and [ESP Encryption]. Select [NULL] if you do not want to set the authentication or encryption algorithm.
[ESP (AES-GCM)]	AES-GCM is used as the ESP algorithm, and authentication and encryption are both performed.
[AH (SHA1)]	Authentication is performed, but data is not encrypted. SHA1 is used as the algorithm.

3 Click [OK] .

9 Click [OK].

10 Enable the registered policies and check the order of priority.

- Policies are applied in the order that they are listed, starting at the top. If you want to change the order of priority, select a policy in the list and click [Raise Priority] or [Lower Priority].

NOTE

Managing IPsec policies

You can edit policies on the screen displayed in step 4.

- To edit the details of a policy, click the policy name in the list.
- To disable a policy, click the policy name in the list ► select [Off] for [Policy On/Off] ► click [OK].
- To delete a policy, select the policy in the list ► click [Delete] ► [OK].

Using the control panel

- You can also enable or disable IPSec communication from <Set> in the <Home> screen. ▶<IPSec Settings>(P. 456)

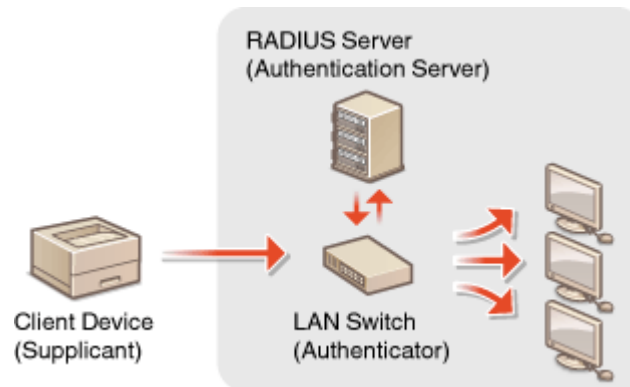
Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶
Importing/Exporting the Setting Data(P. 357)
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶**Importing/
Exporting All Settings(P. 359)**

Configuring the IEEE 802.1X Authentication Settings

E9SJ-061

In a network environment that uses IEEE 802.1X authentication, unauthorized network access is blocked by a LAN switch (authenticator) that only grants access privileges to client devices (supplicants) that are authorized by the authentication server (RADIUS server). To connect this machine to an IEEE 802.1X network, settings such as the authentication method used by the authentication server must be configured on the machine. Administrator privileges are required in order to configure these settings. [IEEE 802.1X Settings] exists for both the main line and sub line. Register the settings as necessary.



IEEE 802.1X Authentication Method

The machine supports the authentication methods described below. You must register a CA certificate before using any of these authentication methods. [▶Registering a CA Certificate\(P. 338\)](#)

■ EAP-TLS (Extensible Authentication Protocol-Transport Level Security)

The machine and the authentication server authenticate each other by mutually sending certificates. A CA certificate must be registered on the machine to verify the certificate (server certificate) sent from the authentication server. In addition, a PKCS#12 format key and certificate (client certificate) must be specified in this setting, so that the authentication server can authenticate the machine. Register these items before configuring the settings ([▶Registering a Key and Certificate\(P. 337\)](#)). This authentication method cannot be used in combination with the other methods.

■ EAP-TTLS (EAP-Tunneled TLS)

Only the authentication server sends a certificate. A CA certificate must be registered on the machine to verify the certificate (server certificate) sent from the authentication server. In addition, a user name and password need to be specified in these settings, so that the authentication server can authenticate the machine. Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) or Password Authentication Protocol (PAP) can be selected as the internal authentication protocol to support EAP-TTLS.

■ PEAP (Protected EAP)

Only the authentication server sends a certificate. A CA certificate must be registered on the machine to verify the certificate (server certificate) sent from the authentication server. In addition, a user name and password need to be specified in these settings, so that the authentication server can authenticate the machine. Only MS-CHAPv2 can be selected as the internal authentication protocol to support PEAP.

Setting the IEEE 802.1X Authentication Method

- 1 Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)**
- 2 Click [Settings/Registration] on the portal page. [▶Remote UI Screen\(P. 331\)](#)**

3 Click [Network Settings] ► [IEEE 802.1X Settings].

- To specify the IEEE 802.1X settings for the sub line, select [Network Settings] ► [Sub Line Settings] ► [IEEE 802.1X Settings].

4 Select [Use IEEE 802.1X] and configure the required settings.

a [Login Name]

Enter the name (EAP Identity) of the login user to receive IEEE 802.1X authentication.

b [Verify Authentication Server Certificate]

Select this check box when verifying server certificates sent from an authentication server.

c [Verify Authentication Server Name]

To verify the common name in the server certificate, select this check box and enter the name of the authentication server where the login user is registered in [Authentication Server Name].

5 Select the authentication method and configure the necessary settings.

■ Selecting EAP-TLS

- Select [Use TLS] and click [Key and Certificate].
- Click [Use] for the key to use in the list.

■Selecting EAP-TTLS/PEAP

- 1 Select [Use TTLS] or [Use PEAP].
 - To use EAP-TTLS, select [Use MSCHAPv2] or [Use PAP] for [TTLS Settings (TTLS Protocol)].
- 2 Click [Change User Name/Password].
 - To set a user name that differs from the login name for IEEE 802.1X authentication, deselect [Use Login Name as User Name]. To use the same name as the login name for IEEE 802.1X authentication, leave it selected.
- 3 Enter the user name and password.
 - To set or change the password, select this check box and enter the same password in [Password] and [Confirm].

6 Click [OK].

NOTE

Using the control panel

- You can also enable or disable IEEE 802.1X authentication from <Set> in the <Home> screen. ▶<IEEE 802.1X Settings>(P. 458)

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶**Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶**Importing/Exporting All Settings(P. 359)**

Restricting the Machine's Functions

E9SJ-062

You can restrict the use of certain functions that may lead to information leaks or that are subject to misuse. It is also possible to completely disable the use of individual functions.

Restricting Printing from a Computer

You can prohibit all users from printing documents from a computer, or only allow printing if the user is authorized on the machine. You can also configure the machine so that only Encrypted Secure Print documents can be printed. **Restricting Printing from a Computer(P. 321)**



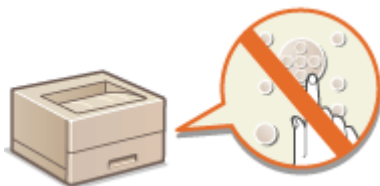
Restricting the Use of Memory Media

Although memory media such as USB memory devices provide convenience, they also increase the potential for security risks such as information leakage. You can set access restrictions for memory media based on your security policy. **Restricting the Use of Memory Media(P. 325)**



Restricting Use of the Control Panel

You can restrict use of the functions and keys on the control panel to protect the machine settings from inadvertent changes or operations. **Restricting Use of the Control Panel(P. 326)**



Restricting Printing from a Computer

E9SJ-063

You can restrict printing from a computer ([▶Printing From a Computer\(P. 170\)](#)) so that only specific types of documents can be printed. You can also configure the machine so that documents are not printed until the user is authorized on the machine ([▶Printing Documents that are Forced to be Held in the Machine\(P. 180\)](#)). You can also restrict the machine to only print Encrypted Secure Print documents, which can prevent information leakage due to unattended printouts or unprotected print data. Administrator privileges are required in order to configure these settings.

- ▶[Prohibiting Printing from a Computer\(P. 321\)](#)
- ▶[Configuring the Forced Hold Printing Settings\(P. 321\)](#)
- ▶[Setting Other Limitations\(P. 323\)](#)

Prohibiting Printing from a Computer

You can prohibit users from printing documents from a computer.



<Set> ▶ <Function Settings> ▶ <Printer> ▶ <Restrict Printer Jobs> ▶ <On> ▶ Select the restriction exceptions

Configuring the Forced Hold Printing Settings



When printing documents from a computer, you can hold print data in the machine and prevent documents from being printed immediately ([▶Printing Documents that are Forced to be Held in the Machine\(P. 180\)](#)). You can configure settings so that printing cannot be performed until the user is authorized on the machine, which ensures greater security and reduces the risk of other people viewing or inadvertently picking up sensitive documents. Administrator privileges are required in order to configure these settings.

- 1** Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)
- 2** Click [Settings/Registration] on the portal page. [▶Remote UI Screen\(P. 331\)](#)
- 3** Click [Printer] ▶ [Print].
- 4** Select [Force Hold], set the necessary conditions, and click [OK].

- You can set detailed conditions for holding printer jobs, such as the user or IP address. If no conditions are set, all print jobs are held except for jobs from unidentified users. If no conditions are set and a print job from an unidentified user is received, it is canceled without being held.

■Setting the conditions for holding documents

- Click [Register New].
- Set the conditions for holding documents, and click [OK].

a [Condition Name]

Enter a name for the condition. Use a name that will be easy to identify when displayed in a list.

b [Enable Condition]

Select this check box to enable the condition.

c [Job Condition]

The types of conditions listed below can be selected.

[User Name]	Specify a particular user name as the condition. If this is left blank, print documents for which the user cannot be identified will be targeted.
[IP Address]	Specify a particular IP address as the condition. You can also specify a range of IP addresses.
[Input Method]	Specify a particular printing protocol as the condition.

d [Target]

You can set either a value specified by the operation target, or one not specified.

e [Action]

Select how to handle documents that match the conditions. When [Hold as Shared Job] is selected, you can set [ID for Substitution] to specify the user name output to the log when printing. Select [Cancel] to discard the document.

- Set the order in which to apply the conditions, and select [OK].

- The conditions are applied in the order that they are listed, starting at the top. To change the priority, click [Up] or [Down] in the list.
- To edit the details of a condition, click the condition name in the list.
- To disable a condition, click the condition name in the list ► deselect [Enable Condition].
- To delete a condition, select [Delete] for the condition to delete in the list ► click [OK].

NOTE

Configuring the detailed settings for forced hold printing

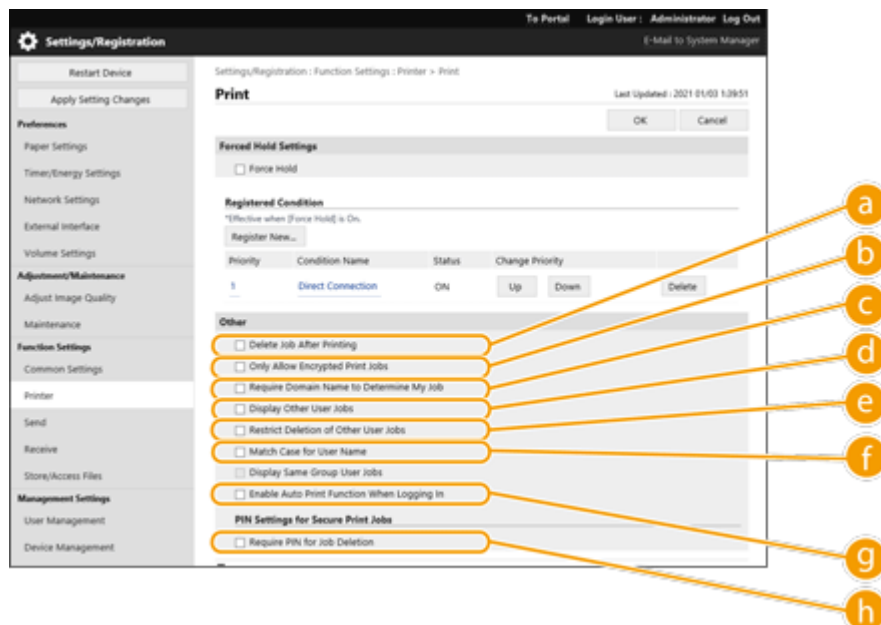
- You can configure detailed settings for documents that are held for printing, such as how long to save them and how to display them. ▶<Print>(P. 484)

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

Setting Other Limitations

- 1 Start the Remote UI. ▶<Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page. ▶<Remote UI Screen(P. 331)
- 3 Click [Printer] ▶ [Print].
- 4 Set the other limitations.



- a [Delete Job After Printing]**
Select this check box to delete jobs after they are printed.
- b [Only Allow Encrypted Print Jobs]**
Select this check box to only receive encrypted secured print jobs from computers.
- c [Require Domain Name to Determine My Job]**
Select this check box to determine the print jobs of login users as "user name + domain name."
- d [Display Other User Jobs]**
Select this check box to display the jobs of users other than the authenticated user.
- e [Restrict Deletion of Other User Jobs]**

Select this check box to restrict jobs of users other than the authenticated user to be deleted when the jobs of users other than the authenticated user are displayed.

f [Match Case for User Name]

Select this check box to make user names case-sensitive.

g [Enable Auto Print Function When Logging In]

Select this check box to allow forced hold print jobs to be automatically printed when each user logs in.

h [Require PIN for Job Deletion]

Select this check box to prompt the user to enter a PIN when deleting a secure print job.

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

Restricting the Use of Memory Media

E9SJ-064

Although memory media such as USB memory devices provide convenience, they can also be a source of information leakage if they are not properly managed. This section describes the procedure for prohibiting the use of memory media to prevent the printing of data saved on memory media. Administrator privileges are required in order to configure these settings.



Select <Set> ► <Function Settings> ► <Access Files> ► <Memory Media Settings> ► <Use Print Function> ► <Off>.

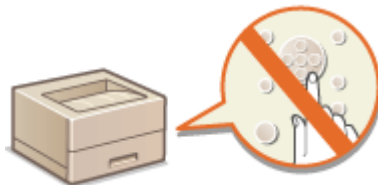
LINKS

- ▶ **Using Memory Media(P. 202)**
- ▶ **Printing From Memory Media (Media Print)(P. 192)**

Restricting Use of the Control Panel

E9SJ-065

You can restrict use of the functions and keys on the control panel to protect the machine settings from inadvertent changes or operations.



- 1** Start the Remote UI. ▶ **Starting the Remote UI(P. 329)**
- 2** Click [Settings/Registration] on the portal page. ▶ **Remote UI Screen(P. 331)**
- 3** Click [Device Management] ▶ [Key Lock/Function Lock Settings].
- 4** Select the keys and functions to lock, and click [OK].

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

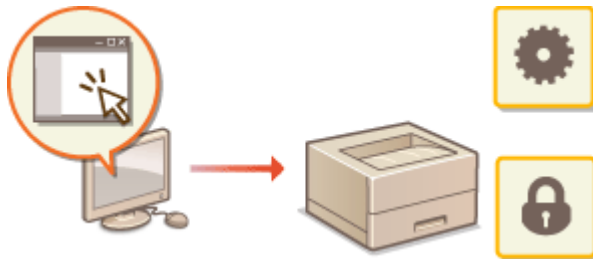
Managing the Machine from a Computer (Remote UI)

E9SJ-066

You can remotely operate the machine from your computer's Web browser to perform operations such as checking the printing status or changing the machine settings. This convenient feature enables you to remain at your desk while operating the machine. To perform remote operation, enter the IP address of the machine in your Web browser and open the Remote UI portal page. For more information on the system requirements for the Remote UI, see [▶ System Specifications\(P. 598\)](#) .

How to Use the Remote UI

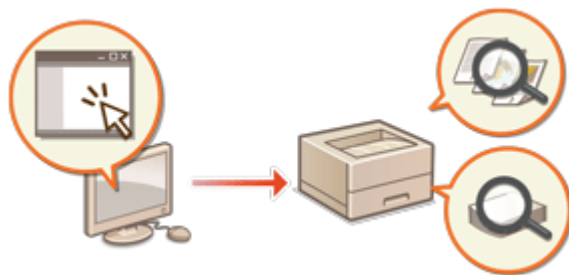
This section describes the Remote UI login procedure and the features of the Remote UI main screen.



▶ Starting the Remote UI(P. 329)

Checking the Status of Waiting Documents and the Machine

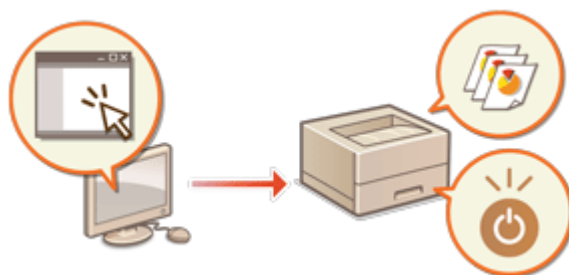
This section describes how to check the status of printed documents, as well as error information and the remaining amount of paper.



▶ Checking the Status and Logs(P. 334)

Other Functions Available Using the Remote UI

This section describes various other convenient functions that can be performed via computer using the Remote UI, such as backing up the machine settings in case they are needed.



- ▶ Turning OFF/Restarting the Machine(P. 336)
- ▶ Registering a Key and Certificate for Network Communication(P. 337)
- ▶ Configuring the Expiration Check Method for Received Certificates(P. 340)
- ▶ Generating a Key and Certificate Signing Request (CSR)(P. 343)
- ▶ Retrieving/Updating a Certificate from an SCEP Server(P. 346)
- ▶ Managing the Logs(P. 352)
- ▶ Importing/Exporting the Setting Data(P. 357)
- ▶ Updating the Firmware(P. 363)
- ▶ Updating the Firmware (Distribution)(P. 365)
- ▶ Setting Scheduled Updates(P. 368)
- ▶ Displaying Messages from the Administrator(P. 370)

 IMPORTANT

- Do not access other websites when the browser is accessing the Remote UI of your printer. Do not forget to close the web browser if you step away from the computer or after you finish changing settings.

When using a proxy server

- You cannot access the machine via a proxy server. If a proxy server is used in your environment, configure your Web browser to bypass the proxy server and access the machine directly.

Starting the Remote UI

E9SJ-067

To start the Remote UI, enter the IP address of the machine in your Web browser. Check the IP address configured for the machine before performing this operation. [▶Setting an IP Address\(P. 119\)](#)

For security reasons, you cannot log in to the Remote UI using the default password (7654321) for the Administrator user. Log in to the Remote UI after changing the password of the Administrator user from the control panel.



<Set> ▶ <Management Settings> ▶ <User Management> ▶ <Authentication Management> ▶ <Set Administrator Password> ▶ change the password for "Administrator"

! IMPORTANT

- Make sure that you do not forget your password. If you forget your password, contact your dealer or service representative.
- When both the machine and the Active Directory server are set as user authentication devices ([▶Configuring the User Login Methods and Authentication Devices\(P. 270\)](#)), the time setting of the Active Directory server needs to match that of the machine.

NOTE

Using TLS encryption for communication

- When you want to encrypt the Remote UI communication, configure the TLS key and certificate ([▶Configuring the Key and Certificate for TLS\(P. 303\)](#)), go to the <Remote UI Settings> setting ([▶<Remote UI Settings>\(P. 489\)](#)) and set <Use TLS> to <On>, then turn the machine OFF and back ON.

Logging in to the Remote UI using the default password of the Administrator user

- You can also set to allow logging in to the Remote UI using the default password of the Administrator user. [▶Setting a Password Policy\(P. 284\)](#)

[▶Starting the Remote UI\(P. 329\)](#)

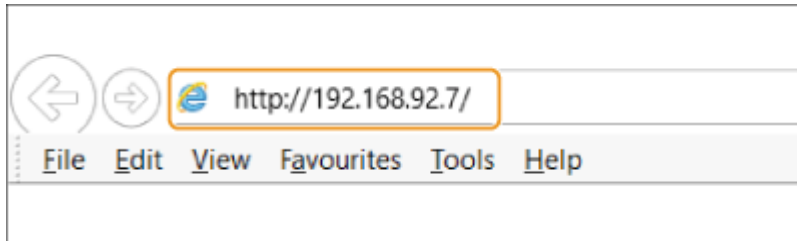
[▶Setting the Timeout Time after Logging In to the Remote UI\(P. 331\)](#)

[▶Remote UI Screen\(P. 331\)](#)

Starting the Remote UI

1 Start the Web browser.

2 Enter the IP address of the machine, and press the [ENTER] key on the computer keyboard.



- Enter "http://<IP address of the machine>/" in the address input field.
- When using an IPv6 address, enclose the IP address portion in brackets ([]) (**Example:** http://[fe80:2e9e:fcff:fe4e:dbce]/).

NOTE:

If the Remote UI does not start

- If the login screen is not displayed in step 3 of this procedure, clear the Web browser's cache and enter the IP address again.

If a message related to security is displayed

- A warning message may be displayed if the Remote UI communication is encrypted. If there are no problems with the certificate or TLS settings, you can continue using the Web browser.

3 Log in to the Remote UI.

- Enter a registered user name and password in [User Name] and [Password], select the login destination in [Login Destination], and click [Log In].
- If [Log In (Guest)] is displayed, unregistered users can click this button and log in as general users.

NOTE:

- With some user authentication settings, the Remote UI may skip the login screen and display the main screen (portal page) directly. ➤ **Remote UI Screen(P. 331)**

■ If two-factor authentication is enabled

You must enter a one-time password to log in, in addition to the password set in " ➤ **Registering User Information(P. 246)** ."

NOTE

- To obtain a one-time password, a mobile app (Microsoft Authenticator or Google Authenticator) must be installed to a mobile device such as a smartphone or tablet. The time of the mobile device must also match that of the machine.

- 1 Enter a registered user name and password in [User Name] and [Password], select the login destination in [Login Destination], and click [Log In].**

NOTE:

- If you have already registered an account to the mobile app, proceed to step 4.
- If two-factor authentication is disabled for a user account but the account is set to require the use of two-factor authentication in [Always Require Two-Factor Authentication:], two-factor authentication must be enabled with the mobile app.

- 2 Check the displayed message and press [OK].**

- 3 Start the mobile app and use it to scan the QR code displayed on the screen of the Remote UI.**

NOTE:

- If you cannot scan the QR code, enter the key displayed in [Manual Entry Key:].

4 On the [One-Time Password:] screen, enter the one-time password displayed in the mobile app.

- For subsequent logins, you can log in simply by entering the one-time password for the account registered in the mobile app.

NOTE

- If you cannot log in to the Remote UI because the mobile device was lost or the account information registered to the mobile app was accidentally deleted, see "  **Enabling Two-Factor Authentication(P. 249)** ."

4 Check that the Remote UI portal page is displayed. Remote UI Screen(P. 331)** IMPORTANT**

- When using the Remote UI to operate the machine, do not use the Web browser's [Back] button. The page may not change properly if you use the [Back] button.

Setting the Timeout Time after Logging In to the Remote UI

The user is automatically logged out if no operations are performed for a certain period of time after logging in to the Remote UI. You can set the time until the user is logged out.



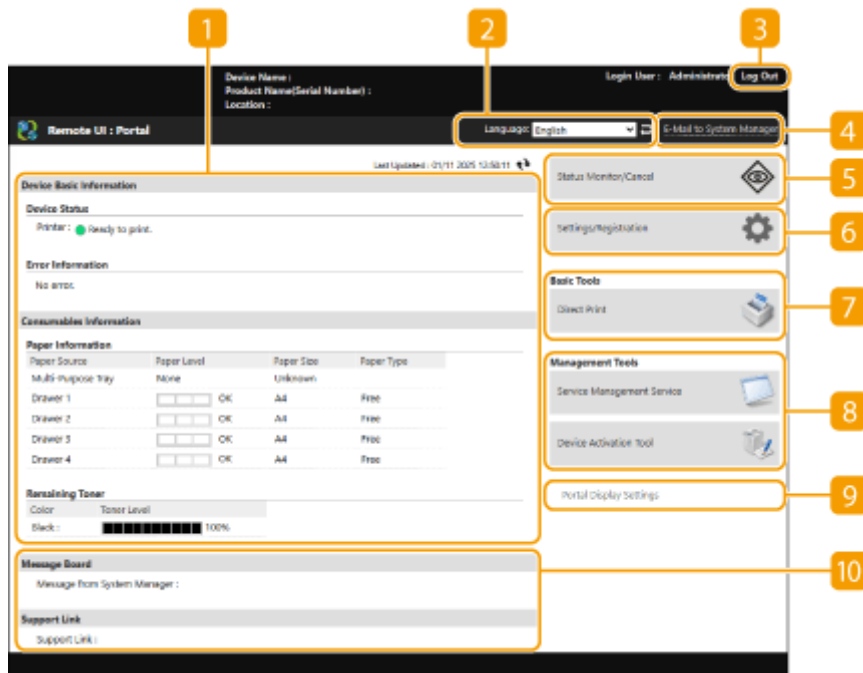
Start the Remote UI ► [Settings/Registration] ► [Network Settings] ► [Session Settings] ► [Timeout After Logging in to Remote UI] ► set the timeout time after login ► [OK]

Remote UI Screen

The portal page shown below is displayed when you log in to the Remote UI. This section describes the items displayed on the portal page and the basic operations.

** IMPORTANT**

- Some display items and functions are only available if you log in with Administrator privileges.
- If multiple users are operating the Remote UI at the same time or the control panel of the machine is being operated at the same time as the Remote UI, the last operation that is performed is effective.



1 Device information

The current machine status is displayed, along with information about errors, consumables, etc.

2 Display language

You can switch the language that is displayed on the Remote UI screen.

3 [Log Out]

Log out from the Remote UI and return to the login page.

4 [E-Mail to System Manager]

Create an e-mail message to send to the administrator. The administrator's e-mail address can be set in [Settings/Registration] ► [User Management] ► [System Manager/Contact Person Information Settings].

5 [Status Monitor/Cancel]

You can check the status of jobs or cancel processing. You can also check detailed information about the amount of remaining toner and paper, etc. ► **Checking the Status and Logs(P. 334)**

6 [Settings/Registration]

You can change the machine settings. You can save the setting details to a computer, or import them from a computer to the machine. ► **Importing/Exporting the Setting Data(P. 357)**

NOTE:

- You can use either the control panel or the Remote UI to change most machine settings, but some settings can only be changed using one or the other.

7 [Basic Tools]

You can print documents.

► **Directly Printing Files without Opening Them(P. 188)**

8 [Management Tools]

You can manage applications.

9 [Portal Display Settings]

You can change the order in which the [Basic Tools] and [Management Tools] buttons are displayed on the portal page.

10 Messages/support

Messages from the administrator are displayed, along with links to machine support information. ▶

Displaying Messages from the Administrator(P. 370)

NOTE

- To update the current page with the latest information, click  .

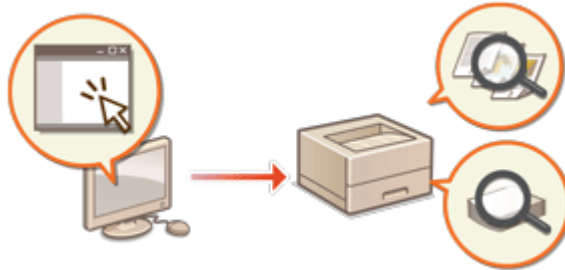
LINKS

▶ **Settings/Registration(P. 386)**

Checking the Status and Logs

E9SJ-068

You can use the Remote UI to check the status of documents that are waiting to be processed, as well as the logs for documents that have been processed. You can also check the status of the machine, such as error information and the remaining amount of consumables.



- ▶ **Checking the Status of Prints(P. 334)**
- ▶ **Checking the Job Log(P. 335)**
- ▶ **Checking the Machine Status(P. 335)**

NOTE

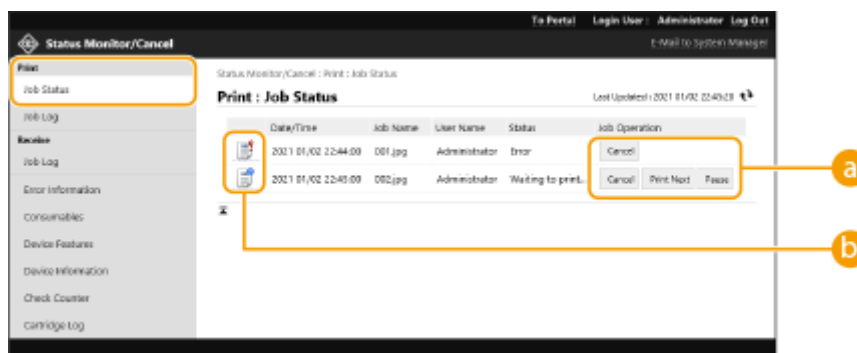
- When personal authentication management is used, you can restrict users from performing operations on the jobs of other users on the <Status Monitor> screen. ▶ **<Restrict Access to Other User Jobs>(P. 487)**

Checking the Status of Prints

You can check the status of documents that are waiting to be printed. You can also output a document before the others, or cancel a document.



Start the Remote UI ▶ [Status Monitor/Cancel] ▶ [Job Status] under [Print]



a Operation buttons

- [Cancel]: Printing is canceled. The canceled document is deleted and cannot be recovered.
- [Print Next]: The document is output immediately after the current document is complete.
- [Pause]: You can cancel printing. Click [Resume] to resume printing a document that was paused.

b Document icon

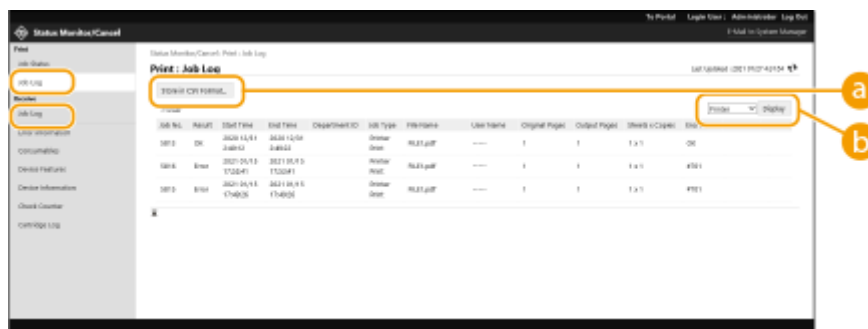
Click the icon to display detailed information about the document.

Checking the Job Log

You can display a log for documents that were printed or received.



Start the Remote UI ► [Status Monitor/Cancel] ► [Job Log]



a [Store in CSV Format]

The log data can be exported and saved as a CSV file (*.csv) on the computer.

b Function selection

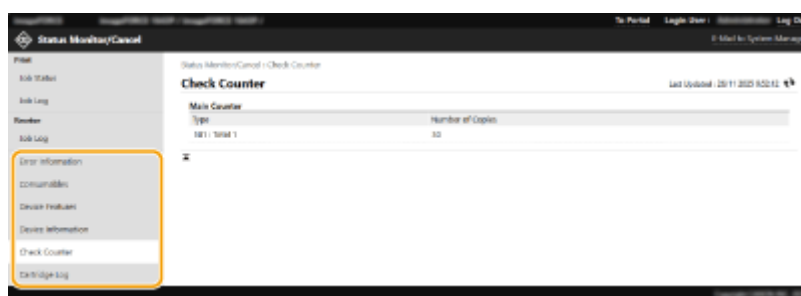
Select the function that you want to check, and click [Display]. The displayed functions may vary depending on your machine model and optional equipment.

Checking the Machine Status

You can check a variety of information about the machine, such as error information, the amount of remaining paper and toner, information about attached optional equipment, and the total number of pages that have been printed up to now.



Start the Remote UI ► [Status Monitor/Cancel] ► Select the item that you want to check



LINKS

▶ Starting the Remote UI(P. 329)

Turning OFF/Restarting the Machine

E9SJ-069

You can use the Remote UI to shut down or restart the machine.

IMPORTANT

- When the machine is turned OFF or restarted, any documents that are being printed are canceled.

▶ **Turning OFF the Machine(P. 336)**

▶ **Restarting the Machine(P. 336)**

Turning OFF the Machine



Start the Remote UI ▶ [Settings/Registration] ▶ [Device Management] ▶ [Remote Shutdown] ▶ [Start]

Restarting the Machine



Start the Remote UI ▶ [Settings/Registration] ▶ [Restart Device] ▶ [Perform Restart] ▶ [OK]

LINKS

▶ **Starting the Remote UI(P. 329)**

▶ **Turning ON the Machine(P. 29)**

▶ **Turning OFF the Machine(P. 30)**

Registering a Key and Certificate for Network Communication

E9SJ-06A

You can use the Remote UI to register keys/certificates and CA certificates to the machine from your computer. Designate an administrator to register these items.



▶ **Registering a Key and Certificate(P. 337)**

▶ **Registering a CA Certificate(P. 338)**

NOTE

The communication methods listed below use a key/certificate or CA certificate. If you want to use a registered key and certificate in actual communication, you need to specify the key and certificate in the settings for each communication method. However, an X.509 DER format CA certificate does not need to be specified in the settings for each communication method. You can use it simply by registering it to the machine.

- TLS encrypted communication ▶ **Configuring the Key and Certificate for TLS(P. 303)**
- IPSec ▶ **Configuring the IPSec Settings(P. 310)**
- IEEE 802.1X ▶ **Configuring the IEEE 802.1X Authentication Settings(P. 317)**

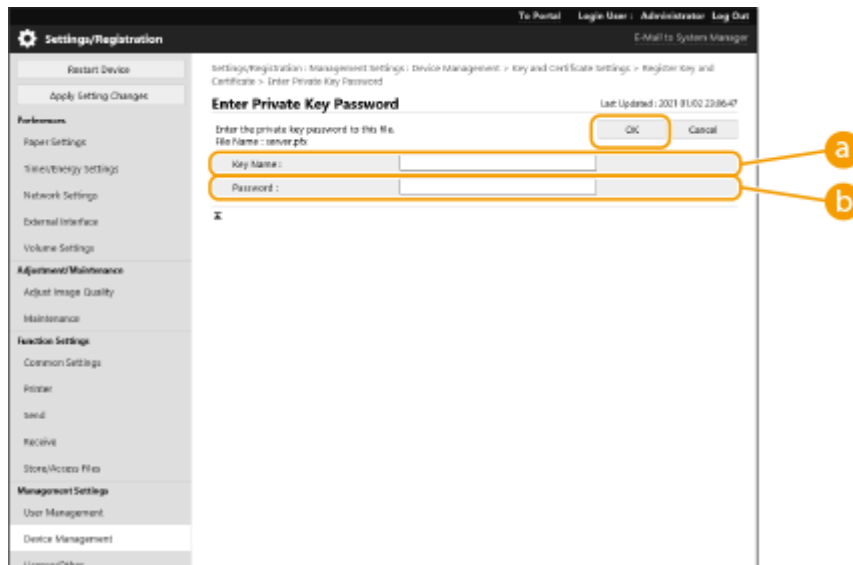
Registering a Key and Certificate

Keys and certificates (server certificates) can be registered via the Remote UI. For information on the keys and certificates that can be registered on the machine, see ▶ **System Specifications(P. 598)** .

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Key and Certificate Settings].**
- 4 Click [Register Key and Certificate].**
- 5 Click [Install].**
- 6 Install the key and certificate.**
 - Click [Choose File], specify the files (key and certificate) to install, and click [Start Installation].

7 Register the key and certificate.

- 1 Select the key and certificate that you want to register, and click [Register].
- 2 Enter the key name and password, and click [OK].



a [Key Name]

Use alphanumeric characters to enter the name of the key that was registered to the machine.

b [Password]

Use alphanumeric characters to enter the password of the private key that is set for the file to register.

NOTE

Managing keys and certificates

You can check the detailed settings or delete keys and certificates on the screen displayed in step 4.

- If  is displayed, the key is corrupted or invalid.
- If  is displayed, the certificate for the key does not exist.
- Click a key name to display detailed information about the certificate. You can also click [Verify Certificate] on this screen to check whether the certificate is valid.
- To delete a key and certificate, select the one that you want to delete, and click [Delete] ► [OK].

Registering a CA Certificate

X.509 DER format CA certificates are preinstalled in the machine. You can register a new CA certificate if it is required by a particular function. For information on the CA certificates that can be registered on the machine, see **System Specifications(P. 598)** .

1 Start the Remote UI. Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)

3 Click [Device Management] ▶ [CA Certificate Settings].

4 Click [Register CA Certificate].

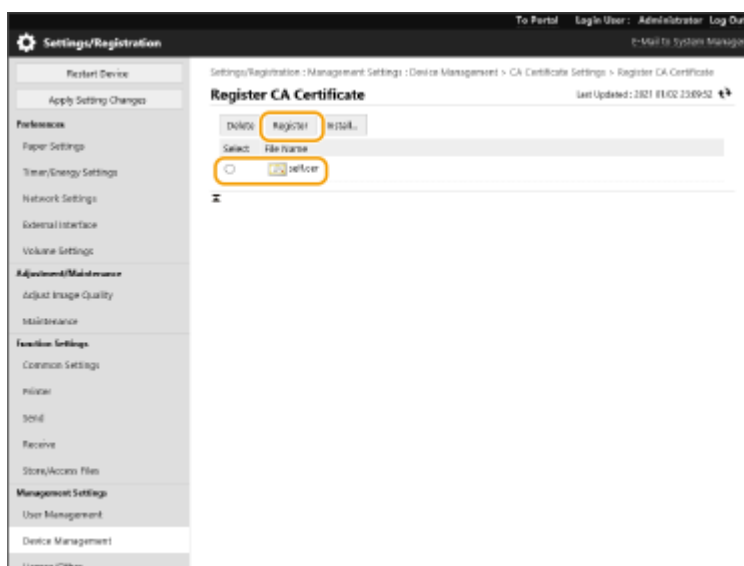
5 Click [Install].

6 Install the CA certificate.

- Click [Choose File], specify the file (CA certificate) to install, and click [Start Installation].

7 Register the CA certificate.

- Select the CA certificate that you want to register, and click [Register].



NOTE

Managing CA certificates

You can check the detailed settings or delete CA certificates on the screen displayed in step 4.

- Click  to display detailed information about the CA certificate. You can also click [Verify Certificate] on this screen to check whether the CA certificate is valid.
- To delete a CA certificate, select the one that you want to delete, and click [Delete] ▶ [OK].

Configuring the Expiration Check Method for Received Certificates

E9SJ-06C

There are two methods for verifying whether certificates received from the other party in communication are valid: Comparing with the certificate revocation list (CRL) registered in the machine and querying an OCSP (online certificate status protocol) responder (a server that supports OCSP). Set the method for checking the expiration of certificates according to your environment. This registration can only be performed by the administrator.

- ▶ **Registering a Certificate Revocation List (CRL)(P. 340)**
- ▶ **Configuring the Online Certificate Status Protocol (OCSP)(P. 341)**

Registering a Certificate Revocation List (CRL)

You can use the Remote UI to register a certificate revocation list (CRL). For information on the CRLs that can be registered on the machine, see ▶ **System Specifications(P. 598)** .

- 1 Start the Remote UI.** ▶ **Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page.** ▶ **Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Certificate Revocation List (CRL) Settings].**
- 4 Click [Register CRL].**
- 5 Register the CRL.**
 - Click [Choose File], specify the file (CRL) to register, and click [Register].

NOTE

Managing CRLs

You can check the detailed settings or delete CRLs on the screen displayed in step 4.

- Click  to display detailed information about it. You can also click [Verify CRL] on this screen to check whether the CRL is valid.
- To delete a CRL, select the one that you want to delete, and click [Delete] ▶ [OK].

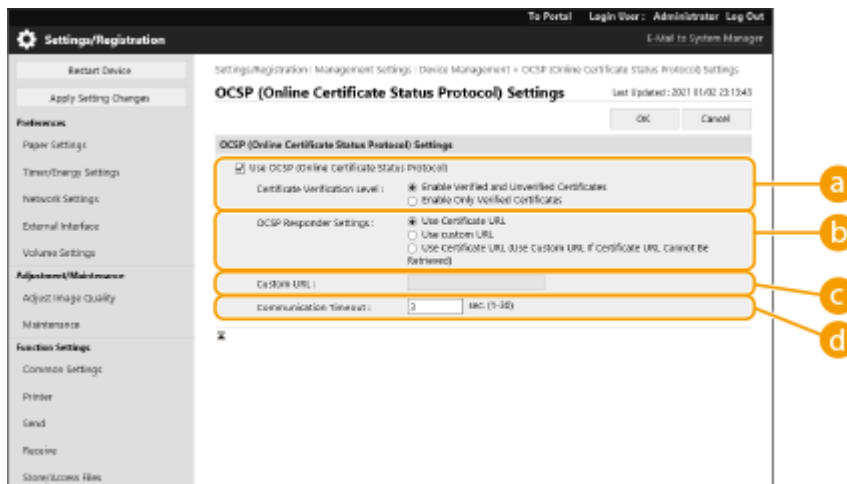
Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. ▶ **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Certificate/Certificate Revocation List (CRL) Settings] when batch exporting. ▶ **Importing/Exporting All Settings(P. 359)**

Configuring the Online Certificate Status Protocol (OCSP)

You can configure the certificate verification level and the OCSP responder to connect to.

- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3 Click [Device Management] ▶ [OCSP (Online Certificate Status Protocol) Settings].
- 4 Select the check box for [Use OCSP (Online Certificate Status Protocol)], and configure the online certificate status protocol (OCSP).



a [Certificate Verification Level]

Set whether to disable certificates in situations such as the following:

- When the machine cannot connect to the OCSP responder
- When a timeout occurs
- When expiration cannot be checked, such as when the result of checking the expiration of a certificate via the OCSP responder is unknown

b [OCSP Responder Settings]

Specify the URL for connecting to the OCSP responder.

c [Custom URL]

When [Use custom URL] or [Use Certificate URL (Use Custom URL If Certificate URL Cannot Be Retrieved)] is selected, enter the URL of the OCSP responder (ASCII code only, maximum 255 characters).

d [Communication Timeout]

Set the time until communication with the OCSP responder times out. The connection is canceled if there is no response from the OCSP responder within the set time.

- 5 Click [OK].

NOTE

Batch importing/batch exporting

- This setting can be imported/exported with models that support batch importing of this setting. 
Importing/Exporting the Setting Data(P. 357)
- This setting is included in [Settings/Registration Basic Information] when batch exporting.  **Importing/
Exporting All Settings(P. 359)**

Generating a Key and Certificate Signing Request (CSR)

E9SJ-06E

Certificates generated on this machine do not have a CA signature, which may cause communication errors with some communication peers. To request a certificate with a CA signature, certificate signing request (CSR) data is required. A user who logs in with administrator privileges can generate a CSR.

▶ **Generating a Key and CSR(P. 343)**

▶ **Registering a Certificate to a Key(P. 344)**

Generating a Key and CSR

You can generate a key and CSR on the machine. You can also display the CSR data on the screen and export it as a file.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Key and Certificate Settings].**
- 4 Click [Generate Key].**
- 5 Click [Key and Certificate Signing Request (CSR)].**
- 6 Configure the necessary items for the key and certificate.**

a [Key Name]

Enter a name for the key. Use a name that will be easy to find when displayed in a list.

b [Signature Algorithm]

Select the hash algorithm to use for the signature.

c [Key Algorithm]

Select the key algorithm, and specify the key length if [RSA] is selected, or specify the key type if [ECDSA] is selected.

d [Country/Region]

Select the country code from the list, or enter it directly.

e [State]/[City]

Enter the location.

f [Organization]/[Organization Unit]

Enter the organization name.

g [Common Name]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the machine's IP address.
- A DNS server is required in order to enter the FQDN of the machine. Enter the IP address if a DNS server is not used.

h [Issued To (Alternate Name)]

Enter the IP address or domain to be set for the Subject Alternative Name (SAN), as needed.

- If you are not configuring the [Issued To (Alternate Name)] setting, select the [Do Not Set] checkbox.
- Only IPv4 addresses can be set in [IP Address].

7 Click [OK].

➡ The CSR data is displayed.

- If you want to save the CSR data to a file, click [Store in File] and specify the save location.

NOTE

- The key that generated the CSR is displayed on the key and certificate list screen, but you cannot use it by itself. To use this key, you need to register the certificate that is later issued based on the CSR. ➡ **Registering a Certificate to a Key(P. 344)**

Registering a Certificate to a Key

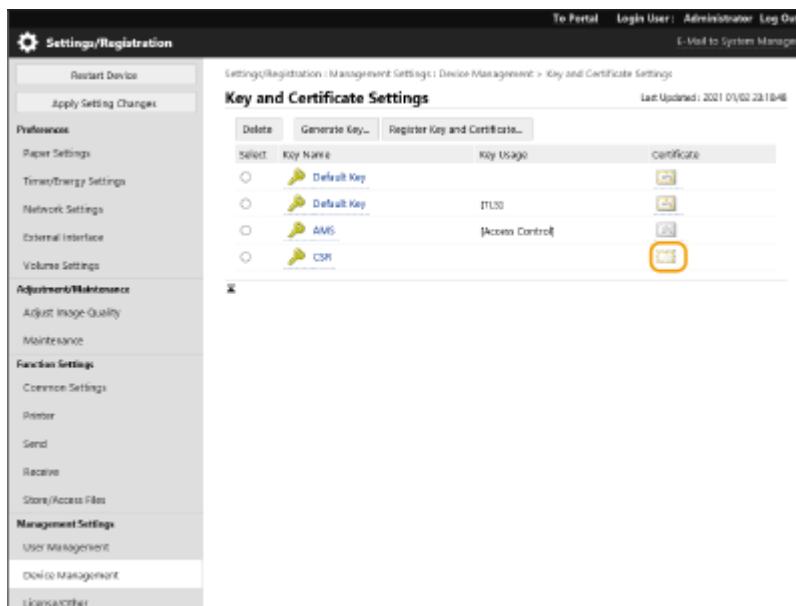
You can register the certificate that was applied for and issued based on the CSR.

1 Start the Remote UI. ➡ **Starting the Remote UI(P. 329)**

2 Click [Settings/Registration] on the portal page. ➡ **Remote UI Screen(P. 331)**

3 Click [Device Management] ▶ **[Key and Certificate Settings].**

4 In the [Certificate] list, click  for the certificate that you want to register.



5 Click [Register Certificate].

6 Register the certificate.

- Click [Choose File], specify the file (certificate) to register, and click [Register].

Retrieving/Updating a Certificate from an SCEP Server

E9SJ-06F

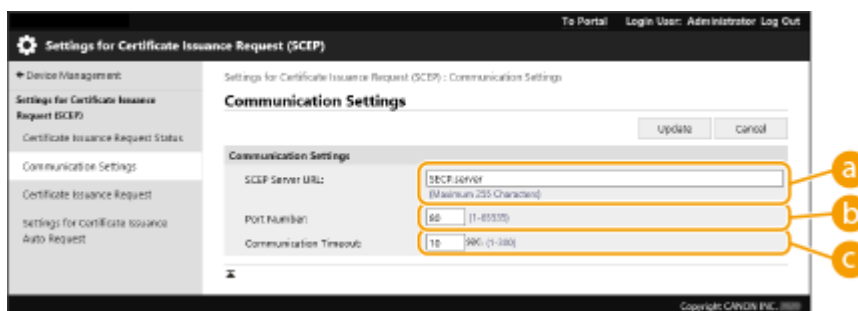
A request for issuing the certificate required for keys generated with the machine can be sent to an SCEP (Simple Certificate Enrollment Protocol) server that manages certificates. Certificates issued from the SCEP server are automatically registered to the machine. Administrator privileges are required to send a request for issuing a certificate.

- ▶ **Specifying the Communication Settings of the SCEP Server(P. 346)**
- ▶ **Requesting a Certificate to Be Issued(P. 347)**
- ▶ **Requesting a Certificate to Be Issued at the Specified Time(P. 348)**
- ▶ **Checking the Status of Requesting a Certificate to Be Issued(P. 350)**

Specifying the Communication Settings of the SCEP Server

You can specify the settings for communicating with the SCEP server.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Settings for Certificate Issuance Request (SCEP)].**
- 4 Click [Communication Settings].**
- 5 Set the required communication settings.**



a [SCEP Server URL:]

Specify the URL of the SCEP server to connect to.

b [Port Number:]

Enter the port number to use for communicating with the SCEP server.

c [Communication Timeout:]

Enter the timeout time for communication with the SCEP server. The connection is canceled if there is no response from the SCEP server within the set time.

- 6 Click [Update].**

NOTE

- The settings cannot be updated when [Enable Timer for Certificate Issuance Auto Request] is selected.
▶Requesting a Certificate to Be Issued at the Specified Time(P. 348)
- For information on the supported versions of SCEP, see **▶Management Functions(P. 602)** .
- Communication using HTTPS is not supported.

Requesting a Certificate to Be Issued

You can manually request a certificate to be issued.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Settings for Certificate Issuance Request (SCEP)].**
- 4 Click [Certificate Issuance Request].**
- 5 Set the items required for requesting a certificate to be issued.**

a [Key Name:]

Enter the name for the key. Enter a name that will be easy to find when displayed in a list.

b [Signature Algorithm:]

Select the hash function to use for the signature.

c [Key Length (bit):]

Select the key length.

d [Organization:]

Enter the organization name.

e [Common Name:]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if a DNS server is not used.

f [Issued To (Alternate Name)]

Enter the IP address or domain to be set for the Subject Alternative Name (SAN), as needed.

- If you are not configuring the [Issued To (Alternate Name)] setting, select the [Do Not Set] checkbox.
- Only IPv4 addresses can be set in [IP Address].

g [Challenge Password:]

When a password is set on the SCEP server side, enter the challenge password included in the request data (PKCS#9) for requesting a certificate to be issued.

h [Key Use Location:]

Select the destination where the key will be used. When [IPSec] is selected, select the IPSec of the destination from the drop-down list.

NOTE:

- When selecting something other than [None], enable the various functions in advance. If a certificate is successfully obtained with the various functions disabled, the certificate is assigned as the destination, but the various functions are not automatically enabled.

6 Click [Send Request].**7 Click [Restart].****NOTE**

- A manual request for issuing a certificate cannot be sent when [Enable Timer for Certificate Issuance Auto Request] is selected. ➤ **Requesting a Certificate to Be Issued at the Specified Time(P. 348)**
- The information set here is not saved to the storage of the machine.

Requesting a Certificate to Be Issued at the Specified Time

You can set to automatically request a certificate to be issued at a specified time.

1 Start the Remote UI. ➤ Starting the Remote UI(P. 329)**2 Click [Settings/Registration] on the portal page. ➤ Remote UI Screen(P. 331)****3 Click [Device Management] ▶ [Settings for Certificate Issuance Request (SCEP)].**

4 Click [Settings for Certificate Issuance Auto Request].

5 Set the items required for requesting a certificate to be issued.

The screenshot shows the 'Settings for Certificate Issuance Auto Request' page. The left sidebar has a menu with 'Settings for Certificate Issuance Auto Request' selected. The main content area has a title bar with 'Update' and 'Cancel' buttons. Below the title bar, there are two main sections:

- Settings for Certificate Issuance Auto Request:**
 - a** ☐ Enable Timer for Certificate Issuance Auto Request. Below it is a 'Request Start Date/Time' field with a date/time picker.
 - b** ☐ Auto Adjust Issuance Request Time.
 - c** ☐ Perform Polling When Communication Error Occurs or When Issuance Request Is Deferred. Below it are 'Polling Repetitions' (set to 3) and 'Polling Interval' (set to 1 sec).
 - d** ☐ Send Periodic Issuance Requests. Below it are 'Request Interval: Every' (set to 6 months) and 'Next Request Date/Time'.
 - e** ☐ Automatically Restart Device After Acquiring Certificate.
 - f** ☐ Delete Old Key and Certificate.
- Settings for Key and Certificate To Be Issued:**
 - g** This section contains fields for 'Key Name', 'Signature Algorithm' (SHA256), 'Key Length (bit)' (RSA2048), 'Organization', 'Common Name', 'Issued To (Alternate Name)' (with radio buttons for 'Do Not Set', 'IP Address', and 'Domain Name'), 'Challenge Password', and 'Key Use Location' (with radio buttons for 'None', 'TLS', 'IEEE 802.1X', and 'IPSec').

a [Enable Timer for Certificate Issuance Auto Request]

Select this to automatically request a certificate to be issued at a specified time, and specify the start date/time in [Request Start Date/Time:].

b [Auto Adjust Issuance Request Time]

Select this to adjust the time to send the request. This reduces load on the SCEP server when multiple printers/multifunction printers send a request at the same time. The time is randomly adjusted 1 to 600 seconds from the time specified in [Request Start Date/Time:].

c [Perform Polling When Communication Error Occurs or When Issuance Request Is Deferred]

Select this to check the status of the SCEP server when a communication error has occurred or when a certificate issue request is pending. Specify the number of polling times and polling interval.

NOTE:

- In the following cases, polling is not performed and an error occurs.
 - When the machine has exceeded the limit of keys and certificates it can hold
 - When an error is included in the retrieved response data
 - When an error occurs on the SCEP server side

d [Send Periodic Issuance Requests]

Select this to periodically send an automatic request for a certificate to be issued, and specify the interval in [Request Interval: Every:].

When an automatic request for a certificate to be issued is performed successfully, the next date/time to issue a request is displayed in [Next Request Date/Time:].

e [Automatically Restart Device After Acquiring Certificate]

Select this to restart the machine after the certificate is retrieved.

! IMPORTANT:

- The machine is restarted even during batch importing/exporting.

f [Delete Old Key and Certificate]

Select this to overwrite the old key and certificate.

NOTE:

- The key and certificate with the same destination for use are overwritten.
- The default key is not overwritten.

g [Settings for Key and Certificate To Be Issued]

Enter the information for the key to generate. For information on the settings, see step 5 of **Requesting a Certificate to Be Issued(P. 347)** .

6 Click [Update].**Checking the Status of Requesting a Certificate to Be Issued**

The certificate requested and issued based on the CSR is registered in the key.



Start the Remote UI ► click [Settings/Registration] ► [Device Management] ► [Settings for Certificate Issuance Request (SCEP)] ► [Certificate Issuance Request Status].

- The following statuses are displayed in [Status].
 - [To Be Processed]: The next date/time to issue a request is displayed in [Request Date/Time].
 - [Processing...]: Polling is being performed.
 - [Error]: An error such as a communication error or key upper limit exceeded error has occurred.
 - [Successful]: The date/time that the certificate was successfully issued is displayed in [Request Date/Time].
- The information displayed in [Details] in [Error] is indicated below.

[Details]	Cause
Deferred	The pending status was returned from the SCEP server.
Key and Certificate Registration Limit Error	The limit to the number of keys and certificates that can be registered in the machine was reached.
Communication Error (TCP ERROR)	Connection to the SCEP server failed/a communication timeout occurred.
Communication Error (HTTP ERROR <CODE>)	An HTTP error occurred.
Communication Error (SCEP ERROR - Fail Info 0: Unrecognized or Unsupported Algorithm)	Unrecognized or unsupported algorithm.

[Details]	Cause
Communication Error (SCEP ERROR - Fail Info 1: CMS Message Integrity Verification Failure)	Integrity check (meaning signature verification of the CMS message) failed.
Communication Error (SCEP ERROR - Fail Info 2: Forbidden or Unsupported Transaction)	Transaction not permitted or supported.
Communication Error (SCEP ERROR - Fail Info 3: Excessive Time Difference Between CMS signingTime and System Time)	The signingTime attribute from the CMS authenticated Attributes was not sufficiently close to the system time.
Communication Error (SCEP ERROR - Fail Info 4: No Certificate Identified That Matches Provided Criteria)	No certificate could be identified matching the provided criteria.

NOTE

- History for the last 20 certificates is displayed. When the number of certificates exceeds 20, the oldest information is overwritten.
- This setting can be imported/exported with models that support batch importing of this setting.  **Importing/Exporting the Setting Data(P. 357)**
- When performing batch exporting, this setting is included in [Settings/Registration Basic Information].  **Importing/Exporting All Settings(P. 359)**

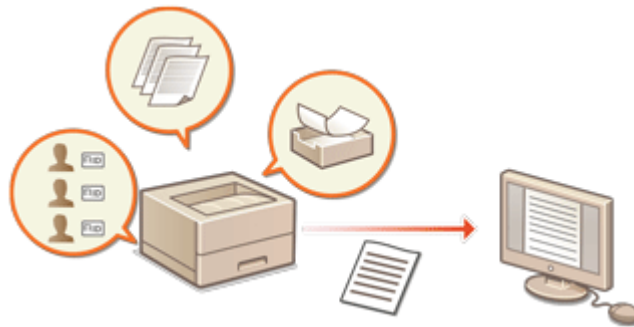
LINKS

-  **Configuring the Key and Certificate for TLS(P. 303)**
-  **Configuring the IEEE 802.1X Authentication Settings(P. 317)**
-  **Configuring the IPSec Settings(P. 310)**

Managing the Logs

E9SJ-06H

You can use the logs to check or analyze how the machine is being used. A variety of information about each operation is recorded in the logs, such as the operation date/time, user name, operation type, function type, and operation result. For more information on the types of logs, see [System Specifications\(P. 598\)](#) . Administrator privileges are required in order to manage the logs.



- ▶ [Starting Log Recording\(P. 352\)](#)
- ▶ [Exporting Logs Automatically\(P. 353\)](#)
- ▶ [Exporting a Log as a File\(P. 354\)](#)
- ▶ [Deleting the Logs\(P. 354\)](#)
- ▶ [Sending Logs via the Syslog Protocol\(P. 355\)](#)

! IMPORTANT

- If Audit Log Collection is enabled and an error occurs in the memory area managed by this function, initialization is automatically performed and then an error screen appears.
- If you can obtain the audit log from before the error occurred, click [Download Audit Log] to obtain the log, and then click [OK].
- If you cannot obtain the audit log from before the error occurred, click [OK].
- When initialization is completed, Audit Log Collection is resumed, and the automatic initialization process is recorded in the log.

Starting Log Recording

Follow the procedure below to start recording logs.



Start the Remote UI ▶ [Settings/Registration] ▶ [Device Management] ▶ [Export/Clear Audit Log] ▶ [Audit Log Information] ▶ Click [Start] for [Audit Log Collection]

NOTE

- If Sleep Mode Energy Use is set to [Low], logs are not collected when the machine enters the Sleep mode.
- When generating a network connection log or machine management log, click [Device Management] ▶ [Save Audit Log] ▶ select the check box for [Save Audit Log] ▶ click [OK] ▶ [Apply Setting Changes].
- If the power of the machine is turned OFF while collecting logs due to a power outage, etc., collection starts again when the machine restarts, from the log that was being collected before the power turned OFF.

- If you stop log collection while logs are being collected, the logs for the period that log collection was stopped are not collected when log collection is next started.

Exporting Logs Automatically

You can set the machine to automatically export audit logs to a specified folder at a predetermined time each day, or when the number of audit logs reaches 95% of the maximum number (approximately 38,000).

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Export/Clear Audit Log] ▶ [Settings for Auto Export Audit Logs].**
- 4 Select the check box for [Use Auto Export] and specify the required settings.**

a [User Name:] / [Password:]

Enter the user name and password necessary for logging into a server to which logs are exported.

b [SMB Server Name:]

Enter the host name of the SMB server to export log files to, along with the path that requires authentication.

- \\Host Name
- \\IP Address\Shared Folder Name

c [Destination Folder Path:]

Enter the path for the folder in which to store the log files.

d [Perform At:]

You can specify the time at which to perform exporting.

- 5 Click [Check Connection], confirm that you can connect, and then click [Update].**

- Audit logs will now be automatically exported. The file extension is ".csv."

NOTE

- After automatic exporting of the audit logs has succeeded, the collected audit logs are automatically deleted. Audit logs cannot be deleted manually.
- After automatic exporting and deleting of the audit logs have succeeded, each log is generated. If other log collections do not occur by the next automatic export time, the audit log will not be automatically exported.
- You can also manually export audit logs from the Remote UI. ➤ **Exporting a Log as a File(P. 354)**
- If automatic exporting fails, the machine will retry multiple times. An error message is displayed on the control panel of the machine if automatic exporting fails even once.
- Specify an SMB server for Windows Server 2012 or later, or Windows 10 or later.
- If the machine is turned OFF, exporting will not be performed, even at the specified time. Also, it will not be performed when the machine recovers.
- If the machine is in the Sleep mode, it will automatically recover and perform exporting at the specified time.
- Note that if you are using a server that does not support SMB 3.0/3.1 encrypted communication, audit log data travels unencrypted across communication paths while it is being automatically exported.
- Depending on your environment, automatic exporting of logs may be performed later than the specified time.

6 Follow the instructions on the screen to specify the location to store the files.

➡ The csv files are stored.

Exporting a Log as a File

The various logs can be exported and saved to a computer as CSV files, which can be opened using a CSV file editor or a text editor.

IMPORTANT

- When exporting logs as files, use TLS or IPsec. ➤ **Configuring the IPsec Settings(P. 310)**



Start the Remote UI ▶ [Settings/Registration] ▶ [Device Management] ▶ [Export/Clear Audit Log] ▶ [Export Audit Logs] ▶ [Export] ▶ Follow the on-screen instructions to save the file

- If you want to automatically delete all logs after they are exported, select the check box for [Delete logs from device after export] before clicking [Export]. If you then click [Cancel], exporting is canceled and the logs are deleted, even if they were not finished being exported as files.
- Log collection is stopped while the export process is being performed.

Deleting the Logs

You can delete all of the collected logs.



Start the Remote UI ▶ [Settings/Registration] ▶ [Device Management] ▶ [Export/Clear Audit Log] ▶ [Delete Audit Logs] ▶ [Delete] ▶ [Yes]

NOTE

- If [Settings for Auto Export Audit Logs] is enabled, you cannot manually delete audit logs.

Sending Logs via the Syslog Protocol

Syslog Information can be sent to an SIEM (security information/event management) system. Linking with an SIEM system enables various information analyzed from realtime alert information to be centrally managed.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Export/Clear Audit Log] ▶ [Syslog Settings].**
- 4 Select [Use Syslog Send], and specify the required settings.**

a [Syslog Server Address:]

Specify the address of the Syslog server to connect to. Enter the necessary information, such as IP address and host name, according to your environment.

b [Syslog Server Port Number:]

Enter the port number used by the Syslog server for Syslog communication. If left blank, the port number defined in RFC (UDP: 514, TCP: 1468, TCP (TLS): 6514) is used.

c [Facility:]

Specify the type of log messages to send. Select one of the following: [Local0] to [Local7], [Log Alert], [Log Audit], [Security Messages], or [LPR] defined in RFC.

d [Connection Type:]

Specify the communication type ([UDP]/[TCP]).

e [Use TLS]

Select this to use TLS to encrypt information communicated with the Syslog server.

NOTE:

- When [TCP] is selected in [Connection Type:], you can set to use TLS.

 [Confirm TLS Certificate]/[Add CN to Verification Items]

Set whether to verify the TLS server certificate sent when connecting and its CN (Common Name).

5 Click [Update].

NOTE

- A slight time lag occurs after the error for some audit logs, because Syslog transmission is performed after polling every 30 seconds.
- The supported RFCs are 5424 (Syslog format), 5425 (TLS), and 5426 (UDP).

LINKS

 **Starting the Remote UI(P. 329)**

 **Configuring the Key and Certificate for TLS(P. 303)**

Importing/Exporting the Setting Data

E9SJ-06J

Machine data such as user setting information and various setting values can be exported and saved to a computer. Exported data can also be imported into the machine from a computer. Data exported from the machine can be imported into other Canon printers/multifunction printers, making it easier to configure the settings on a new machine, such as when you purchase a replacement. For more information on the setting items that can be imported, see **Settings/Registration Table(P. 387)**. When importing or exporting, you can specify whether to import or export all of the machine data, or only particular data.



Importing/Exporting All Settings(P. 359)

! IMPORTANT

Designate an administrator to manage operations

- Designate an administrator with Administrator privileges to perform data import/export operations. When data is imported, user settings, network settings, and other data are overwritten, which may prevent some functions from working properly or cause problems with machine operation. Exercise caution when importing data.

Do not turn OFF the machine until importing or exporting is complete

- It may take several minutes for the process to complete. Do not turn OFF the machine before the process is complete. Doing so may result in data loss or cause the machine to malfunction.
- The following functions/processes cannot be carried out while importing/exporting data:
 - Report print jobs
 - Batch Importing/Batch Exporting
 - Update process for the Register/Update Software function
 - Operating from the control panel of the machine
 - Operating from the Remote UI
 - Putting the machine to the sleep mode
- Importing/exporting data cannot be performed while the following functions/processes are being carried out:
 - Report print jobs
 - Batch Importing/Batch Exporting
 - Update process for the Register/Update Software function
 - Processing the shutdown of the machine
 - Displaying error code

Do not import or export in different display languages

- If the display language differs between the exporting machine and the importing machine, the setting values may corrupt, causing malfunction of the machine.

Do not edit exported files.

- Do not open and edit exported XML files, as this may cause the machine to malfunction.

NOTE

When importing to a Canon printer/multifunction printers other than this machine

- Some settings may not be imported. ▶ **Settings/Registration Table(P. 387)**

When using a password to protect the security policy settings

- The security policy settings can only be imported if the security policy setting password on the exporting machine matches that of the importing machine, or if no password has been set for the importing machine. If no password has been set for the importing machine, the password configured for the exporting machine is set to the importing machine.

Importing/Exporting All Settings

E9SJ-06K

You can export all of the setting data from the machine and save it to a computer, and then import it when configuring the settings on a new machine, such as when you purchase a replacement. If you want to configure the same settings on two or more Canon printers/multifunction printers*, you can simply export all settings from one machine and import them all to the others, eliminating the need to configure each machine separately. To perform these operations, log in to the Remote UI with Administrator privileges.

* Only models that support the import/export of all settings

▶ **Exporting All Settings(P. 359)**

▶ **Importing All Settings(P. 360)**

Exporting All Settings

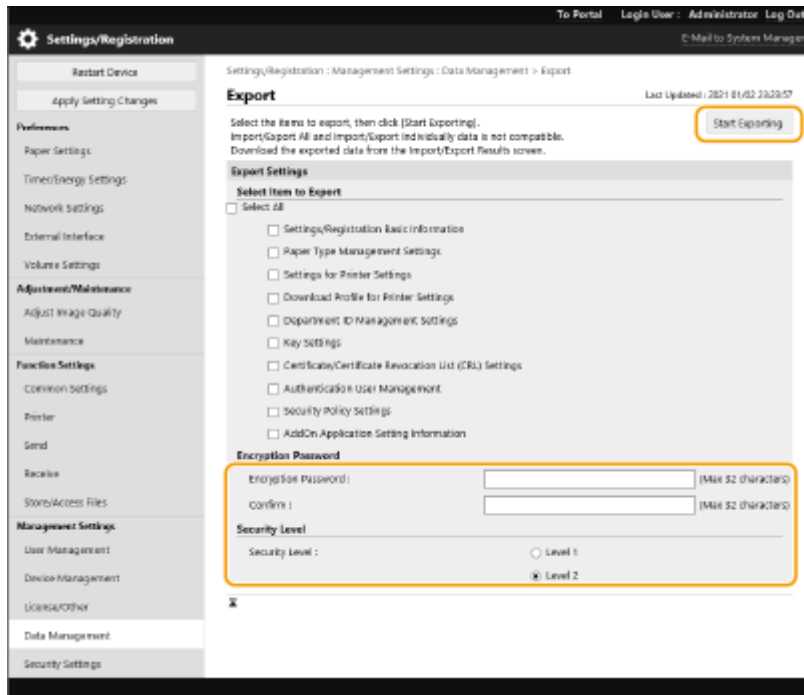
- 1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)**
- 3 Click [Data Management] ▶ [Export].**
- 4 Select the check box for [Select All].**

NOTE:

- Specific items can also be exported. For information on which Settings/Registration items correspond with which items of the batch export function of the Remote UI, see ▶ **Settings/Registration Table(P. 387)** .

- 5 Enter the password in [Encryption Password] ▶ select the security level from [Security Level] ▶ click [Start Exporting] ▶ [OK].**

- The password in [Encryption Password] will be required when importing the exported setting data. Use alphanumeric characters.
- For confirmation, enter the password again in [Confirm].
- To encrypt all the settings data, select [Level 2] in [Security Level].



! IMPORTANT:

- It may take some time for the screen to change. Do not click [Start Exporting] more than once.
- When importing settings data to another model that does not support the setting in [Security Level], select [Level 1].

6 Click [Check Status].

- If the [Cannot be used when exporting.] message is displayed, do not use the Remote UI to perform the operations.

7 Click [Start Downloading].

8 Follow the on-screen instructions to specify where to save the data.

NOTE

To export all setting data without using a computer

- You can export all setting data to memory media such as a USB memory device. ➡<Export to USB Memory>(P. 491)

Importing All Settings

You can import all setting data that was exported to a computer. When importing, the previously configured setting values are overwritten. Note, however, that some machine models may not be able to import all setting items. ➡<Settings/Registration Table>(P. 387)

! IMPORTANT

Check the System Manager information

- When importing the Department ID Management settings to a different printer/multifunctional printer with Department ID Management enabled, the System Manager information is overwritten, which may prevent you from logging in with the previous System Manager ID and PIN. Before performing this operation, make sure to check the System Manager information that is saved on the exporting machine.

NOTE

When applying security policy settings

- The security policy settings can only be imported if the security policy setting password of the exporting machine matches that of the importing machine, or if no password has been set for the importing machine. If no password has been set for the importing machine, the password configured for the exporting machine is automatically set to the importing machine.

1 Start the Remote UI. ▶Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)

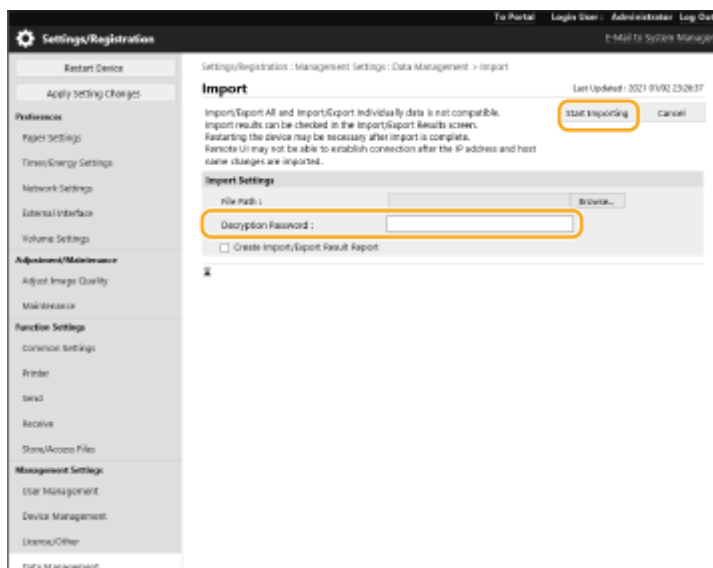
3 Click [Data Management] ▶ [Import].

4 Click [Choose File], and specify the file to import.

5 Enter the password in [Decryption Password], and click [Start Importing] ▶ [OK].

- In [Decryption Password], enter the same password that was entered when the setting data was exported.
- Select the check box for [Create Import/Export Result Report] if you want to output the import results as a CSV file.

➡ The data of the selected file is imported into the machine.



6 Click [OK] ► [Check Status].

- The machine may need to be restarted, depending on the imported data. Click [Perform Restart].
- If you select the check box for [Create Import/Export Result Report] in the previous step, click [Settings/Registration] ► [Data Management] ► [Import/Export Results] ► [Create Report] to export the import results.

NOTE

To import all setting data without using a computer

- You can import all setting data from memory media such as a USB memory device. ►<Import from USB Memory>(P. 491)
- Only one report file is saved. The next time a batch import is executed, the existing report file is deleted.
- Reports are created in the following language.
 - If the display language of the machine is set to Japanese immediately after the import process: Japanese
 - If the display language of the machine is set to something other than Japanese immediately after the import process: English

Updating the Firmware

E9SJ-06L



New firmware is periodically released to add new functions or resolve issues with existing functions. If new firmware is available, follow the procedure below to update it on the machine. Administrator privileges are required in order to update the firmware.

▶ **Checking the Firmware Version(P. 363)**

▶ **Updating the Firmware(P. 364)**

! IMPORTANT

- Do not perform the following operations while updating the firmware. Doing so may cause a critical error.
 - Turn OFF the main power
 - Remove the LAN cable
 - Perform communication (such as printing) with the machine from another computer or application^{*1}
 - Configure the sleep settings of your computer^{*2}

^{*1} When updating the firmware in a network environment, ensure that other users do not perform operations such as printing.

^{*2} The firmware may not be updated correctly if the computer enters the sleep mode.

NOTE

Preparing to update the firmware

- Download the latest firmware from the Canon website (<https://global.canon/>).
- Back up the machine data and settings in case the firmware update is not performed properly.

▶ **Importing/Exporting the Setting Data(P. 357)**

Note regarding the update process

- The machine restarts several times.
- The update process is interrupted if jobs remain.
- The screen switches several times during the update process. It may take some time for the screen to switch, but do not close the browser until the update process is complete.

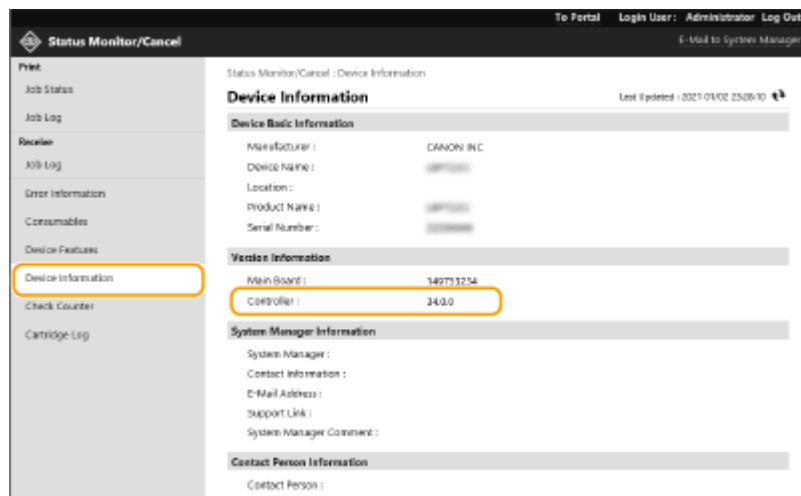
Checking the Firmware Version

Check the firmware version of the machine before updating the firmware and after updating the firmware.

1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)

2 Click [Status Monitor/Cancel] on the portal page. ▶ Remote UI Screen(P. 331)

3 Click [Device Information] ▶ [Version Information] ▶ check [Controller].



Updating the Firmware

1 Start the Remote UI. ▶ Starting the Remote UI(P. 329)

2 Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)

3 Click [License/Other] ▶ [Register/Update Software].

4 Click [Manual Update].

5 Click [Choose File], select the firmware update to use, and click [Update].

➡ When the <The process has stopped because there are one or more unfinished jobs. Restart the device manually in order to start the process. The browser may be closed.> message appears, turn the machine OFF and back ON. ▶ Turning OFF/Restarting the Machine(P. 336)

TIPS

Updating the Firmware from the Home Screen

- Firmware updates can also be performed from <Update Firmware> on the <Home> screen, depending on the region. Administrator privileges are required for this operation.

Updating the Firmware (Distribution)

E9SJ-06R



If the machine has access to the Internet, you can download the latest firmware for the machine from Canon's distribution server. This might be more flexible and convenient than the other update method ([▶Updating the Firmware\(P. 363\)](#)) because both manual and automatic update options are available, enabling you to download the firmware at a specified time or as soon as the latest version is available. Administrator privileges are required in order to perform these operations. You must apply to use this function. For details, contact your dealer or service representative.

NOTE

- This feature may not be available depending on your country or region.

Preparing to update the firmware

- Back up the machine data and settings in case the firmware update is not performed properly.

[▶Importing/Exporting the Setting Data\(P. 357\)](#)

- 1 Start the Remote UI.** [▶Starting the Remote UI\(P. 329\)](#)
- 2 Click [Settings/Registration] on the portal page.** [▶Remote UI Screen\(P. 331\)](#)
- 3 Click [License/Other] ▶ [Register/Update Software].**
- 4 Perform a communication test.**
 - Test whether you can access the distribution server over the network.
 - 1** Click [Display Logs/Communication Test].
 - 2** Click [Communication Test] ▶ [Yes].
 - ▮ The results of the communication test are displayed.
 - If [Could not connect to the distribution server. Check the distribution server and network.] is displayed, check that the LAN cable is connected and the network settings are configured properly. [▶Setting up Using the Setup Guide\(P. 104\)](#)
- 5 Click [Distributed Update] ▶ [Confirm New Firmware].**
- 6 Configure the necessary settings.**

The screenshot shows a firmware update configuration interface. At the top, there is an information box with a blue 'i' icon and text: "Set the distribution settings and click [Execute]. If you set [Distribute now] for the distribution schedule and set [Apply immediately after distribution] for the timing to apply, the applicable firmware will be distributed and updated automatically when the device will restart. [Execute] [Cancel]". Below this, the form is divided into several sections: "Firmware" with fields for "Current Version" (12000002, 1200) and "Applicable Firmware" (62000002, 1200); "Release Note" with a large text area; "Additional Languages" with a "Language Name" field; "Distribution Settings" containing a "Distribution Schedule" section with radio buttons for "Distribute now", "Distribute at specified date and time", and "Apply manually", each with date and time pickers; a "Timing to Apply" section with radio buttons for "Apply immediately after distribution", "Apply manually", and "Apply at specified date and time", also with date and time pickers; an "Updated Module Only" section with radio buttons for "On" and "Off"; an "E-Mail Address" field; and a "Comments" field. Labels a through g are placed to the right of the form, pointing to specific sections: a points to the Firmware section, b to the Release Note, c to the Distribution Schedule, d to the Timing to Apply, e to the Updated Module Only, f to the E-Mail Address, and g to the Comments field.

a [Current Version]/[Applicable Firmware]

You can check the current firmware version and new one respectively.

b [Release Note]

Important information is displayed. Make sure to read and understand the contents.

c [Distribution Schedule]

To download the firmware immediately, select [Distribute now]. To automatically download the firmware at a specified date and time, select [Distribute at specified date and time] and specify the date and time in [Year:]/[Month:]/[Day:]/[Time:]. You can schedule a time within a week in advance.

d [Timing to Apply]

To automatically apply the firmware immediately after downloading is complete, select [Apply immediately after distribution]. To automatically apply the firmware at a specified date and time, select [Apply at specified date and time] and specify the date and time in [Year:]/[Month:]/[Day:]/[Time:]. You can also select [Apply manually] to manually apply the firmware.

e [Updated Module Only]

Select [On] to perform an incremental update (download only the difference between the current and new firmware versions). If you want to download the entire firmware, select [Off]. Note that some firmware versions do not support incremental update.

f [E-Mail Address]

Enter your e-mail address. The distribution server sends the update status to the e-mail address entered here.

g [Comments]

Enter a description or note to add to the e-mail. If you are managing multiple printers/multifunction printers, entering a device name makes it easier to identify the status of each device.

7 Click [Execute] ► [OK].

- If the license agreement screen is displayed, check the information and click [I Accept].
- If [Apply immediately after distribution] or [Apply at specified date and time] is selected in the previous step, the machine automatically restarts immediately after the firmware is applied. If [Apply manually] is selected, you need to apply the downloaded firmware manually. ► **Applying the Downloaded Firmware(P. 367)**

IMPORTANT

- Changing the distributed update settings again may delete the downloaded firmware or cancel the scheduled settings.

NOTE

Canceling the distribution schedule

- On the screen displayed in step 5, click [Delete Scheduled Distribution] ► [Yes].

TIPS

Automatically check for new firmware (scheduled update)

- If you click [Scheduled Update Settings] ► [Edit] in step 5, you can set the machine to periodically access the distribution server for new firmware. If new firmware is available, it is downloaded to update the firmware on the machine.  **Setting Scheduled Updates(P. 368)**

■ Applying the Downloaded Firmware

- 1 Start the Remote UI.**  **Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page.**  **Remote UI Screen(P. 331)**
- 3 Click [License/Other] ► [Register/Update Software].**
- 4 Click [Distributed Update] ► [Apply Firmware] ► [OK].**

- The machine automatically restarts immediately after the firmware is applied.

NOTE:

To delete the firmware

- Click [Delete Firmware] ► [OK].

Setting Scheduled Updates

E9SJ-06S



You can set the machine to regularly check for new applicable firmware and automatically update the firmware of the machine.

NOTE

- This operation can only be performed by a user with the required privileges.
- If the downloading of the firmware is not complete, or the downloaded firmware has not been applied, you cannot perform a scheduled update.

- 1 Start the Remote UI.** ▶ Starting the Remote UI(P. 329)
- 2 Click [Settings/Registration] on the portal page.** ▶ Remote UI Screen(P. 331)
- 3 Click [License/Other] ▶ [Register/Update Software].**
- 4 Click [Scheduled Update Settings] ▶ [Edit...].**
- 5 Select the check box for [Enable scheduled update settings], and configure the necessary settings.**

Scheduled Update Settings

☒ Enable scheduled update settings

Update Schedule * It may take up to 3 hours to finish checking for updates.

confirm: Biweekly | Not Set | Not Set | 00

apply at: Not Set | 00 * updates are applied after confirmation and downloading are complete.

E-Mail:

Comments:

* If you consent that your email address is transferred to Canon Inc. in Japan to receive notices, please register.

a [Update Schedule]

[Confirm]

Select the cycle ([Biweekly] or [Weekly], a day ([Sun] to [Sat]), and the time). The time is displayed in 24-hour notation. The firmware check may take up to 3 hours to complete from the specified time.

[Apply at]

Select the time to apply downloaded firmware.

b [E-Mail]

Enter the e-mail address of the administrator. You can receive e-mails regarding the update status that is sent from the distribution server.

[Comments]

Enter the comment that will automatically be added to the e-mail. If the model name is entered, you can identify which device status the e-mail is about.

NOTE

- If previously downloaded firmware has not been applied by scheduled update, the next scheduled update is not performed.
- If Scheduled Update is set, a firmware update is applied at the specified time after the new firmware is downloaded from the distribution server. After application is complete, the machine automatically restarts.

6 Click **[Set]**.

Displaying Messages from the Administrator

E9SJ-06U



You can display messages to users on the portal page of the Remote UI. Administrator privileges are required in order to configure these settings.

- 1** Start the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2** Click [Settings/Registration] on the portal page. ▶ Remote UI Screen(P. 331)
- 3** Click [License/Other] ▶ [Message Board/Support Link].
- 4** Enter the message, and click [OK].

a [Message]

Enter the content of the message. Use this setting for displaying operational tips and other low-priority messages.

b [Remote UI]

Select this check box to display the message on the portal page of the Remote UI.

c [Support Link]

Enter the link to support information for the machine to display on the portal page of the Remote UI.

Setting the Website for Purchasing Consumables

E9SJ-06W

You can set a link to the website for purchasing consumables, which is displayed when checking consumables information from the Remote UI. Setting a link to the website makes it easier for users to purchase consumables.

- 1 Start the Remote UI. ▶Starting the Remote UI(P. 329)**
- 2 Click [Settings/Registration] on the portal page. ▶Remote UI Screen(P. 331)**
- 3 Click [Device Management] ▶ [Information for Purchasing Consumables].**
- 4 Specify settings as necessary.**

- a [Supplier]**
Set the name of the place for purchasing consumables.
- b [E-Mail Address]**
Set the e-mail address of the place for purchasing consumables.
- c [URL]**
Set the URL of the website for purchasing consumables.
- d [Display Consumables Purchase Button]**
Select this to display a button for accessing the website for purchasing toner cartridges on the Remote UI.
- e [Use Toner Status]**
Select this when using the toner cartridge level notification tool.
- f [Display Consumables Purchase Button When Using Toner Status]**
Select this to display a button for accessing the website for purchasing toner cartridges on the toner cartridge level notification tool.

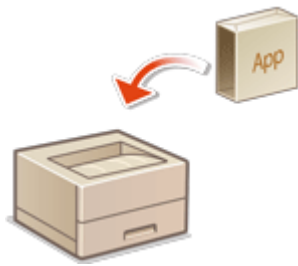
- 5 Click [OK].**

NOTE

- This setting can only be specified by a user with Administrator privileges.
- This setting can only be imported from/exported to the same series machines.  **Importing/Exporting the Setting Data(P. 357)**
- This setting is included in [Settings/Registration Basic Information] when batch exporting.  **Importing/Exporting All Settings(P. 359)**

Installing System Options

E9SJ-06X



When using system options, you may need to log in with Administrator privileges to register licenses. To register a license, you will need the number that is printed on the license access number certificate. Make sure you have it with you before you start. You can perform license registration even if the machine is not connected to the network.

1 Perform a communication test.

- Test whether you can register the license over the network.

1 Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)

2 Click [Settings/Registration] on the portal page. [▶Remote UI Screen\(P. 331\)](#)

3 Click [License/Other] ▶ [Register/Update Software] ▶ [Display Logs/Communication Test].

4 Click [Communication Test].

⇒ The [Are you sure you want to execute the communication test?] message is displayed.

5 Click [Yes].

⇒ The results of the communication test are displayed.

- If [Connect Failed] is displayed, check that the LAN cable is connected and the network settings are configured properly. [▶Setting up Using the Setup Guide\(P. 104\)](#)
- If you cannot connect to the network, register the license offline. [▶When Registration Cannot Be Performed over the Network\(P. 374\)](#)

2 Click [Distributed Installation].

3 Enter the license access number.

4 Confirm the number, and click [Next >].

5 Select the function to install, and click [Start].

- If the license agreement screen is displayed, check the information and click [I Accept].

6 Click [To Distributed Installation].

■ When Registration Cannot Be Performed over the Network

If for some reason the machine is unable to connect to the network, register the license offline. First obtain a license key using a computer connected to the network, then register it by entering it into the machine. To obtain a license key, you will need the number that is printed on the license access number certificate, along with the serial number of the machine.

1 Access the license issuing website (<http://www.canon.com/lms/license/>) and obtain the license key.

- Follow the on-screen instructions and enter the license access number and serial number to obtain the license key.

2 Select <Set> on the <Home> screen.

3 Select <Management Settings> ► <License/Other> ► <Register License>.

4 Enter the license key.

5 Select <Start>.

NOTE

Confirming the serial number

- It is displayed in <Check Counter> ► <Check Device Configuration>. It can also be confirmed from the Remote UI portal page.

Managing Storage Device Data

E9SJ-06Y



The storage of the machine contains data such as undeleted job data and password information. By encrypting this data, you can prevent the information from being accessed without authorization.

▶ Initializing Settings(P. 376)

! IMPORTANT

- Encrypting the data in the Storage does not guarantee that the data is protected from all unauthorized acts. Take sufficient care when managing data.

NOTE

- For encryption, the machine uses an AES algorithm in accordance with FIPS PUB 197.

Initializing Settings

E9SJ-070



You can initialize the settings to the factory default values. Administrator privileges are required in order to perform initialization.

- ▶ **Initializing the Network Settings(P. 376)**
- ▶ **Initializing the Panel Settings(P. 376)**
- ▶ **Initializing All Data/Settings(P. 377)**

! IMPORTANT

- Before initializing, make sure that there are no documents being processed or waiting to be processed. These documents will be deleted when initialization is performed.
- Do not turn OFF the machine during initialization. Doing so may lead to defects in the memory of the machine.
- Initialization may take 30 minutes or more to complete. The machine cannot be used during the initialization process.

NOTE

Before performing initialization

Back up your important data or export it as a file.

- Machine setting information ▶ **Importing/Exporting the Setting Data(P. 357)**
- User authentication information registered in the local device for personal authentication management ▶ **Registering User Information in the Local Device(P. 246)**

When using a password to protect the security policy settings

- Password entry is required to execute <Initialize All Set. without Network Set.> or <Initialize All Data/Settings>. ▶ **Using a Password to Protect the Security Policy Settings(P. 232)**

Initializing the Network Settings

You can initialize the network settings to the factory default values.



<Set> ▶ <Management Settings> ▶ <Data Management> ▶ <Initialize Network Settings> ▶ <Yes>

Initializing the Panel Settings

You can initialize the various settings to the factory default values.



<Set> ▶ <Management Settings> ▶ <Data Management> ▶ <Initialize All Set. without Network Set.> ▶ <Yes>

NOTE

- The network settings are not initialized.

Initializing All Data/Settings

You can restore all of the machine settings to the factory default values. After initialization is complete, the Initialize All Data/Settings Report is printed.



<Set> ▶ <Management Settings> ▶ <Data Management> ▶ <Initialize All Data/Settings> ▶ <Yes>
 ▶ After initialization is complete, press the power switch to turn the power OFF (▶ **Turning OFF the Machine(P. 30)**), wait for longer than 10 seconds, and then turn the power ON again (▶ **Turning ON the Machine(P. 29)**).

NOTE

- Although the job log information can be deleted by initializing all data/settings, the result of printing the Initialize All Data/Settings Report is recorded in the print log. ▶ **Checking the Printing Status and History(P. 175)**

TIPS

- It is also possible to individually select some machine settings and restore their factory default values. ▶ **Settings/Registration(P. 386)**

Checking the Number of Pages for Print

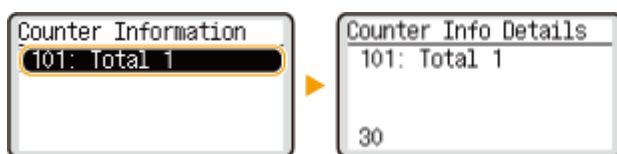
E9SJ-071

You can check the total number of pages that have been printed. The number of printouts includes printouts of the memory media print and the list as well as printouts of data from computers.

1 Select **<Check Counter>** on the **<Home>** screen.  **<Home> Screen(P. 150)**

2 Select **<Counter Information>**.

3 Check the total number of printed pages.



<101: Total 1>

Displays the total number of pages for printing.

NOTE

- You can print a list that shows the number of pages used for printing.
 **Output Report(P. 444)**  **<Counter Report>**
- For information on the count conditions, contact your dealer or service representative.

Printing Reports and Lists

E9SJ-072

You can print reports and lists of several types of information, such as consumable status, print history, and settings.

For more information on the reports and lists, see  **<Output Report>(P. 495)** and  **Output Report(P. 444)** .

Paper Type Management Settings

E9SJ-073

You can register and edit detailed information of frequently used paper types as the [Custom Type].

To register a new paper type, first duplicate the paper type that resembles the new type in order to copy all of the internal operational parameters. This procedure copies the suitable settings to the new paper type from the registered custom paper easily.

You can also improve printing quality and paper feeding trouble by editing the custom paper, depending on the characteristics.

NOTE

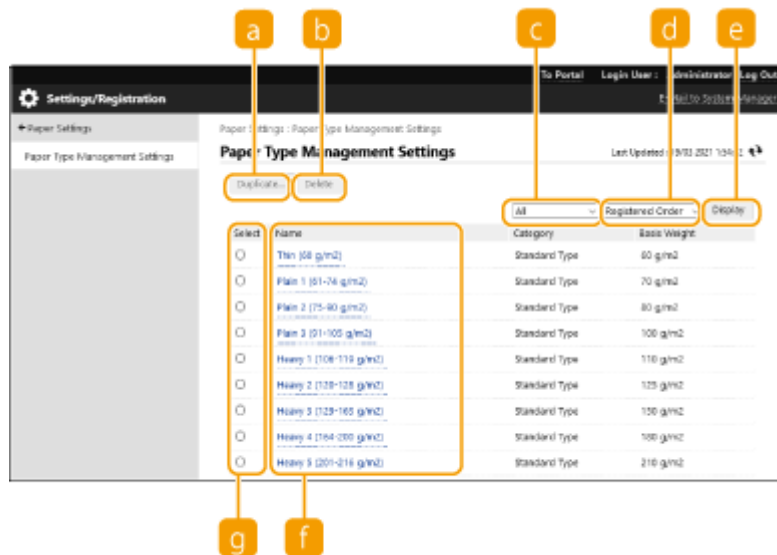
- It is necessary to log in as an administrator to register custom paper types or change the settings of registered custom paper types. [▶Logging into the Machine\(P. 159\)](#)
- When you register the custom paper type, you cannot specify the paper source. For more information on registering the paper source, see [▶Specifying Paper Size and Type in the Paper Drawer\(P. 52\)](#) .
- You can import/export the registered custom paper type information, and share it with another Canon machine. [▶Importing/Exporting All Settings\(P. 359\)](#)

[▶Registering frequently used paper types\(P. 380\)](#)

[▶Items that can be specified\(P. 382\)](#)

Registering frequently used paper types

- 1** Start the Remote UI. [▶Starting the Remote UI\(P. 329\)](#)
- 2** Click [Settings/Registration] on the Portal page. [▶Remote UI Screen\(P. 331\)](#)
- 3** Click [Paper Settings] ▶ [Paper Type Management Settings].
- 4** Select the paper type to edit.



a [Duplicate]

Duplicates the paper type selected in [Select] as a custom paper type.

b [Delete]

Deletes the paper type selected in [Select].

! IMPORTANT:

- Only paper types with [Custom Type] displayed for [Category] can be deleted.

c Paper type drop-down list

Enables you to select the paper type to display.

d Sort List By

Enables you to change the display order of the list.

e [Display]

Switches the list display to the items selected in **c** and **d**.

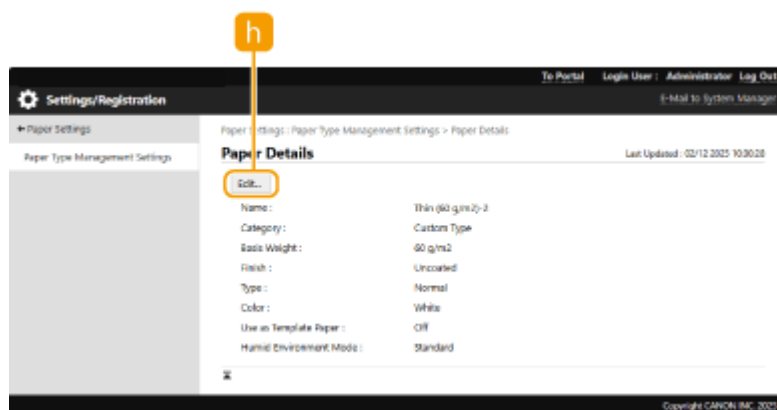
f [Name]

Displays [Paper Details] when you click the paper type displayed in [Name]. If you select a custom paper type, you can edit it.

g [Select]

Select a paper type to duplicate or delete.

5 Select [Edit] and configure the various settings.



 [Edit]

Appears on the [Paper Details] screen for the custom paper type and enables you to change the settings for the selected item.

 IMPORTANT:

- Only paper types with [Custom Type] displayed for [Category] can be edited.

6 Click [OK] .**Items that can be specified**

The following items can be specified.

■ [Name]

You can change the name of the custom paper type.

NOTE

- When you register the settings for the custom paper type, make sure to change its name. You cannot change the settings of the default paper types registered in the machine.

■ [Basis Weight]

You can change the basis weight of the custom paper type.

 IMPORTANT

- If you enter a value that is different from the actual weight of the set paper, paper jams may occur, and the quality of the image may be adversely affected.

■ [Finish]

You can change the Finish setting of Custom Type you have registered.

 IMPORTANT

- If you select a finishing type which is different from that of the loaded paper, paper jams may occur, and the quality of the image may be adversely affected.

■ [Type]

You can change the Type setting of Custom Type you have registered.

IMPORTANT

- If you select a paper type which is different from that of the loaded paper, paper jams may occur, and the quality of the image may be adversely affected.

■ [Color]

You can change the color of the custom paper type.

IMPORTANT

- If you select a color which is different from that of the loaded paper, paper jams may occur, and the quality of the image may be adversely affected.

■ [Use as Template Paper]

You can select [Use as Template Paper] to use preprinted paper (paper which has logos already printed on it), such as a letterhead.

NOTE

- Methods for loading paper if [Use as Template Paper] is selected:
 - Paper source other than the multi-purpose tray: the side with a logo facing down
 - Multi-purpose tray: the side with a logo facing up

■ [Humid Environment Mode]

Print problems may occur due to humidity in the environment of the machine. This setting may improve this problem.

NOTE

- Set this in the following cases. The print results may be improved.
 - [High Humidity]: Set this if the print density is light or irregular when using the machine in a high humidity environment.
 - [Low Humidity 1]: Set this if images and text are blurred when using the machine in a low humidity environment.
 - [Low Humidity 2]: Set this if images show toner scattering or shaded parts of the image have white patches (areas left white) when using the machine in a low humidity environment.
- Set [Standard] to not use either setting.

Settings/Registration

Settings/Registration	386
Settings/Registration Table	387
Preferences	389
Display Settings	390
Timer/Energy Settings	391
Network	393
External Interface	412
Accessibility	413
Volume Settings	414
Adjustment/Maintenance	415
Adjust Image Quality	416
Maintenance	418
Function Settings	419
Common	420
Printer	422
Custom Settings	423
UFR II	425
PCL	426
PS	428
Imaging	429
PDF	430
XPS	431
Utility	432
Send	433
Receive	434
Access Files	435
Print	437
Management Settings	438
User Management	439
Device Management	440
License/Other	441
Data Management	442
Security Settings	443
Output Report	444
<Preferences>	445
<Display Settings>	446
<Timer/Energy Settings>	448

<Network>	452
<External Interface>	465
<Accessibility>	467
<Volume Settings>	468
<Adjustment/Maintenance>	469
<Adjust Image Quality>	470
<Maintenance>	474
<Function Settings>	475
<Common>	476
<Printer>	479
<Send>	481
<Receive>	482
<Access Files>	483
<Print>	484
<Management Settings>	485
<User Management>	486
<Device Management>	487
<License/Other>	489
<Data Management>	491
<Security Settings>	493
<Output Report>	495

Settings/Registration

E9SJ-074

You can customize the machine based on your environment and needs by configuring settings described in this chapter. The Settings/Registration screen is displayed by selecting <Set> on the <Home> screen.

This section describes what each item in the setting menu can configure.

NOTE

- Some of the settings may not be displayed depending on the configuration of optional equipment installed on the machine.
- Some changes may not be reflected immediately, depending on the settings. In this case, it is necessary to perform one of the following.
 - Select <Yes> on the screen confirming whether you want to make changes.
 - Select <Apply Set. Changes> on the <Home> screen.
 - Restart the machine.

Settings/Registration Table

E9SJ-075

The following settings can be selected or stored on the Settings/Registration screen:

- ▶ Preferences(P. 389)
- ▶ Adjustment/Maintenance(P. 415)
- ▶ Function Settings(P. 419)
- ▶ Management Settings(P. 438)
- ▶ Output Report(P. 444)

NOTE

- Some of the settings may not be displayed depending on the configuration of optional equipment installed on the machine.
- Some changes may not be reflected immediately, depending on the settings. In this case, it is necessary to perform one of the following.
 - Select <Yes> on the screen confirming whether you want to make changes.
 - Select <Apply Set. Changes> on the <Home> screen.
 - Restart the machine.
- The settings that can be specified differ between administrators and general users, and vary depending on restrictions imposed by the administrator.

■ Description of the Settings

Describes the functions of each setting item on Settings/Registration. The settings that can be operated vary depending on the user authority and the machine you use. Setting items and values are written under Setting Description. The factory defaults are written in **bold red characters**.

■ "Can be set in Remote UI"

The "Can be set in Remote UI" item is written for each item in the Settings/Registration table. "Yes" or "No" indicates if the settings can/cannot be set in the Remote UI.

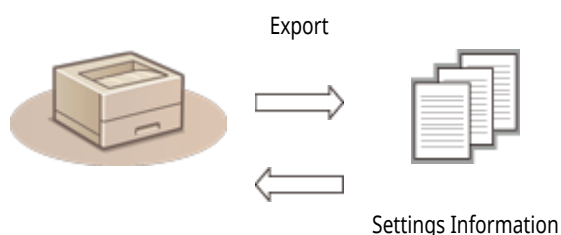
■ Import All Function

The "Import All Function" item is written in the Settings/Registration table. Depending on whether a setting item can be batch imported, "A", "B", "C", or "No" is written. "A", "B", and "C" refer to the following cases.

Case A

Importing all to your machine

Restoring the settings information to your machine for backups.



Import

Case B

Importing all to the same model machine

Applies to machines of the same series as this machine.



Case C

Importing all to the different model machine

Applies to models that support batch importing.



■ Name of Item When Exporting with the Remote UI

This section indicates which Settings/Registration items correspond with which items of the batch export function of the Remote UI. "-" is indicated for items that are not imported/exported. [▶Importing/Exporting All Settings\(P. 359\)](#)

The items that can be selected for the batch export function of the Remote UI are indicated below.

Items That Can Be Selected with the Batch Export Function
Settings/Registration Basic Information
Paper Type Management Settings
Settings for Printer Settings
Download Profile for Printer Settings
Department ID Management Settings
Key Settings
Certificate/Certificate Revocation List (CRL) Settings
Authentication User Management
Security Policy Settings
MEAP Application Setting Information

Preferences

E9SJ-076

- ▶ **Display Settings**(P. 390)
- ▶ **Timer/Energy Settings**(P. 391)
- ▶ **Network**(P. 393)
- ▶ **External Interface**(P. 412)
- ▶ **Accessibility**(P. 413)
- ▶ **Volume Settings**(P. 414)

NOTE

- Some items can be set using the Remote UI. Use the control panel of the device to set items which cannot be set using the Remote UI.
- The names may be different on the Remote UI.

Display Settings

E9SJ-077

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Button Display Order on Home Screen>	<Select Button to Move> <Set>, <Paper Settings>, <Memory Media>, <Print>, <Mobile Portal>, <Display Order (Home)>, <Update Firmware>	No	C	Settings/Registration Basic Information
<Default Screen After Startup/Restoration>	<Home>, <Memory Media Print>, <Print>, <Status Monitor>	No	C	Settings/Registration Basic Information
<Language>	<Bahasa Melayu>, <Català>, <Čeština>, <Dansk>, <Deutsch>, <Eesti>, <English>, <Español>, <Euskara>, <Français>, <Hrvatski>, <Italiano>, <Latviešu>, <Lietuvių>, <Magyar>, <Nederlands>, <Norsk>, <Polski>, <Português>, <Română>, <Slovenčina>, <Slovenščina>, <Suomi>, <Svenska>, <Tiếng Việt Nam>, <Türkçe>, <Ελληνικά>, <български>, <Русский>, <Українська>, <الْعَرَبِيَّةُ>, <ภาษาไทย>, <日本語>, <中文（繁體）>, <中文（简体）>, <한국어>	No	C	Settings/Registration Basic Information
<Millimeter/Inch Entry Switch>	<Millimeter>, <Inch>	No	C	Settings/Registration Basic Information
<Confirm When Loading Paper in Drawer>	<Off>, <On>	No	B	Settings/Registration Basic Information
<IP Address Display Settings>	<Off>, <On>	No	C	Settings/Registration Basic Information
<Display Icon Showing Remaining Toner>	<Off>, <On>	No	C	Settings/Registration Basic Information
<Display Mobile Portal>	<Off>, <On>	No	C	Settings/Registration Basic Information
<Timing of Toner Cart. Replacement Notif.>	<Default>, <Custom> When <Custom> is selected: <Specify Toner Level>: 2 to 20 to 99%	No	B	Settings/Registration Basic Information

Timer/Energy Settings

E9SJ-078

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Date/Time Settings>	<Current Date/Time Settings>: Date and Time Setting (12-digit number)	Yes	No	Settings/Registration Basic Information
	<Time Zone>: UTC-12:00 to UTC+08:00 to UTC+14:00	Yes	C	Settings/Registration Basic Information
	<Daylight Saving Time Settings>:<Off>, <On> When <On> is selected: <Month>, <Day>, <Time>	Yes	C	Settings/Registration Basic Information
<Time Format>	<12 Hour>, < 24 Hour >	Yes	C	Settings/Registration Basic Information
<Quick Startup Settings for Main Power>	<Off>, < On >	Yes	C	Settings/Registration Basic Information
<Auto Reset Time>	0 min=Off, 10 to 50 seconds in 10 second increments, 1 to 2 to 9 minutes in one minute increments	Yes	C	Settings/Registration Basic Information
<Restrict Auto Reset Time>	< Off >, <On>	Yes	C	Settings/Registration Basic Information
<Function After Auto Reset>	< Default Function >, <Selected Function>	Yes	C	Settings/Registration Basic Information
<Auto Shutdown Time>	0 hr =Off, 1 to 8 hours in one hour increments	Yes	C	Settings/Registration Basic Information
<Auto Shutdown Weekly Timer>	<Sunday> to <Saturday>, 00:00 to 23:59, in one minute increments	Yes	C	Settings/Registration Basic Information
<Allow Sleep Mode During Error>	<Off>, < On >	Yes	C	Settings/Registration Basic Information
<Auto Sleep Time>	10 secs, 1 min , 2 mins, 10 mins, 15 mins, 20 mins, 30 mins, 40 mins, 50 mins, 1 hr, 90 mins, 2 hrs	Yes	C	Settings/Registration Basic Information
<Sleep Mode Energy Use>	< Low >, <High>	Yes	C	Settings/Registration Basic Information
<Settings for Sleep Mode Exit upon Job RX>	< Do Not Turn Device Control Panel On >, <Turn Device Control Panel On>	Yes	C	Settings/Registration Basic Information
<Auto Sleep Weekly Timer>	<Sunday> to <Saturday>, 00:00 to 23:59, in one minute increments	Yes	C	Settings/Registration Basic Information

Settings/Registration

<Sleep Mode Exit Time Settings>	<Off>, <On> When <On> is selected:00:00 to 23:59, in one minute increments	Yes	C	Settings/Registration Basic Information
---------------------------------	---	-----	---	---

Network

E9SJ-079

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

- <Output Report> *1

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Output Report>	<Print>	Yes	No	-

*1 This setting can only be specified from the Remote UI.

- <Confirm Network Connection>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Confirm Network Connection>	<Off>, <On>	No	C	Settings/Registration Basic Information

- <TCP/IP Settings>: <IPv4 Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use IPv4>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<IP Address Settings>	<Auto Acquire> <Select Protocol>: <Off>, <DHCP> <Auto IP>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Manually Acquire> <IP Address>: Enter the IP address. <Subnet Mask>: Enter the IP address. <Gateway Address>: Enter the IP address.	Yes	C	Settings/Registration Basic Information
	<Check Settings> <IP Address>: Display only <Subnet Mask>: Display only <Gateway Address>: Display only	Yes	C*2	Settings/Registration Basic Information
<DHCP Option Settings>	<Acquire Host Name>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<DNS Dynamic Update>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Acquire DNS Server Address>: <Off>, <On>	Yes	C	Settings/Registration Basic Information

Settings/Registration

	<Acquire Domain Name>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Acquire POP Server Address>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Release Address Last Acquired from DHCP Server When Address Cannot Be Acquired>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<DNS Settings>*1	<Host Name>: Canon ***** ("*****" represents the last six digits of a MAC address.)	Yes	A	Settings/Registration Basic Information
	<Domain Name>: Enter the domain name.	Yes	A	Settings/Registration Basic Information
	<Perform DNS Dynamic Update>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<PING Command>	<PING Command>: <0.0.0.0>	No	No	-

*1 This setting can only be specified from the Remote UI.

*2 <IP Address> is categorized as "A".

● <TCP/IP Settings>: <IPv6 Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use IPv6>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Use Stateless Address>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Use Manual Address>*1: <Off>, <On> ● When <On> is selected: <IP Address>(IPv6 Address (39 characters maximum)) <Prefix Length>: 1 to 64 to 128 <Default Router Address> (39 characters maximum)	Yes	A	Settings/Registration Basic Information
	<Use DHCPv6>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<Only Retrieve Stateful Address Prefix>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<DHCP Option Settings>	<Acquire DNS Server Address>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Acquire Domain Name>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<DNS Settings>*1	<Primary DNS Server Address>	Yes	C	Settings/Registration Basic Information
	<Secondary DNS Server Address>	Yes	C	Settings/Registration Basic Information

Settings/Registration

	<Use Same Host Name/Domain Name as IPv4>: <Off>, <On>	Yes	A	Settings/Registration Basic Information
	<Host Name>: Canon ***** ("*****" represents the last six digits of a MAC address.)	Yes	A	Settings/Registration Basic Information
	<Domain Name>: Enter the domain name.	Yes	A	Settings/Registration Basic Information
	<Perform DNS Dynamic Update>: <Off>, <On> • When <On> is selected: <Register Stateless Address>: <Off>, <On> <Register Manual Address>: <Off>, <On> <Register Stateful Address>: <Off>, <On>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <TCP/IP Settings>: <DNS Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<DNS Server Address Settings>	<Primary DNS Server>: Enter the IP address.	Yes	C	Settings/Registration Basic Information
	<Secondary DNS Server>: Enter the IP address.	Yes	C	Settings/Registration Basic Information
<mDNS Settings>	<Use IPv4 mDNS>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• When <On> is selected: <mDNS Name> (63 characters maximum)	Yes	C	Settings/Registration Basic Information
	<Use IPv6 mDNS>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• When <On> is selected: <Use IPv4 Name for mDNS>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• When <Off> is selected: <mDNS Name> (63 characters maximum)	Yes	C	Settings/Registration Basic Information

• <TCP/IP Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<LPD Print Settings>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	• When <On> is selected: <Output LPD Banner Page>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<RX Timeout>*1: 1 to 5 to 60 (min.)	Yes	C	Settings/Registration Basic Information

Settings/Registration

<RAW Print Settings>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Bidirectional Comm.>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<RX Timeout>*1: 1 to 5 to 60 (min.)	Yes	C	Settings/Registration Basic Information
<SNTP Settings>	<Use SNTP>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Polling Interval>*1: 10 to 1440 to 2880 min.	Yes	C	Settings/Registration Basic Information
	<NTP Server Address>*1: (IP Address or Host Name)	Yes	C	Settings/Registration Basic Information
<FTP Print Settings>	<Use FTP Printing>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<User Name>: guest	Yes	C	Settings/Registration Basic Information
	<Password>: 7654321	Yes	C	Settings/Registration Basic Information
<Use UTF-8 to Display FTP Print Job Name>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<WSD Settings>	<Use WSD Print>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Use WSD Browsing>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<IPP Print Settings>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Allow When Using TLS>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Use Authentication>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<Multicast Discovery Settings>	<Response>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Scope Name>	Yes	C	Settings/Registration Basic Information
<Sleep Mode Notification Settings>*1	<Notify>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Port Number>: 1 to 11427 to 65535	Yes	C	Settings/Registration Basic Information
	<Number of Routers to Traverse>: 0 to 3 to 254	Yes	C	Settings/Registration Basic Information
	<Notification Interval>: 60 to 600 to 65535 sec.	Yes	C	Settings/Registration Basic Information

Settings/Registration

<Use HTTP>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<TLS Settings>*1				
<Key and Certificate Settings>	<Use>	Yes	No	-
	<Certificate Details> (<Version>, <Serial Number>, <Signature Algorithm>, <Issued To>, <Validity Start Date>, <Validity End Date>, <Issuer>, <Public Key>, <Certificate Thumbprint>, <Issued To (Alternate Name)>, <Verify Certificate>)	Yes	No	-
	<Key Usage> (Displays what the key pair is being used for)	Yes	No	-
<Specify Allowed Versions>	<Maximum Version>: <TLS 1.0>, <TLS 1.1>, <TLS 1.2>, <TLS 1.3>	Yes	C	Settings/Registration Basic Information
	<Minimum Version>: <TLS 1.0>, <TLS 1.1>, <TLS 1.2>, <TLS 1.3>	Yes	C	Settings/Registration Basic Information
<Algorithm Settings>	Encryption Algorithm <AES-CBC (256-bit)>: <Off>, <On> <AES-CBC (128-bit)>: <Off>, <On> <AES-GCM (256-bit)>: <Off>, <On> <AES-GCM (128-bit)>: <Off>, <On> <3DES-CBC>: <Off>, <On> <CHACHA20-POLY1305>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	Key Exchange Algorithm <RSA>: <Off>, <On> <ECDHE>: <Off>, <On> <X25519>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	Signature Algorithm <RSA>: <Off>, <On> <ECDSA>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	HMAC Algorithm <SHA1>: <Off>, <On> <SHA256>: <Off>, <On> <SHA384>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<Proxy Settings>	<Use Proxy>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Server Address> (IP Address or FQDN)	Yes	C	Settings/Registration Basic Information
	<Port Number>: 1 to 80 to 65535	Yes	C	Settings/Registration Basic Information
	<Proxy withn Same Domain>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Authentication Set.>: <Use Proxy Auth.>(<Off>, <On>), <User Name> (128 characters maximum), <Password> (128 characters maximum)	Yes	C	Settings/Registration Basic Information

Settings/Registration

<Confirm Auth Info When in Auth Mngt Mode>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
--	-------------	-----	---	---

*1 This setting can only be specified from the Remote UI.

• <TCP/IP Settings>: <IPSec Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use IPSec>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Receive Non-Policy Packets>*1	<Allow>, <Reject>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <TCP/IP Settings>: <IPSec Settings>: <IPSec Policy List>*1

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<IPSec Policy List>	<Register New IPSec Policy>, <Delete>, <Raise Priority>, <Lower Priority>	Yes	C	Settings/Registration Basic Information
<Register Policy>	<Policy Name> (24 characters maximum), <Policy On/Off> (<Off>, <On>), <Only Allow 256-bit for AES Key Length> (<Off>, <On>), <Selector Settings>, <IKE Settings>, <IPSec Network Settings>	Yes	C	Settings/Registration Basic Information
<Selector>	<Local Address Settings> (<All IP Addresses>, <IPv4 Address>, <IPv6 Address>, <IPv4 Manual Settings>, <IPv6 Manual Settings>)	Yes	C	Settings/Registration Basic Information
	• <IPv4 Manual Settings> (<Single Address>(<First Address>), <Range Address>(<First Address>, <Last Address>), <Subnet Settings>(<First Address>, <Subnet Settings>))	Yes	C	Settings/Registration Basic Information
	• <IPv6 Manual Settings> (<Single Address>(<First Address>), <Range Address> (<First Address>, <Last Address>), <Prefix Address> (<First Address>, <Prefix Length>))	Yes	C	Settings/Registration Basic Information
	• <Prefix Length> (1 to 64 to 128)	Yes	C	Settings/Registration Basic Information
	<Remote Address Settings>(<All IP Addresses>, <All IPv4 Addresses>, <All IPv6 Addresses>, <IPv4 Manual Settings>, <IPv6 Manual Settings>)	Yes	C	Settings/Registration Basic Information
	• <IPv4 Manual Settings>(<Single Address>(<First Address>), <Range Address>(<First Address>, <Last Address>), <Subnet Settings>(<First Address>, <Subnet Settings>))	Yes	C	Settings/Registration Basic Information
	• <IPv6 Manual Settings> (<Single Address>(<First Address>), <Range Address> (<First Address>, <Last Address>), <Prefix Address> (<First Address>, <Prefix Length>))	Yes	C	Settings/Registration Basic Information

Settings/Registration

	<Prefix Length> (1 to 64 to 128)	Yes	C	Settings/Registration Basic Information
	<Port Settings> (< Specify by Port Number >, <Specify by Service Name>)	Yes	C	Settings/Registration Basic Information
	<Specify by Port Number>(<Local Port>(<All Ports>, <Single Port>), <Remote Port>(<All Ports>, <Single Port>))	Yes	C	Settings/Registration Basic Information
	<Single Port> (1 to 65535)	Yes	C	Settings/Registration Basic Information
	<Specify by Service Name> <SMTP RX>: <Off>, <On> <SMTP TX>: <Off>, <On> <POP3>: <Off>, <On> <LPD>: <Off>, <On> <RAW>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<IKE>	<IKE Mode>: < Main >, <Aggressive>	Yes	C	Settings/Registration Basic Information
	<Validity>: 1 to 480 to 65535 min.	Yes	C	Settings/Registration Basic Information
	<Authentication Method>: < Pre-Shared Key Method > (<Shared Key Settings>), <Digital Signature Method> (<Key and Certificate>)	Yes	C	Settings/Registration Basic Information
	<Key and Certificate>: <Use>	Yes	C	Settings/Registration Basic Information
	<Key and Certificate>: <Certificate Details>(<Version>, <Serial Number>, <Signature Algorithm>, <Issued To>, <Validity Start Date>, <Validity End Date>, <Issuer>, <Public Key>, <Certificate Thumbprint>, <Issued To (Alternate Name)>, <Verify Certificate>)	Yes	C	Settings/Registration Basic Information
	<Key and Certificate>: <Key Usage>(Displays what the key pair is being used for)	Yes	C	Settings/Registration Basic Information
	<Authentication/Encryption Algorithm> (< Auto >, <Manual Settings>)	Yes	C	Settings/Registration Basic Information
	<Authentication/Encryption Algorithm>: <Manual Settings> <Authentication> <SHA1>, <SHA2>, <SHA1 and SHA2>	Yes	C	Settings/Registration Basic Information
	<Encryption> <AES-CBC>	Yes	C	Settings/Registration Basic Information
	<DH Group> <Group 14 (2048)>, <ECDH-P256>, <ECDH-P384>	Yes	C	Settings/Registration Basic Information
<IPSec Network>	<Validity> <Time>: <Off>, < On >	Yes	C	Settings/Registration Basic Information
	When <On> is selected: (1 to 480 to 65535min.)	Yes	C	Settings/Registration Basic Information

Settings/Registration

	<Validity> <Size>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: (0 to 1 to 65535 MB)	Yes	C	Settings/Registration Basic Information
	<PFS>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Authentication/Encryption Algorithm>: <Auto>, <Manual Settings>	Yes	C	Settings/Registration Basic Information
	<Authentication/Encryption Algorithm>: <Manual Settings> (<ESP>, <ESP (AES-GCM)>, <AH (SHA1)>)	Yes	C	Settings/Registration Basic Information
	<ESP> Settings: <ESP Authentication>: <SHA1>, <NULL> <ESP Encryption>: <AES-CBC>, <NULL>	Yes	C	Settings/Registration Basic Information
	<ESP (AES-GCM)> Settings: None	Yes	C	Settings/Registration Basic Information
	<AH (SHA1)> Settings: None	Yes	C	Settings/Registration Basic Information
	<Connection Mode>: <Transport> (display only)	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <TCP/IP Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<TCP/IP Option Settings>*1	<Use Window Scale Option>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<MTU Size>: 600 to 1500 bytes (600-1500)	Yes	C	Settings/Registration Basic Information
	<Minimum Value of MSS>: 48 to 560 bytes (48-560)	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <SNMP Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use SNMPv1>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Use Dedicated Community>*1	<Use Dedicated Community>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<MIB Access Permission>: <Read/Write>, <Read Only>	Yes	C	Settings/Registration Basic Information

Settings/Registration

<Use Community Name 1>*1	<Use Community Name 1>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<MIB Access Permission>: <Read/Write>, <Read Only>	Yes	C	Settings/Registration Basic Information
	<Community Name>: public	Yes	C	Settings/Registration Basic Information
<Use Community Name 2>*1	<Use Community Name 2>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<MIB Access Permission>: <Read/Write>, <Read Only>	Yes	C	Settings/Registration Basic Information
	<Community Name>: public2	Yes	C	Settings/Registration Basic Information
<Use SNMPv3>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Administrator Settings>*1	<Use Administrator>: <Off>, <On> <User Name>: Display only <MIB Access Permission>: Display only <Security Settings>: Display only <Authentication Algorithm>: Display only <Encryption Algorithm>: Display only	Yes	C	Settings/Registration Basic Information
	<Use Same Password as for Authentication>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Set/Change Password>: <Off>, <On> <Encryption Password>: Enter the password. <Confirm>: Enter the password.	Yes	C	Settings/Registration Basic Information
<User Settings>*1	<User On/Off>	Yes	C	Settings/Registration Basic Information
	<Register> (<User Name>, <MIB Access Permission> (<Read/Write>, <Read Only>), <Security Settings> (<Auth. Yes/Encrypt. Yes>, <Auth. Yes/Encrypt. No>, <Auth. No/Encrypt. No>), <Authentication Algorithm> (<MD5>, <SHA1>, <SHA2-224>, <SHA2-256>, <SHA2-384>, <SHA2-512>), <Authentication Password>, <Encryption Algorithm> (<DES>, <AES>), <Encryption Password>)	Yes	C	Settings/Registration Basic Information
	<Edit User> (<User Name>, <MIB Access Permission> (<Read/Write>, <Read Only>), <Security Settings> (<Auth. Yes/Encrypt. Yes>, <Auth. Yes/Encrypt. No>, <Auth. No/Encrypt. No>), <Authentication Algorithm> (<MD5>, <SHA1>, <SHA2-224>, <SHA2-256>, <SHA2-384>, <SHA2-512>), <Authentication Password>, <Encryption Algorithm> (<DES>, <AES>), <Encryption Password>)	Yes	C	Settings/Registration Basic Information
	<Delete>	Yes	No	-
<Get Printer Management Information from Host>*1	<Off>, <On>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <Format Host Resources MIB to RFC2790>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Format Host Resources MIB to RFC2790>	<Off>, <On>	No	C	Settings/Registration Basic Information

• <Dedicated Port Settings>*1

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Dedicated Port Settings>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Dedicated Port Authentication Method>	<Mode 1>, <Mode 2>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <Use Spool Function>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use Spool Function>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

• <Receive in Parallel>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Receive in Parallel>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

• <Waiting Time for Connection at Startup>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Waiting Time for Connection at Startup>	0 to 300 sec.	Yes	C	Settings/Registration Basic Information

• <Ethernet Driver Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Ethernet Driver Settings>	<Auto Detect>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Communication Mode>: <Half Duplex>, <Full Duplex>	Yes	C	Settings/Registration Basic Information
	• <Ethernet Type>: <10BASE-T>, <100BASE-TX>, <1000BASE-T>	Yes	C	Settings/Registration Basic Information

Settings/Registration

	<Current Transmission Speed>: <---->, <10 Mbps (Half Dplx)>, <10 Mbps (Full Dplx)>, <100 Mbps(Half Dplx)>, <100 Mbps (Full Dplx)>, <1000 Mbps(Full Dplx)>	Yes	No	-
	<MAC Address>: Display only	Yes	No	-

• <IEEE 802.1X Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use IEEE 802.1X>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Login Name> *1	Login Name	Yes	C	Settings/Registration Basic Information
<Verify Authentication Server Certificate> *1	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Verify Authentication Server Name> *1	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Authentication Server Name> *1	Authentication Server Name	Yes	C	Settings/Registration Basic Information
<Use TLS> *1	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Key and Certificate> *1	<Use>	Yes	No	-
	<Certificate Details> (<Version>, <Serial Number>, <Signature Algorithm>, <Issued To>, <Validity Start Date>, <Validity End Date>, <Issuer>, <Public Key>, <Certificate Thumbprint>, <Issued To (Alternate Name)>, <Verify Certificate>)	Yes	No	-
	<Key Usage> (Key and Certificate)	Yes	No	-
<Use TTLS> *1	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <TTLS Settings (TTLS Protocol)>: <Use MSCHAPv2>, <Use PAP>	Yes	C	Settings/Registration Basic Information
<Use PEAP> *1	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Use Login Name as User Name> *1	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<User Name> *1	Name of the user to be authenticated with IEEE802.1X authentication	Yes	C	Settings/Registration Basic Information
<Password> *1	Password of the user to be authenticated with IEEE802.1X authentication	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

- <Firewall Settings>: <IPv4 Address Filter>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Outbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Register New> (Up to 16 IPv4 addresses), <Delete>	Yes	C	Settings/Registration Basic Information
	• <Address to Register>*1	Yes	C	Settings/Registration Basic Information
	• <Specify Port Number>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Port Number>*1: Enter the port number. <Delete>, <Add>	Yes	C	Settings/Registration Basic Information
<Inbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Register New> (Up to 16 IPv4 addresses), <Delete>	Yes	C	Settings/Registration Basic Information
	• <Address to Register>*1	Yes	C	Settings/Registration Basic Information
	• <Specify Port Number>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Port Number>*1: Enter the port number. <Delete>, <Add>	Yes	C	Settings/Registration Basic Information
<IPv4 Address ICMP Settings>*1	<Always Allow Sending/Receiving Using ICMP>: <Off>, <On>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

- <Firewall Settings>: <IPv6 Address Filter>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Outbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Register New> (Up to 16 IPv4 addresses), <Delete>	Yes	C	Settings/Registration Basic Information

Settings/Registration

	• <Address to Register>*1	Yes	C	Settings/Registration Basic Information
	• <Specify Port Number>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Port Number>*1: Enter the port number. <Delete>, <Add>	Yes	C	Settings/Registration Basic Information
<Inbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Register New> (Up to 16 IPv4 addresses), <Delete>	Yes	C	Settings/Registration Basic Information
	• <Address to Register>*1	Yes	C	Settings/Registration Basic Information
	• <Specify Port Number>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Port Number>*1: Enter the port number. <Delete>, <Add>	Yes	C	Settings/Registration Basic Information
<IPv6 Address ICMP Settings>*1	<Always Allow Sending/Receiving Using ICMP>: <Off>, <On>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <Firewall Settings>: <MAC Address Filter>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Outbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Add> (Up to 100 Mac addresses), <Edit>, <Delete>	Yes	C	Settings/Registration Basic Information
<Inbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Add> (Up to 100 Mac addresses), <Edit>, <Delete>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <Firewall Settings>: <IP Address Block Log>*1

Settings/Registration

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<IP Address Block Log>	<Date/Time>, <Type>, <IP Address>, <Port Number>, <Result>	Yes	No	-

*1 This setting can only be specified from the Remote UI.

● <Use Mopria>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use Mopria>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

● <Use AirPrint>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use AirPrint>	<Off>, <On> When <On> is selected: <Printer Name>*1: Enter the Printer Name <Location>*1: Enter the Location	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

● <Display Errors for AirPrint>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Display Errors for AirPrint>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

● <Position Information>*1

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Position Information>	<Auto Acquire>	Yes	No	-
	<Latitude>: Specify the latitude.	Yes	No	-
	<Longitude>: Specify the longitude.	Yes	No	-

*1 This setting can only be specified from the Remote UI.

● <Use IPP Everywhere>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use IPP Everywhere>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

- <Settings for Universal Print>*1

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Basic Settings>				
<Use Universal Print>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Verify Server Certificate>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Add CN to Verification Items>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Printer Name>	OIP_PRINTER	Yes	A	Settings/Registration Basic Information
<Application ID>	f9fc375cc7ba-4e5c-b213-23affd792cc1	Yes	C	Settings/Registration Basic Information
<Microsoft Entra ID Authentication URL>	https://login.microsoftonline.com/organizations/oauth2/v2.0	Yes	C	Settings/Registration Basic Information
<Microsoft Entra ID Registration URL>	https://register.print.microsoft.com/api/v1.0/register	Yes	C	Settings/Registration Basic Information
<Registration Status>	<Not Registered> <Registered> <Checking>	Yes	-	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

- <Select Interface>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Select Interface>	<Main Line> <Wired LAN> SubLine <Off>, <Wired LAN>, <Wireless LAN> <Main Line> <Wireless LAN> SubLine <Off>, <Wired LAN>	No	C	Settings/Registration Basic Information

- <Wireless LAN Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<WPS Push Button Mode>				
<WPS PIN Code Mode>				
<SSID Settings>	<Select Access Point>: Select from the list.	No	No	-
	<Enter Manually>: Enter SSID.	No	No	-

Settings/Registration

	<Security Settings>: <None>, <WPA/WPA2-PSK>, <WPA/WPA2-EAP>, <WPA2-PSK/WPA3-SAE>, <WPA3-SAE>	No	No	-
<Power Save Mode>	<Off>, <On>	No	No	-
<Connection Information>	<MAC Address>: Display Only <Wireless LAN Status>: Display Only <Latest Error Information>: Display Only <Channel>: Display Only <SSID Settings>: Display Only <Security Settings>: <Encryption Method>, <Encryption Key> <Power Save Mode>: Display Only	Yes	No	-

• <Direct Connection Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Use Direct Connection>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Direct Connection Type>	<Access Point Mode>, <Wi-Fi Direct>	Yes	C	Settings/Registration Basic Information
<Device Name for Wi-Fi Direct>	<Dev Name(Wi-Fi Direct)>: Device Name	Yes	No	Settings/Registration Basic Information
<Time Until Direct Connection Termination>	0 = None, 1 to 30 to 60 min.	Yes	C	Settings/Registration Basic Information
<Access Point Mode Settings>	<Use Custom SSID>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <SSID>: Enter SSID	Yes	C	Settings/Registration Basic Information
	<Use Custom Network Key>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Network Key>: Enter the network key	Yes	C	Settings/Registration Basic Information
<Keep Enabled If SSID/Net. Key Specified>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Direct Connection IP Address Settings>	192.168.22.1	Yes	C	Settings/Registration Basic Information

• <Session Settings>*1

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Timeout After Logging in to Remote UI>	15 to 150 min.	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

• <Sub Line Settings>

Settings/Registration

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<IP Address Settings>	<Auto Acquire>: <DHCP>, <Off>	No	C	Settings/Registration Basic Information
	<Manually Acquire> <IP Address>: <0.0.0.0> <Subnet Mask>: <0.0.0.0> <Gateway Address>: <0.0.0.0>	No	A	Settings/Registration Basic Information
	<Check Settings>: Display only	No	A	-
<Priority Line for Comm w/ Mobile Devices>	<Main Line>, <Sub Line>	No	C	Settings/Registration Basic Information
<Ethernet Driver Settings>	<Auto Detect>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Communication Mode>: <Half Duplex>, <Full Duplex>	Yes	C	Settings/Registration Basic Information
	• <Ethernet Type>: <10BASE-T>, <100BASE-TX>, <1000BASE-T>	Yes	C	Settings/Registration Basic Information
	<Current Transmission Speed>: <----->, <10 Mbps (Half Dplx)>, <10 Mbps (Full Dplx)>, <100 Mbps (Half Dplx)>, <100 Mbps (Full Dplx)>, <1000 Mbps (Full Dplx)>	Yes	C	Settings/Registration Basic Information
	<MAC Address>: Display only	Yes	C	Settings/Registration Basic Information
<IEEE 802.1X Settings>	<Use IEEE 802.1X>: <Off>, <On>	Yes	C	Settings/Registration Basic Information

- <Sub Line Settings>: <Firewall Settings>: <IPv4 Address Filter>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Outbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Register New> (Up to 16 IPv4 addresses), <Delete>	Yes	C	Settings/Registration Basic Information
	• <Address to Register>*1	Yes	C	Settings/Registration Basic Information
	• <Specify Port Number>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Port Number>*1: Enter the port number. <Delete>, <Add>	Yes	C	Settings/Registration Basic Information

Settings/Registration

<Inbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Register New> (Up to 16 IPv4 addresses), <Delete>	Yes	C	Settings/Registration Basic Information
	• <Address to Register>*1	Yes	C	Settings/Registration Basic Information
	• <Specify Port Number>*1: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	• <Port Number>*1: Enter the port number. <Delete>, <Add>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

- <Sub Line Settings>: <Firewall Settings>: <MAC Address Filter>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Outbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Delete>, <Add>, <Edit>	Yes	C	Settings/Registration Basic Information
<Inbound Filter>	<Use Filter>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Default Policy>*1: <Allow>, <Reject>	Yes	C	Settings/Registration Basic Information
	<Exception Addresses>*1: <Delete>, <Add>, <Edit>	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

- <Sub Line Settings>: <Settings for System Data Communication>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<DNS Server Address Settings>	<Primary DNS Server>	Yes	C	Settings/Registration Basic Information
	<Secondary DNS Server>	Yes	C	Settings/Registration Basic Information
<Proxy Settings>	<Use Proxy>: <Off>, <On>	Yes	C	Settings/Registration Basic Information

Settings/Registration

	<Server Address> (IP Address or FQDN)	Yes	C	Settings/Registration Basic Information
	<Port Number>: 1 to 80 to 65535	Yes	C	Settings/Registration Basic Information
<Authentication Set.>	<Use Proxy Auth.>: <Off> , <On>	Yes	C	Settings/Registration Basic Information
	<User Name> (24 characters maximum)	Yes	C	Settings/Registration Basic Information
	<Password> (24 characters maximum) <Confirm> (24 characters maximum)	Yes	C	Settings/Registration Basic Information
<Select Line to Use>	<Main Line> , <Sub Line>	Yes	C	Settings/Registration Basic Information

● <Static Routing Settings>

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Static Routing Settings>	<Use Static Routing>: <Off> , <On>	Yes	C	Settings/Registration Basic Information
	<Register>*1, <Delete>*1	Yes	No	-
	● <Register> <Destination Address>(< 0.0.0.0 >), <Gateway Address>(< 0.0.0.0 >)	Yes	C	Settings/Registration Basic Information

*1 This setting can only be specified from the Remote UI.

External Interface

E9SJ-07A

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<USB Settings>				
<Use as USB Device>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Use MEAP Driver for USB Storage Device>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Use USB Storage Device>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Restrict Auto Install of Printer Driver>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

Accessibility

E9SJ-07C

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Key Repetition Settings>	< Standard >, <Slightly Slow>, <Slow>	No	C	Settings/Registration Basic Information
<Acceptance Delay for Repeated Presses>	< Off >, <On> 0.1 to 1.0 seconds	No	C	Settings/Registration Basic Information
<Invert Screen Colors>	< Off >, <On>	No	C	Settings/Registration Basic Information
<Contrast>	-3 to 0 to +3 (7 levels)	No	C	Settings/Registration Basic Information
<Backlight Brightness>	0 to 4	No	C	Settings/Registration Basic Information
<Message Display Time>	1 to 2 to 5 seconds	No	C	Settings/Registration Basic Information
<Scrolling Speed>	<Slow>, < Standard >, <Fast>	No	C	Settings/Registration Basic Information

Volume Settings

E9SJ-07E

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Entry Tone>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Invalid Entry Tone>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Restock Supplies Tone>	<Off>, <On> ,	Yes	C	Settings/Registration Basic Information
<Warning Tone>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Job Done Tone>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Sleep Mode Tone>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Login Tone>	<Off>, <On>	Yes	C	Settings/Registration Basic Information

Adjustment/Maintenance

E9SJ-07F

- ▶ Adjust Image Quality(P. 416)
- ▶ Maintenance(P. 418)

Adjust Image Quality

E9SJ-07H

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Adjust Print Position>				
<Print Sample>	<Yes>, <No>	No	No	-
<Multi-Purpose Tray>	<Adj. Vertically (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1st Side for 2-Sided)>	Yes	No	-
<Drawer 1>	<Adj. Vertically (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1st Side for 2-Sided)>	Yes	No	-
<Drawer 2>*1	<Adj. Vertically (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1st Side for 2-Sided)>	Yes	No	-
<Drawer 3>*1	<Adj. Vertically (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1st Side for 2-Sided)>	Yes	No	-
<Drawer 4>*1	<Adj. Vertically (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1-Sd/2nd Sd for 2-Sd)>, <Adj. Horizontally (1st Side for 2-Sided)>	Yes	No	-
<Common>	<Adj. Vertically (1st Side for 2-Sided)>	Yes	No	-
<Special Processing>				
<Waterdrop Pattern Prevention Mode>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Reduce Paper Sticking at Output>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Reduce Ghosting>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Reduce Wrinkles (from Humidity)/Streaks>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Paper Wrinkle Correction>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Streak Prevention>	<Off>, <Mode 1>, <Mode 2>, <Mode 3>, <Mode 4>	Yes	B	Settings/Registration Basic Information
<Curl Prevention Mode>	<Off>, <On>	Yes	B	Settings/Registration Basic Information

Settings/Registration

<Quiet Mode>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Adjust Fixing Level for Envelopes>	<Low>, <Standard>, <High>	Yes	B	Settings/Registration Basic Information
<Reduce Toner Flaking from Postcards>	<Off>, <On>	Yes	B	Settings/Registration Basic Information
<Adjust Standard Density>	-4 to 0 to +4	Yes	B	Settings/Registration Basic Information
<Adjust Density for Specific Paper>	-4 to 0 to +4	Yes	B	Settings/Registration Basic Information

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

Maintenance

E9SJ-07J

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Clean Pressure Roller for Fixing>	-	No	No	-

Function Settings

E9SJ-07K

- ▶ Common(P. 420)
- ▶ Printer(P. 422)
- ▶ Send(P. 433)
- ▶ Receive(P. 434)
- ▶ Access Files(P. 435)
- ▶ Print(P. 437)

Common

E9SJ-07L

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Paper Feed Settings>				
<Paper Source Auto Selection>	<Printer>: <Multi-Purpose Tray>: <Off>, <On> - Other: <Off>, <On> <Group Settings>: <Off>, <On> <Use Group>: <Off>, <On>	Yes	B	Settings/Registration Basic Information
	<Access Stored Files>: <Multi-Purpose Tray>: <Off>, <On> - Other: <Off>, <On>	Yes	B	Settings/Registration Basic Information
	<Receive>: <Multi-Purpose Tray>: <Off>, <On> - Other: <Off>, <On>	Yes	B	Settings/Registration Basic Information
	<Other>: <Multi-Purpose Tray>: <Off>, <On> - Other: <Off>, <On>	Yes	B	Settings/Registration Basic Information
<Switch Paper Feed Method>	<Multi-Purpose Tray> and Other: <Speed Priority>, <Print Side Priority>	Yes	B	Settings/Registration Basic Information
<Suspended Job Timeout>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: 0 to 5 to 999 min.	Yes	C	Settings/Registration Basic Information
<Paper Output Settings>				
<Job Separator Between Jobs>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Job Separator Between Copies>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Number of Copies> (1 to 10 to 9999)	Yes	C	Settings/Registration Basic Information
<Print Settings>				
<Print Priority>	<Printer>: <1>, <2>, <3> <Access Stored File>: <1>, <2>, <3> <Other>: <1>, <2>, <3>	Yes	C	Settings/Registration Basic Information

Settings/Registration

<Auto Delete Suspended Jobs>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: 0 to 5 to 999 min.	Yes	C	Settings/Registration Basic Information
<Action When Remaining Toner Is Low>	<Continue Printing>, <Display Warning Screen>	Yes	No	-
	When <Continue Printing> is selected: <Displ Tnr Cart Warning>: <Off>, <On>	Yes	B	Settings/Registration Basic Information

Printer

E9SJ-07R

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Printer Settings>				
<Custom Settings>	▶ Custom Settings(P. 423)	-	-	-
<UFR II>	▶ UFR II(P. 425)	-	-	-
<PCL>	▶ PCL(P. 426)	-	-	-
<PS>	▶ PS(P. 428)	-	-	-
<Imaging>	▶ Imaging(P. 429)	-	-	-
<PDF>	▶ PDF(P. 430)	-	-	-
<XPS>	▶ XPS(P. 431)	-	-	-
<Utility>	▶ Utility(P. 432)	-	-	-
<Restrict Printer Jobs>	<Off>, <On>	Yes	C	Settings for Printer Settings
	When <On> is selected: <Select Jobs to Allow>: <Reserved Jobs>	Yes	C	Settings for Printer Settings
<Switch Paper Source Auto Selection Mode>	<Short Edge Feed Paper Priority>, <Long Edge Feed Paper Priority>	Yes	C	Settings/Registration Basic Information
<Feed from MP Tray When No Paper Source>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<MP Tray Priority for Ppr Src Auto Select>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<PDL Selection (Plug and Play)>	<UFR II>, <PCL6>, <PS3>	Yes	C	Settings for Printer Settings
<Ppr Size Mismatch for Free Size Ppr Src>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Vertical Printing Priority for Free Size>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<PS Password Settings>	<SystemParams Password>, <StartJob Password>	Yes	C	Settings for Printer Settings
<Paper Feed Mode When Using PCL Emulation>	<Mode 0>, <Mode 1>, <Mode 2>	Yes	C	Settings/Registration Basic Information

Custom Settings

E9SJ-07S

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Number of Copies>	1 to 9999	Yes	C	Settings for Printer Settings
<2-Sided Printing>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Paper Feed>				
<Default Paper Feed Source>	<Auto>, <MP Tray>, <Drawer 1>, <Drawer 2>, <Drawer 3>, <Drawer 4>	Yes	B	Settings for Printer Settings
<Default Paper Size>	<A4>, <A5>, <A6>, <B5>, <16K>, <Letter>, <Legal>, <Statement>, <Executive>, <Postcard>, <Reply Postcard>, <4 on 1 Postcard>, <Env. NAGAGATA 3>, <Env. NAGAGATA 4>, <Env. NAGAGATA 40>, <Env. YOGATANAGA3>, <Env. No. 10>, <Envelope ISO-C5>, <Envelope DL>, <Envelope Monarch>, <FOOLSCAP/FOLIO>, <FOOLSCAP (Australia)>, <LETTER (Government)>, <LEGAL (Government)>, <OFICIO>, <OFICIO (Brazil)>, <OFICIO (Mexico)>, <F4A>, <LEGAL (India)>, <3x5 inch>	Yes	B	Settings for Printer Settings
<Default Paper Type>	<Thin>, <Plain 1>, <Plain 2>, <Plain 3>, <Heavy 1>, <Heavy 2>, <Heavy 3>, <Color>, <Recycled 1>, <Recycled 2>, <Labels>, <Bond 1>, <Bond 2>, <Bond 3>, <Letterhead 1>, <Letterhead 2>, <Letterhead 3>, <Letterhead 4>, <Letterhead 5>, <Letterhead 6>, <Postcard>, <Envelope>	Yes	B	Settings for Printer Settings
<Paper Size Override>	<On>, <Off>	Yes	C	Settings for Printer Settings
<2nd Side of MP Tray 2-Sided Page>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Paper Output>				
<Finishing>	<Finishing>: <Off>, <Collate>, <Group>	Yes	C	Settings for Printer Settings
<Print Quality>				
<Image Refinement>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Density>*1	-8 to +8; 0	Yes	C	Settings for Printer Settings
<Density (Fine Adjust)>*1	<High>: -8 to +8; 0 <Medium>: -8 to +8; 0 <Low>: -8 to +8; 0	Yes	C	Settings for Printer Settings
<Toner Save>	<On>, <Off>	Yes	C	Settings for Printer Settings

Settings/Registration

<Line Refinement>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Horizontal Line Refinement>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Vertical Line Refinement>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Resolution>	<1200 dpi>, <600 dpi>	Yes	B	Settings for Printer Settings
<Barcode Adjustment Mode>	<Off>, <Mode 1>, <Mode 2>, <Mode 3>, <Mode 4>, <Mode 5>	Yes	C	Settings for Printer Settings
<Layout>				
<Binding Location>	<Long Edge>, <Short Edge>	Yes	C	Settings for Printer Settings
<Gutter>	-50.0 mm to +50.0 mm; 00.0 mm	Yes	C	Settings for Printer Settings
<Offset Short Edge (Front)>	-50.8 mm to +50.8 mm; 00.0 mm	Yes	C	Settings for Printer Settings
<Offset Long Edge (Front)>	-50.8 mm to +50.8 mm; 00.0 mm	Yes	C	Settings for Printer Settings
<Offset Short Edge (Back)>	-50.8 mm to +50.8 mm; 00.0 mm	Yes	C	Settings for Printer Settings
<Offset Long Edge (Back)>	-50.8 mm to +50.8 mm; 00.0 mm	Yes	C	Settings for Printer Settings
<Auto Error Skip>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Timeout>	<Timeout>: <On>, <Off> <Timeout>: 5 seconds to 300 seconds; 15 seconds	Yes	C	Settings for Printer Settings
<Personality>*1	<Auto>, <PS>, <PCL>, <XPS>, <Imaging>, <PDF>	Yes	C	Settings for Printer Settings
<Mode Priority>*1	<None>, <PS>, <PCL>, <XPS>, <PDF>	Yes	C	Settings for Printer Settings
<Auto Select>*1	<PS>: <On>, <Off> <PCL>: <On>, <Off> <XPS>: <On>, <Off> <Imaging>: <On>, <Off> <PDF>: <On>, <Off>	Yes	C	Settings for Printer Settings
<Compressed Image Output>	<Output>, <Display Error>	Yes	C	Settings for Printer Settings
<Initialize>	<Yes>, <No>	No	No	-

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Halftones>	<Text>: <Color Tone>, <Gradation>, <Resolution>, <High Resolution>	Yes	B	Settings for Printer Settings
	<Graphics>: <Color Tone>, <Gradation>, <Resolution>, <High Resolution>			
	<Image>: <Color Tone>, <Gradation>, <Resolution>, <High Resolution>			

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Paper Save>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Orientation>	<Portrait>, <Landscape>	Yes	C	Settings for Printer Settings
	<Internal>, <Soft/External>	No	C	Settings for Printer Settings
	0 to 104; 0 (If the Font Source setting is Internal.) 1 to 999; 1 (If the Font Source setting is Soft/External.)	Yes	C	Settings for Printer Settings
<Point Size>*1	4.00 to 999.75 <point>; 12.00 <point>	Yes	C	Settings for Printer Settings
<Pitch>*1	0.44 to 99.99 <dpi>; 10.00 <dpi>	Yes	C	Settings for Printer Settings
<Form Lines>	5 to 128 <lines>; 64 <lines>	Yes	C	Settings for Printer Settings
<Character Code>	<ARABIC8>, <DESKTOP>, <GREEK8>, <HEBREW7>, <HEBREW8>, <ISO4>, <ISO6>, <ISO11>, <ISO15>, <ISO17>, <ISO21>, <ISO60>, <ISO69>, <ISOCYR>, <ISOGRK>, <ISOHEB>, <ISOL1>, <ISOL2>, <ISOL5>, <ISOL6>, <ISOL9>, <LEGAL>, <MATH8>, <MCTEXT>, <MSPUBL>, <PC8>, <PC8DN>, <PC8GRK>, <PC8TK>, <PC775>, <PC850>, <PC851>, <PC852>, <PC858>, <PC862>, <PC864>, <PC866>, <PC1004>, <PIFONT>, <PSMATH>, <PSTEXT>, <ROMAN8>, <ROMAN9>, <VNINTL>, <VNMATH>, <VNUS>, <WIN30>, <WINARB>, <WINBALT>, <WINCYR>, <WINGRK>, <WINL1>, <WINL2>, <WINL5>	Yes	C	Settings for Printer Settings
<Custom Paper>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Unit of Measure>*1	<Millimeters>, <inches>	Yes	C	Settings for Printer Settings
<X dimension>*1	76.2 mm to 216.0 mm; 216.0 mm	Yes	B	Settings for Printer Settings
<Y dimension>*1	127.0 mm to 355.6 mm; 355.6 mm	Yes	B	Settings for Printer Settings
<Append CR to LF>	<Yes>, <No>	Yes	C	Settings for Printer Settings
<Enlarge A4 Print Width>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Halftones>	<Text>: <Color Tone>, <Gradation>, <Resolution>, <High Resolution>	Yes	B	Settings for Printer Settings
	<Graphics>: <Color Tone>, <Gradation>, <Resolution>, <High Resolution>			

Settings/Registration

	<Image>: <Color Tone>, <Gradation>, <Resolution>, <High Resolution>			
<BarDIMM>*1	<Enable>, <Disable>	Yes	C	Settings for Printer Settings
<FreeScape>*1	<Off>, <->, <">, <#>, <\$>, </>, <\>, <?>, <{>, <}>, < >	Yes	C	Settings for Printer Settings

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Paper Save>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Job Timeout>	0 to 3600 seconds; 0 second	Yes	C	Settings for Printer Settings
<Print PS Errors>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Halftones>	<Text>:<Gradation>, <Resolution>, <High Resolution>	Yes	B	Settings for Printer Settings
	<Graphics>:<Gradation>, <Resolution>, <High Resolution>			
	<Image>: <Gradation>, <Resolution>, <High Resolution>			
<Grayscale Conversion>*1	<sRGB>, <NTSC>, <Uniform RGB>	Yes	C	Settings for Printer Settings
<Dot Gain Adjustment>	<-10%>, <-5%>, <Standard>, <+5%>, <+10%>	Yes	C	Settings for Printer Settings

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

Imaging

E9SJ-07Y

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Image Orientation>	< Auto >, <Vertical>, <Horizontal>	Yes	C	Settings for Printer Settings
<Zoom>	< Off >, <Auto>	Yes	C	Settings for Printer Settings
<Print Position>	< Auto >, <Center>, <Top Left>	Yes	C	Settings for Printer Settings
<Show Warnings>	< On >, <Off>	Yes	C	Settings for Printer Settings
<Enlarge Print Area>	< Off >, <On>	Yes	C	Settings for Printer Settings
<Halftones>	< Gradation >, <Resolution>, <High Resolution>	Yes	B	Settings for Printer Settings
<Grayscale Conversion>*1	<sRGB>, < NTSC >, <Uniform RGB>	Yes	C	Settings for Printer Settings

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Paper Save>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Enlarge/Reduce to Fit Size>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Enlarge Print Area>	<On>, <Off>	Yes	C	Settings for Printer Settings
<N on 1>	<Off>, <2 on 1>, <4 on 1>, <6 on 1>, <8 on 1>, <9 on 1>, <16 on 1>	Yes	C	Settings for Printer Settings
<Comment Print>	<Off>, <Auto>	Yes	C	Settings for Printer Settings
<Halftones>	<Text>: <Gradation>, <Resolution>, <High Resolution>	Yes	B	Settings for Printer Settings
	<Graphics>: <Gradation>, <Resolution>, <High Resolution>			
	<Image>: <Gradation>, <Resolution>, <High Resolution>			
<Grayscale Conversion>*1	<sRGB>, <NTSC>, <Uniform RGB>	Yes	C	Settings for Printer Settings
<Dot Gain Adjustment>	<-10%>, <-5%>, <Standard>, <+5%>, <+10%>	Yes	C	Settings for Printer Settings

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Paper Save>	<On>, <Off>	Yes	C	Settings for Printer Settings
<Halftones>	<Text>: <Gradation>, <Resolution>, <High Resolution>	Yes	B	Settings for Printer Settings
	<Graphics>: <Gradation>, <Resolution>, <High Resolution>			
	<Image>: <Gradation>, <Resolution>, <High Resolution>			
<Grayscale Conversion>*1	<Text>: <sRGB>, <NTSC>, <Uniform RGB>	Yes	C	Settings for Printer Settings
	<Graphics>: <sRGB>, <NTSC>, <Uniform RGB>			
	<Image>: <sRGB>, <NTSC>, <Uniform RGB>			

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Initialize PCL Storage>	<Yes>, <No>	No	No	-
<Initialize PS Storage>	<Yes>, <No>	No	No	-
<Reset Printer>	<Yes>, <No>	No	No	-

Send

E9SJ-083

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<E-mail Settings>				
<Communication Settings>				
<Basic Settings>	<Use POP RX>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<POP Server Settings>	<POP Interval>: 0 to 99 minutes	Yes	C	Settings/Registration Basic Information
<Allow TLS>	<SMTP RX>: <Off>, <On>, <Always Use TLS>	Yes	C	Settings/Registration Basic Information
	<POP>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<Authentication Settings>	<POP Authentication Method>: <Standard>, <APOP>, <POP AUTH>	Yes	C	Settings/Registration Basic Information
<Confirm TLS Certificate for POP RX>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <CN>: Off, On			

Receive

E9SJ-084

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Common Settings>				
<Print on Both Sides>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Reduce RX Size>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	<Reduction Mode>: <Auto>, <Fixed>			
	<Reduction Ratio>: 75 to 90 to 97%			
	<Reduction Direction>: <Vertical & Horizontal>, <Vertical Only>			
<RX Page Footer>	<On>, <Off>	Yes	C	Settings/Registration Basic Information

Access Files

E9SJ-085

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Common Settings>				
<Access Stored Files Settings>				
<Change Default Set. (Memory Media Print)>	<Number of Copies>:<1>-<9999>	No	C	Favorite Settings
	<Paper>:<MP Tray>, <Drawer 1>, <Drawer 2>*1, <Drawer 3>*1, <Drawer 4>*1			
	<2-Sided>:<Off>, <Book Type>, <Calendar Type>			
	<Resolution>:<600 dpi>, <1200 dpi>			
	<Enlarge Print Area>:<Off>, <On>			
	<Set PDF/XPS Details>: <N on 1>: <Off>, <2 on 1>, <4 on 1>, <6 on 1>, <8 on 1>, <9 on 1>, <16 on 1> <Print Range>: <All Pages>, <Specified Pages> <Fit Paper Size>: <Off>, <On> <Collate>: <Off>, <On> <Halftones>: <Text> (<Gradation>, <Resolution>, <High Resolution>), <Graphics> (<Gradation>, <Resolution>, <High Resolution>), <Image> (<Gradation>, <Resolution>, <High Resolution>)			
	<Set JPEG/TIFF Details>: <Print Range>: <All Pages>, <Specified Pages> <Enlarge/Reduce>: <Off>, <Auto> <Image Orientation>: <Auto>, <Always Portrait>, <Always Landscape> <Print Position>: <Auto>, <Always Center>, <Always Top Left> <Halftones>: <Gradation>, <Resolution>, <High Resolution>			
<Memory Media Settings>				
<Use Print Function>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Select Option When Connecting Mem. Media>	<Off>, <On>	No	C	Settings/Registration Basic Information

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Job Storage Period>	10, 20, 30 min., 1 , 2, 3, 6, 12 hr., 1, 2, 3 days	No	C	Settings/Registration Basic Information
<Job List Display Settings>	<Personal>: < On >, <Off> <Shared>: < On >, <Off> <Group>*1: <On>, < Off >	No	C	Settings/Registration Basic Information

*1 Indicates items that appear only when the appropriate optional product is available for use or the appropriate setting is specified.

Management Settings

E9SJ-087

- ▶ User Management(P. 439)
- ▶ Device Management(P. 440)
- ▶ License/Other(P. 441)
- ▶ Data Management(P. 442)
- ▶ Security Settings(P. 443)

User Management

E9SJ-088

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Authentication Management>				
<Set Administrator Password>	(32 characters maximum)	Yes	C	Authentication User Management
<Set Administrator PIN>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: PIN Entry (16 digits maximum) Default: 7654321			
<System Manager Information Settings>	<System Manager ID and PIN>, <System Manager Name>, <E-Mail Address>, <Contact Information>, <Comment>	Yes	C	Department ID Management Settings
	When <System Manager ID and PIN> is selected: <System Manager ID>: 7654321 (Seven digits maximum) <System Manager PIN>: 7654321 (Seven digits maximum)			
<Department ID Management>	<Off>, <On>	Yes	C	Department ID Management Settings

Device Management

E9SJ-089

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Device Information Settings>	<Device Name>	Yes	A	Settings/Registration Basic Information
	<Location>	Yes	A	Settings/Registration Basic Information
<Display Job Status Before Authentication>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Restrict Access to Other User Jobs>	<Print>: <Off>, <On> <Receive>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<Display Job Log>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <Off> is selected: <Rtrv Log w/ Mngt Sftwr>: <Do Not Allow>, <Allow>	Yes	C	Settings/Registration Basic Information
<Save Audit Log>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Retrieve Network Authentication Log>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Restrict Service Representative Access>	<Off>, <Off (Auth. Needed)>, <On>	Yes	C	Settings/Registration Basic Information
<Remote UI/Toner Status Cnsmbls Info Set.>				
<Dsply Cnsmbls Purchase Btn in Remote UI>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Toner Status Settings>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Dspl Cnsmbls Purch Btn>: <Off>, <On>	Yes	C	Settings/Registration Basic Information
<Prohibit Initialization of Admin. Pswrd.>	<Off>, <On>	No	No	-
<Restrict Special Mode Operations>	<Off>, <On>	No	C	Settings/Registration Basic Information
<Canon Genuine Mode>	<Off>, <On>	Yes	No	-

License/Other

E9SJ-08A

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Register License>	24 characters maximum	No	No	-
<MEAP Settings>				
<Use TLS>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Confirm TLS Certificate Using MEAP App>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Add Items to Verify>: <CN>: Off, On	Yes	C	Settings/Registration Basic Information
<Use DNS Caching>	<On (Unlimited Use)>, <On (Specify Period)>, <Off>	Yes	C	Settings/Registration Basic Information
	When <On (Specify Period)> is selected: <Expires>: 1 to 60 to 120 sec.	Yes	C	Settings/Registration Basic Information
<Use Proxy Settings of This Device>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Add X-FRAME-OPTIONS to HTTP Header>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Remote UI Settings>				
<Enable Remote UI>	<Off>, <On>	No	C	Settings/Registration Basic Information
<Use TLS>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Remote Operation Settings>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
	When <On> is selected: <Password>: 8 characters maximum (Only alphanumeric characters)	Yes	C	Settings/Registration Basic Information
<Register/Update Software>	<Software Management Settings>	Yes	No	-
<Start Setup Guide>	<Yes>, <No>	No	No	-

Data Management

E9SJ-08C

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Import/Export>				
<Import from USB Memory>	<Yes>, <No> <Password>	No	No	-
<Export to USB Memory>	<Password>	No	No	-
<Restrict Import/Export from Web Service>	< Off >, <On>	Yes	C	Settings/Registration Basic Information
<Initialize Network Settings>	<Yes>, <No>	No	No	-
<Initialize All Set. without Network Set.>	<Yes>, <No>	No	No	-
<Initialize All Data/Settings>	<Yes>, <No>	No	No	-

Security Settings

E9SJ-08E

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#).

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<System Verification Settings>				
<Verify System at Startup>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Trellix Embedded Control>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Recommended Security Set. for Usage Env.>	<Usage Environment Settings> <Select Usage Environment> <Check Recommendation> <1. Intranet And Internet Connection>, <2. Direct Internet Connection>, <3. Internet Connection Prohibited>, <4. Private (Home) Network>, <5. Public Network>, <6. Highly Confidential Info. Environment>	Yes	No	Settings/Registration Basic Information
	<Security-Related Notification Settings>: <When Rcmnded. Usage Environ. Is Updated>: <On>, <Off> <When Internet Security Issue Is Detected>: <On>, <Off> <When Encryp. Vuln. Found in Wireless LAN>: <On>, <Off>			

Output Report

E9SJ-08F

NOTE

- For information on the items ("A", "B", "C", and "No") in the "Import All Function" column, see [▶ Import All Function\(P. 387\)](#) .

Item	Setting Description	Can be set in Remote UI	Import All Function	Name of Item When Exporting with the Remote UI
<Default Settings for Output Report>				
<2-Sided Printing>	<Off>, <On>	Yes	C	Settings/Registration Basic Information
<Print List>				
<Consumables Status Report>	<Yes>, <No>	Yes	No	-
<User Data List>	<Yes>, <No>	Yes	No	-
<Network User Data List>	<Yes>, <No>	Yes	No	-
<Communication Management Report>	<Yes>, <No>	Yes	No	-
<Page Count List>	<Yes>, <No>	Yes	No	-
<Counter Report>	<Yes>, <No>	Yes	No	-
<Print Log List>	<Printer>: <Yes>, <No> <Received Job Print>: <Yes>, <No> <Report Print>: <Yes>, <No>	Yes	No	-
<IPSec Policy List>	<Yes>, <No>	Yes	No	-
<MEAP System Information>	<Yes>, <No>	Yes	No	-
<Import Result Report>	<Yes>, <No>	Yes	No	-
<Toner Cartridge Log Report>	<Yes>, <No>	Yes	No	-
<PCL>	<Configuration Page>: <Yes>, <No> : <Yes>, <No>	Yes	No	-
<PS>	<Configuration Page>: <Yes>, <No> : <Yes>, <No>	Yes	No	-

<Preferences>

E9SJ-08H

Item	Description
▶<Display Settings>(P. 446)	This section describes the display settings.
▶<Timer/Energy Settings>(P. 448)	This section describes the timer settings and energy settings.
▶<Network>(P. 452)	This section describes the network settings.
▶<External Interface>(P. 465)	This section describes the USB settings.
▶<Accessibility>(P. 467)	This section describes settings for improving accessibility, such as inverting the screen colors and setting the message display time.
▶<Volume Settings>(P. 468)	This section describes the sound volume settings.

<Display Settings>

E9SJ-08J

This section describes the display settings.

<Button Display Order on Home Screen>

<Set> ► <Preferences> ► <Display Settings>

You can rearrange the order in which the buttons appear on the <Home> screen.  **Customizing the <Home> Screen(P. 161)**

<Default Screen After Startup/Restoration>

<Set> ► <Preferences> ► <Display Settings>

You can set the default screen displayed at startup/restoration.

IMPORTANT

- Depending on the authentication method specified in personal authentication management, the login screen may be displayed before the screen set in <Default Screen After Startup/Restoration> is displayed.

<Language>

<Set> ► <Preferences> ► <Display Settings>

You can select the language displayed on the display.

NOTE

- Some messages may not be displayed properly in the selected language. In this case, restart the machine. Some messages may not change even after the machine is restarted.

<Millimeter/Inch Entry Switch>

<Set> ► <Preferences> ► <Display Settings>

You can set whether to enter numeric values in millimeters or inches on the various numeric entry screens.

<Confirm When Loading Paper in Drawer>

<Set> ► <Preferences> ► <Display Settings>

You can set whether to display the confirmation screen of paper drawer settings when the paper drawer is inserted into the machine.

NOTE

- The confirmation screen of paper drawer settings is not displayed in the following cases.
 - When paper is loaded because it has run out during a job

- When a paper jam is removed
- When a screen for executing, canceling, or confirming jobs is displayed
- When paper is specified in <Paper Settings> on the <Home> screen

<IP Address Display Settings>

<Set> ► <Preferences> ► <Display Settings>

You can set whether to display the IP address on the <Status Monitor> screen.

NOTE

- This setting is only valid when <Use IPv4> is set to <On>.

<Display Icon Showing Remaining Toner>

<Set> ► <Preferences> ► <Display Settings>

You can set whether to display an icon indicating the amount of toner remaining in the toner cartridge on the bottom right of the display.

<Display Mobile Portal>

<Set> ► <Preferences> ► <Display Settings>

You can set whether to display <Mobile Portal> on the <Home> screen.

<Timing of Toner Cart. Replacement Notif.>

<Set> ► <Preferences> ► <Display Settings>

You can set the amount of toner remaining in the toner cartridge for displaying a message notifying the user that a toner cartridge will need to be replaced soon.

<Timer/Energy Settings>

E9SJ-08K

This section describes the timer settings and energy settings.

<Date/Time Settings>

<Set> ► <Preferences> ► <Timer/Energy Settings>

Setting the current date and time is very important. For instructions on how to configure the setting, see ► **Setting the Date/Time(P. 105)** .

<Time Format>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set whether to display the time in 24-hour notation or 12-hour notation.

NOTE

- You can also specify to automatically synchronize the date and time with a server on the network using SNTP. ► **Making SNTP Settings(P. 138)**

<Quick Startup Settings for Main Power>

<Set> ► <Preferences> ► <Timer/Energy Settings>

If you set this function to <On>, you can reduce the time it takes until you can perform operations on the screen after the power is turned ON.

NOTE

- When this function is enabled
 - Standby power is consumed even when the power is turned OFF.
 - A tone sounds when the machine is turned ON, or when the machine is turned OFF if you set <Sleep Mode Tone> to <On>. (However, the machine may not be able to start up quickly and the tone may not sound, depending on the status of the machine.)
- Even if this function is set to <On>, the machine does not startup quickly in the following situations:
 - When any of the network settings below are set to 'On'
 - Wi-Fi
 - When turning ON the main power of the machine after turning OFF the main power in any of the conditions below
 - More than 110 hours have elapsed after quick startup
 - Operating jobs
 - Jobs are reserved
 - Backing up data
 - Accessing to the machine via network
 - After specifying settings which require restarting the machine
 - Error is occurred
 - Using the Limited Functions mode

- The power cord is disconnected after turning OFF the main power
- MEAP applications which do not support quick startup are installed on the machine
- When turning ON the main power of the machine in 20 seconds after turning OFF the main power
- When turning ON the main power of the machine after eight hours have passed since the machine was turned OFF
- When turning ON the main power of the machine after turning OFF the main power from the Remote UI

<Auto Reset Time>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can specify the time period in which you are logged out and the display returns to the default setting automatically.

NOTE

- If the login service is being used, the machine automatically logs out the user when the Auto Reset Time elapses.
- The screen displayed after the Auto Reset initiates differs depending on the following settings.
 - Setting 1: The settings in <Function After Auto Reset>
 - When <Default Function> is set, the screen specified in <Default Screen After Startup/Restoration> (Setting 2) is displayed.
 - When <Selected Function> is set, the function before the Auto Reset initiates is displayed. (The specified settings and entered values for each function will be cleared.) However, the <Selected Function> settings may not be correctly reflected, and the screen specified in <Default Screen After Startup/Restoration> may be displayed.
 - Setting 2: The settings in <Default Screen After Startup/Restoration>

<Restrict Auto Reset Time>

<Set> ► <Preferences> ► <Timer/Energy Settings>

If you set this function to <On>, general users become unable to set <Auto Reset Time> and <Function After Auto Reset>.

<Function After Auto Reset>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set whether the default screen set for <Default Screen After Startup/Restoration> in <Display Settings> or the immediately previous screen is displayed at startup after the Auto Reset initiates.

<Auto Shutdown Time>

<Set> ► <Preferences> ► <Timer/Energy Settings>

With the Auto Shutdown, if the display of the machine is idle for a certain period of time after it has entered the Sleep mode, the machine automatically shuts down.



- Even when operating the machine from the Remote UI, the machine automatically shuts down if the control panel of the machine is idle for a certain period of time. A malfunction may occur particularly if the machine automatically shuts down while importing. Set <Auto Shutdown Time> to <0> when importing data.

NOTE

- The Auto Shutdown may not be performed, depending on the usage conditions of the machine.

<Auto Shutdown Weekly Timer>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set the time that the machine automatically shuts down each day of the week. If you use this function, you do not have to shut down the machine manually every day.

NOTE

- If both <Auto Shutdown Time> and <Auto Shutdown Weekly Timer> are set, priority is given to <Auto Shutdown Time>.

<Allow Sleep Mode During Error>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set whether the machine enters the Auto Sleep mode when an error has occurred.

NOTE

- Disable this setting to prevent the machine from entering the Sleep mode.

<Auto Sleep Time>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set the time until the machine automatically enters the Sleep mode if no operations are performed.

NOTE

- It is recommended that you use the default setting for this item.

<Sleep Mode Energy Use>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set the amount of energy that the machine consumes when it is in the Sleep mode.

IMPORTANT

- If the machine is connected to a computer using a USB cable, depending on the timing for entering the sleep mode, the machine may be unable to receive data correctly. Reactivate the machine from the sleep mode, then execute the job again.
- The energy consumption level may be the same as when <High> is set even when <Low> is set, depending on the status of the machine.

NOTE

- If the energy consumption level is set to <Low>, communication failure may occur, depending on the network utility software you are using. To avoid this, press the Energy Saver key to cancel the Sleep mode before using the machine.
- If you select <Low>, energy consumption in the Sleep mode is low, but it takes longer to recover from the Sleep mode.

<Settings for Sleep Mode Exit upon Job RX>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set whether to keep the control panel in the sleep mode when a print job is received.

NOTE

- If you select <Turn Device Control Panel On> in <Settings for Sleep Mode Exit upon Job RX>, power consumption is higher than when <Do Not Turn Device Control Panel On> is selected.

<Auto Sleep Weekly Timer>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set the time that the machine automatically enters the Sleep mode each day of the week.

NOTE

- If you set both the <Auto Sleep Time> and <Auto Sleep Weekly Timer>, the <Auto Sleep Time> setting is given priority.

<Sleep Mode Exit Time Settings>

<Set> ► <Preferences> ► <Timer/Energy Settings>

You can set the time for recovering from the Sleep mode.

<Network>

E9SJ-08L

This section describes the network settings.

<Output Report>

<Settings/Registration> ► <Preferences> ► <Network Settings>

You can print the settings in <Network>.  <Output Report>(P. 495)

NOTE

- This setting can only be specified from the Remote UI.

<Confirm Network Connection>

<Set> ► <Preferences> ► <Network>

If this setting is set to <On>, you can change network settings. If errors related to network connections occur, an error message appears on the screen of the machine.

<Use IPv4>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv4 Settings>

Set whether to use IPv4.  <Setting an IPv4 Address>(P. 120)

<IP Address Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv4 Settings>

Specify the IPv4 address.  <Setting an IPv4 Address>(P. 120)

<DHCP Option Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv4 Settings>

Specify the optional settings for DHCP.  <Making DNS Settings>(P. 128)

<Perform DNS Dynamic Update>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <IPv4 Settings> / <IPv6 Settings>

Specify whether to perform the automatic update when the mapping between the host name and IP address is changed on an environment such as DHCP.  <Making DNS Settings>(P. 128)

NOTE

- This setting can only be specified from the Remote UI.

<PING Command>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv4 Settings>

Tests whether the IPv4 address is set correctly.  <Conducting a Connection Test for an IPv4 Address>(P. 121)

<Use IPv6>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv6 Settings>

Specify whether to use IPv6. **►Setting an IPv6 Address(P. 122)**

<Use Stateless Address>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <IPv6 Settings>

Specify whether to use the IPv6 stateless address. **►Setting an IPv6 Address(P. 122)**

NOTE

- This setting can only be specified from the Remote UI.

<Use Manual Address>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <IPv6 Settings>

Specify the IPv6 address manually. **►Setting an IPv6 Address(P. 122)**

NOTE

- This setting can only be specified from the Remote UI.

<Use DHCPv6>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <IPv6 Settings>

Specify whether to obtain the IPv6 address from the DHCP server. **►Setting an IPv6 Address(P. 122)**

NOTE

- This setting can only be specified from the Remote UI.

<Only Retrieve Stateful Address Prefix>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv6 Settings>

Specify whether to obtain only the former half of the stateful address from the DHCP server by using DHCPv6.

<DHCP Option Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <IPv6 Settings>

Specify the optional settings for DHCP. **►Making DNS Settings(P. 128)**

<DNS Server Address Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <DNS Settings>

Specify the DNS server address settings. **►Making DNS Settings(P. 128)**

<mDNS Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings> ► <DNS Settings>

Specify settings for using the DNS function on a system that does not have a DNS server.  **Making DNS Settings(P. 128)**

<LPD Print Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify settings for LPD printing. To use LPD printing, select <On> and set the time until the job is automatically canceled when the print data cannot be received due to a communication error, etc.

NOTE

- Banner pages are set to be output by print job. Even if <Output LPD Banner Page> is set to <On>, banner pages are not output for print jobs that are set to not output a banner page.

<RAW Print Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify settings for RAW printing. To use RAW printing, select <On> and set whether to use bidirectional communication and the time until the job is automatically canceled when the print data cannot be received due to a communication error, etc.

<SNTP Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify settings for Simple Network Time Protocol (SNTP).  **Making SNTP Settings(P. 138)**

<FTP Print Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify settings for FTP printing. To use FTP printing, select <On>, and set <User Name> and <Password> as necessary.

<Use UTF-8 to Display FTP Print Job Name>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify whether to use UTF-8 for displaying file names when you perform FTP print.

<WSD Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify the WSD settings. To use WSD (Web Service on Devices) for the print application, set <Use WSD Printing> to <On>. To use WSD to retrieve the information for the machine, set <Use WSD Browsing> to <On>.

NOTE

- If you set <Use WSD Printing> to <On>, <Use WSD Browsing> and <Use HTTP> are also set to <On>.

<IPP Print Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify settings for IPP printing. To use IPP printing, select <On> and set whether to only allow communication data encrypted with TLS (IPP printing) and whether to use IPP authentication.

NOTE

- If you set this to <On>, <Use HTTP> is also set to <On>.
- To perform IPPS printing, a key pair to use is required. You can use a preinstalled key pair or an original key pair generated by the machine as the key to use. For information on the key to use and the method for generating an original key pair, see [▶Generating the Key and Certificate for Network Communication\(P. 307\)](#) or [▶Registering a Key and Certificate for Network Communication\(P. 337\)](#) . If you select <RSA> for <Key Algorithm> when generating the key to use for network communication, set a key length of <1024> or longer. IPPS printing may not be able to be performed correctly if a key length of <512> is set, depending on the operating system you are using.
- To use the IPP authentication function by setting <Use Authentication> to <On>, the user information of the machine is used as the user and password for IPP authentication. Make sure to register the user information in advance when using the IPP authentication function. [▶Registering User Information in the Local Device\(P. 246\)](#)

<Multicast Discovery Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify the multicast discovery settings. [▶Monitoring the Machine From Device Management Systems\(P. 139\)](#)

<Sleep Mode Notification Settings>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <TCP/IP Settings>

Specify settings for multicast sending of the Sleep mode notifications on the network.

NOTE

- This setting can only be specified from the Remote UI.

<Use HTTP>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Enable or disable HTTP setting.

IMPORTANT

- By specifying this setting as <On>, you can open a necessary port. However, it is recommended that you specify it as <Off>, if a port is not used. If you leave the port open, an unauthorized user may access the machine.

NOTE

If you set this to <Off>, the following settings are also set to <Off>.

- <Remote UI Settings>
- <IPP Print Settings>
- <Use WSD Printing> in <WSD Settings>
- <Use WebDAV Server>

<TLS Settings>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <TCP/IP Settings>

You can set a key pair, TLS version, and encryption algorithm to use after confirming that a machine uses TLS encrypted communication. ► **Configuring the Key and Certificate for TLS(P. 303)**

NOTE

- This setting can only be specified from the Remote UI.

<Proxy Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify settings for the proxy. ► **Setting a Proxy(P. 301)**

<Confirm Auth Info When in Auth Mngt Mode>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify whether the machine checks authentication information when you print using the V4 printer driver.

NOTE

- If there is no key to use for TLS communication or it is corrupted, this setting is disabled. ► **Configuring the Key and Certificate for TLS(P. 303)**

<IPSec Settings>

<Set> ► <Preferences> ► <Network> ► <TCP/IP Settings>

Specify the IPSec settings. ► **Configuring the IPSec Settings(P. 310)**

<IPSec Policy List>

<Settings/Registration> ► <Preferences> ► <Network Settings>

You can register IPSec policies and set priorities.

NOTE

- This setting can only be specified from the Remote UI.

<TCP/IP Option Settings>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <TCP/IP Settings>

Specify the TCP option window scale and MTU size.

NOTE

- This setting can only be specified from the Remote UI.

<SNMP Settings>

<Set> ► <Preferences> ► <Network>

Specify the SNMP settings.  **Monitoring and Controlling the Machine with SNMP(P. 132)**

<Format Host Resources MIB to RFC2790>

<Set> ► <Preferences> ► <Network>

Specify whether the host resources MIB is compliant with the specifications of RFC2790.

<Dedicated Port Settings>

<Settings/Registration> ► <Preferences> ► <Network Settings>

Specify whether to configure/refer to detailed information of the machine from the Canon drivers or utility software.

NOTE

- If the setting is set to <Off>, some application that uses dedicated port may not be used.
- This setting can only be specified from the Remote UI.

<Dedicated Port Authentication Method>

<Settings/Registration> ► <Preferences> ► <Network Settings>

Specify the authentication method for the dedicated port.

NOTE

- If the setting is set to <Mode 2>, communication using a dedicated port uses a secure mode. Accordingly, you may not be able to connect from device management software or drivers, etc.
- This setting can only be specified from the Remote UI.

<Use Spool Function>

<Set> ► <Preferences> ► <Network>

Specify whether to spool print jobs that are sent to the machine in the storage device of the machine.

<Receive in Parallel>**<Set>** ▶ **<Preferences>** ▶ **<Network>**

Specify whether to efficiently process the data when multiple print jobs are sent to the machine. If this is set to **<Off>**, the data is printed in the order of reception, but the print speed may be slower.

<Waiting Time for Connection at Startup>**<Set>** ▶ **<Preferences>** ▶ **<Network>**

Specify the waiting time for connecting to a network from when the machine starts. **▶Setting the Wait Time When Connecting to a Network(P. 127)**

<Ethernet Driver Settings>**<Set>** ▶ **<Preferences>** ▶ **<Network>**

Specify the Ethernet driver settings. **▶Making Ethernet Settings(P. 126)**

<IEEE 802.1X Settings>**<Set>** ▶ **<Preferences>** ▶ **<Network>**

Specify the settings for IEEE 802.1X. **▶Configuring the IEEE 802.1X Authentication Settings(P. 317)**

 IMPORTANT

- If you set **<IEEE 802.1X Settings>** to **<On>**, the machine will not completely enter the Sleep mode.

<Outbound Filter>**<Set>** ▶ **<Preferences>** ▶ **<Network>** ▶ **<Firewall Settings>** ▶ **<IPv4 Address Filter>**

Specify the outbound filter. **▶Specifying IP Addresses in Firewall Settings(P. 289)**

<Inbound Filter>**<Set>** ▶ **<Preferences>** ▶ **<Network>** ▶ **<Firewall Settings>** ▶ **<IPv4 Address Filter>**

Specify the inbound filter. **▶Specifying IP Addresses in Firewall Settings(P. 289)**

<Always Allow Sending/Receiving Using ICMP>**<Settings/Registration>** ▶ **<Preferences>** ▶ **<Network Settings>** ▶ **<Firewall Settings>** ▶ **<IPv4 Address Filter>** ▶ **<IPv4 Address ICMP Settings>**

Specify whether to always allow ICMP communication.

NOTE

- This setting can only be specified from the Remote UI.

<Outbound Filter>**<Set>** ▶ **<Preferences>** ▶ **<Network>** ▶ **<Firewall Settings>** ▶ **<IPv6 Address Filter>**

Specify the outbound filter. **▶Specifying IP Addresses in Firewall Settings(P. 289)**

<Inbound Filter>

<Set> ► <Preferences> ► <Network> ► <Firewall Settings> ► <IPv6 Address Filter>

Specify the inbound filter. [►Specifying IP Addresses in Firewall Settings\(P. 289\)](#)

<Always Allow Sending/Receiving Using ICMP>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <Firewall Settings> ► <IPv6 Address Filter>
► <IPv6 Address ICMP Settings>

Specify whether to always allow ICMPv6 communication.

NOTE

- This setting can only be specified from the Remote UI.

<Outbound Filter>

<Set> ► <Preferences> ► <Network> ► <Firewall Settings> ► <MAC Address Filter>

Specify the outbound filter. [►Specifying MAC Addresses in Firewall Settings\(P. 292\)](#)

<Inbound Filter>

<Set> ► <Preferences> ► <Network> ► <Firewall Settings> ► <MAC Address Filter>

Specify the inbound filter. [►Specifying MAC Addresses in Firewall Settings\(P. 292\)](#)

<IP Address Block Log>

<Settings/Registration> ► <Preferences> ► <Network Settings> ► <Firewall Settings>

Displays the log for blocking with an IP address filter. [►Specifying IP Addresses in Firewall Settings\(P. 289\)](#)

NOTE

- This setting can only be specified from the Remote UI.

<Use Mopria>

<Set> ► <Preferences> ► <Network>

Specify whether to print data directly from mobile devices that support Mopria®, such as smartphones and tablets. [►Utilizing the Machine through Applications\(P. 214\)](#)

<Use AirPrint>

<Set> ► <Preferences> ► <Network>

Specify whether to print directly from an iPhone, iPad, iPod Touch, or Mac that supports AirPrint. [►Using AirPrint\(P. 217\)](#)

<Display Errors for AirPrint>

<Set> ► <Preferences> ► <Network>

Specify whether to display an error screen on the control panel if printing cannot be performed as expected due to a problem with the print data when printing with AirPrint.

If this is set to <On>, an error screen is displayed on the control panel. Cancel the job after checking the error screen. If this is set to <Off>, an error screen is not displayed on the control panel but the job remains in the job history with <Error> indicated.

<Position Information>

<Settings/Registration> ► <Preferences> ► <Network Settings>

Specify the device position information settings. [▶Using AirPrint\(P. 217\)](#)

NOTE

- This setting can only be specified from the Remote UI.

<Use IPP Everywhere>

<Set> ► <Preferences> ► <Network>

Specify whether to allow printing directly from Chromebook devices that support IPP Everywhere. [▶Utilizing the Machine through Applications\(P. 214\)](#)

<Settings for Universal Print>

<Settings/Registration> ► <Preferences> ► <Network Settings>

Specify the Universal Print settings. [▶Printing Using the Microsoft Cloud Service \(Universal Print\)\(P. 194\)](#)

NOTE

- This setting can only be specified from the Remote UI.

<Select Interface>

<Set> ► <Preferences> ► <Network>

Select whether to use a wired LAN or wireless LAN by itself, a wired LAN and wireless LAN simultaneously, or a wired LAN and another wired LAN simultaneously. [▶Selecting the Network Connection Method\(P. 108\)](#)

Selecting the Network Connection Method

- When <Main Line> is set to <Wired LAN>
Set <Sub Line> to <Wired LAN> or <Wireless LAN>.
- When <Main Line> is set to <Wireless LAN>
Set <Sub Line> to <Wired LAN>.

<Wireless LAN Settings>

<Set> ► <Preferences> ► <Network>

Specify the wireless LAN settings. [▶Connecting to a Wireless LAN\(P. 112\)](#)

<Power Save Mode>

<Set> ► <Preferences> ► <Network> ► <Wireless LAN Settings>

Specify whether to set the machine to the power save mode periodically, according to the signals sent by a wireless LAN router. [▶Connecting to a Wireless LAN\(P. 112\)](#)

<Connection Information>

<Set> ► <Preferences> ► <Network> ► <Wireless LAN Settings>

Displays the setting information of wireless LAN. ► **Check the settings and information of the wireless LAN(P. 112)**

<Use Direct Connection>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

Specify whether to use direct connection. ► **Connecting Directly(P. 210)**

<Direct Connection Type>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

Select the type of direct connection. ► **Connecting Directly(P. 210)**

NOTE

- If Wi-Fi Direct is selected, only one mobile device can connect.

<Device Name for Wi-Fi Direct>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

Specify the device name to use for direct connections (Wi-Fi Direct).

! IMPORTANT

- "-XY_Canon10" (where XY are random letters) is automatically appended to the device name for Wi-Fi Direct, unless the device name is 22 characters or more, in which case "-XY_Canon10" is not appended.

<Time Until Direct Connection Termination>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

Specify the time before communication is automatically terminated when there is a prolonged period of no data transmission/reception while communicating using direct connection.

NOTE

- This setting is disabled if <Keep Enabled If SSID/Net. Key Specified> is set to <On>.

<Access Point Mode Settings>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

Specify the settings for access point mode.

<Keep Enabled If SSID/Net. Key Specified>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

If <Use Custom SSID> and <Use Custom Network Key> are enabled in <Access Point Mode Settings>, direct connections can be made without pressing <Enable> in <Direct Connection> in <Mobile Portal>.

NOTE

- The machine can connect with multiple mobile devices at the same time. A maximum of five devices can be connected at the same time.
- If this is set to <On>, the <Time Until Direct Connection Termination> setting is disabled.
- If this is set to <On>, the machine will not enter the Sleep mode completely.

<Direct Connection IP Address Settings>

<Set> ► <Preferences> ► <Network> ► <Direct Connection Settings>

Specify the IP address to distribute to mobile devices connecting using direct connection.

NOTE

- The IP address distributed to mobile devices may be up to nine numbers greater than the value of the specified IP address.

<Session Settings>

<Settings/Registration> ► <Preferences> ► <Network Settings>

Specify the timeout time after logging in to the Remote UI.

NOTE

- This setting can only be specified from the Remote UI.

<IP Address Settings>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings>

Specify the IPv4 address to use with a wireless LAN (sub line) when using both a wired LAN and wireless LAN at the same time.

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Priority Line for Comm w/ Mobile Devices>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings>

Select the line to connect mobile devices to when using both a wired LAN (main line) and wireless LAN (sub line) at the same time.

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Ethernet Driver Settings>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings>

Specify the Ethernet driver settings for the sub line. **► Making Ethernet Settings(P. 126)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<IEEE 802.1X Settings>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings>

Specify the IEEE 802.1X settings for the sub line. **► Configuring the IEEE 802.1X Authentication Settings(P. 317)**

<Outbound Filter>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Firewall Settings> ► <IPv4 Address Filter>

Specify the transmission filter in the sub line settings. **► Configuring the Firewall in IP Addresses of the Sub Line(P. 295)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Inbound Filter>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Firewall Settings> ► <IPv4 Address Filter>

Specify the reception filter in the sub line settings. **► Configuring the Firewall in IP Addresses of the Sub Line(P. 295)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Outbound Filter>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Firewall Settings> ► <MAC Address Filter>

Specify the transmission filter in the sub line settings. **► Configuring the Firewall in MAC Addresses of the Sub Line(P. 298)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Inbound Filter>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Firewall Settings> ► <MAC Address Filter>

Specify the reception filter in the sub line settings. **► Configuring the Firewall in MAC Addresses of the Sub Line(P. 298)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<DNS Server Address Settings>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Settings for System Data Communication>

Specify the DNS server address settings for the sub line. **► Making DNS Settings(P. 128)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Proxy Settings>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Settings for System Data Communication>

Specify the proxy settings for the sub line. **► Setting a Proxy(P. 301)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Select Line to Use>

<Set> ► <Preferences> ► <Network> ► <Sub Line Settings> ► <Settings for System Data Communication>

Select the line to use for system data communication. **► Configuring System Data Communication(P. 140)**

Configure the sub line settings when a setting other than <Off> is selected for <Sub Line> in <Select Interface>.

<Static Routing Settings>

<Set> ► <Preferences> ► <Network>

Specify the static routing settings for IPv4 addresses. ► **Setting Static Routing(P. 136)**

<External Interface>

E9SJ-08R

This section describes the USB settings.

<Use as USB Device>

<Set> ► <Preferences> ► <External Interface> ► <USB Settings>

You can set whether to use the machine as a USB device.

NOTE

- If this is set to <Off>, print jobs from a computer connected via USB cable cannot be performed.
- Changes in settings are effective after performing <Apply Set. Changes> on the <Home> screen.

<Use MEAP Driver for USB Storage Device>

<Set> ► <Preferences> ► <External Interface> ► <USB Settings>

You can set whether to use the MEAP driver for USB external storage.

IMPORTANT

- Depending on the type of MEAP application that uses USB external memory device, you may need to set this to <On>. To check whether you need to set this to <On>, see the manual for the MEAP application you are using, or contact your dealer or service representative.

NOTE

- Changes in settings are effective after performing <Apply Set. Changes> on the <Home> screen.

<Use USB Storage Device>

<Set> ► <Preferences> ► <External Interface> ► <USB Settings>

You can set whether to allow the use of USB external storage devices.

NOTE

- Changes in settings are effective after performing <Apply Set. Changes> on the <Home> screen.

<Restrict Auto Install of Printer Driver>

<Set> ► <Preferences> ► <External Interface> ► <USB Settings>

This enables you to prevent a new printer driver from being installed when switching machines with multiple machines connected via USB.

IMPORTANT

- Set this to <Off> when using a USB hub to connect multiple machines.

NOTE

- Changes in settings are effective after performing <Apply Set. Changes> on the <Home> screen.

<Accessibility>

E9SJ-08S

This section describes settings for improving accessibility, such as inverting the screen colors and setting the message display time.

<Key Repetition Settings>

<Set> ► <Preferences> ► <Accessibility>

You can set the amount of time before characters start repeating when you hold down a key on the control panel, as well as the interval between repetitions.

<Acceptance Delay for Repeated Presses>

<Set> ► <Preferences> ► <Accessibility>

You can specify the amount of time during which the machine does not accept the second and subsequent key inputs when a key on the on-screen keyboard is unintentionally pressed repeatedly. Configure this setting in cases such as when you intend to enter a single character, but the same character is entered repeatedly.

<Invert Screen Colors>

<Set> ► <Preferences> ► <Accessibility>

You can invert the screen colors of the display. If you find it hard to view the display even after adjusting <Backlight Brightness>, try specifying this setting.

<Contrast>

<Set> ► <Preferences> ► <Accessibility>

You can adjust the contrast (the difference between the light and dark parts) of the display to suit the installation location of the machine.

<Backlight Brightness>

<Set> ► <Preferences> ► <Accessibility>

You can adjust the brightness of the display to suit the installation location of the machine.

<Message Display Time>

<Set> ► <Preferences> ► <Accessibility>

You can specify the interval in seconds at which two different messages are alternately displayed.

<Scrolling Speed>

<Set> ► <Preferences> ► <Accessibility>

You can adjust the scrolling speed of the screen by selecting from three levels.

<Volume Settings>

E9SJ-08U

All the settings used to generate the confirmation sound of a key being pressed, the sound indicating completion of the printing process, and other sounds, are listed with descriptions.

NOTE

- For information about the setting procedures, see  **Setting Sounds(P. 163)** .

<Entry Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound when a key on the control panel has been pressed.

<Invalid Entry Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound when an invalid key operation has been performed, for example, when an invalid numeric value has been entered.

<Restock Supplies Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound that indicates the end of toner cartridge lifetime is approaching.

<Warning Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound telling that a trouble has occurred on the machine, such as a paper jam, incorrect operation, or press of an inoperable key.

<Job Done Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound when printing has been completed.

<Sleep Mode Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound when the machine enters or exits the sleep mode.

<Login Tone>

<Set> ► <Preferences> ► <Volume Settings>

You can set whether to produce a sound when login is successful.

<Adjustment/Maintenance>

E9SJ-08W

Item	Description
▶<Adjust Image Quality>(P. 470)	This section describes how to adjust image quality for printing.
▶<Maintenance>(P. 474)	This section describes how to use the auto cleaning function for the main unit.

<Adjust Image Quality>

E9SJ-08X

This section describes how to adjust image quality for printing.

<Adjust Print Position>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality>

You can adjust the print position when printing is lopsided or protruding from the print range.  **Adjusting the Print Position(P. 500)**

<Waterdrop Pattern Prevention Mode>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

You can set <Waterdrop Pattern Prevention Mode> for when a splattered image, white patches, streaks, etc. appear on the halftone images of two sided print jobs. Immediately after you turn ON the machine in a low temperature environment, if the halftone reproduction of the printout becomes significantly different from the original document, set this mode to <On>.

NOTE

- If you set <Waterdrop Pattern Prevention Mode>, the printing speed for the first sheet becomes slower.

<Reduce Paper Sticking at Output>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

In 2-sided printing, printed paper may stick to each other depending on the image density of print data. In this case, setting this item to <On> may solve the problem.

NOTE

- If you set to <On>, the printing speed may be slower.

<Reduce Ghosting>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

When you print on large size paper after printing on small size paper, afterimages may appear in blank areas. In this case, setting this item to <On> may solve the problem.

NOTE

- If you set to <On>, the printing speed may be slower.

<Reduce Wrinkles (from Humidity)/Streaks>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

If printouts have creases when damp paper is used or if streaks appear in the leading edge of paper when images with halftones such as photos are printed, setting to <On> may solve the problem.

NOTE

- If you set to <On>, the printing speed may be slower.

<Paper Wrinkle Correction>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

Printouts may wrinkle depending on the paper to use. In this case, setting this item to <On> may solve the problem.

NOTE

- If you set to <On>, the print may be faded or the printing speed may be slower.

<Streak Prevention>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

Streaks may appear on printouts depending on the paper type or the environmental conditions. In this case, setting this item may solve the problem. The improvement effect is weakest with <Mode 1> and strongest with <Mode 4>.

NOTE

- As the improvement effect is increased, the print density becomes lighter. In addition, the edges may be blurred or roughness may be slightly emphasized.
- If you select <Mode 3> or <Mode 4>, the printing speed may be slower.

<Curl Prevention Mode>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

You can set <Curl Prevention Mode> to reduce curling on the end of paper due to the heat and pressure of the fixing assembly during printing.

NOTE

- If this setting is set to <On>, it may affect the printing quality.

<Quiet Mode>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

When printing sounds bother you, set this item to <On>.

NOTE

- If you set to <On>, the printing speed may be slower.

<Adjust Fixing Level for Envelopes>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

When printing on envelopes, if their flaps are glued (which they should not be) or toner fixation is poor, you can adjust the fixing level.

NOTE

- If toner fixation is poor, set this to <Standard>. When you set this to <Standard>, the printing speed may be slower.
- If toner fixation is still poor even when <Standard> is set, set this to <High>. When you set this to <High>, the printing speed may be slower.

<Reduce Toner Flaking from Postcards>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Special Processing>

When you print on postcard, toner may come off printed images depending on the environmental conditions. In this case, setting this item to <On> may solve the problem.

NOTE

- If this setting is set to <On>, the paper may curl.

<Adjust Standard Density>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality>

If the density of the printing is significantly different from the original document, this adjusts the overall density of the printed material to be closer to the original, including filled areas, text, lines, and intermediate densities.

🔴 **Adjusting the Standard Density(P. 503)**

<Adjust Density for Specific Paper>

<Set> ► <Adjustment/Maintenance> ► <Adjust Image Quality>

When printing become faint on some paper after the toner cartridge is used for a long time, this setting may improve this problem.

NOTE

- This setting is only valid for the following paper types.
 - Heavy
 - Bond
 - Letterhead 3

- Letterhead 4
- Letterhead 5
- Letterhead 6
- Label
- Postcard
- Envelope
- Set a lower value to reduce the print density and a higher value to increase the print density.
- Changing this setting also changes the toner consumption.

<Maintenance>

E9SJ-08Y

This section describes how to use the auto cleaning function for the main unit.

<Clean Pressure Roller for Fixing>

<Set> ► <Adjustment/Maintenance> ► <Maintenance>

If printed paper is dirty, execute <Clean Pressure Roller for Fixing>.

<Function Settings>

E9SJ-090

This section describes the settings for functions.

NOTE

- Some settings can only be set by the Administrator.
- Some of the settings may not be displayed depending on the configuration of optional equipment installed on the machine.

Item	Description
▶<Common>(P. 476)	This section describes settings for functions such as Paper Feed Settings, Paper Output Settings, and Print Settings.
▶<Printer>(P. 479)	This section describes how to specify printer settings.
▶<Send>(P. 481)	This section describes how to specify E-mail settings.
▶<Receive>(P. 482)	This section describes how to specify receive settings.
▶<Access Files>(P. 483)	This section describes the settings for printing stored files.
▶<Print>(P. 484)	This section describes the print settings.

<Common>

E9SJ-091

This section describes settings for functions such as Paper Feed Settings, Paper Output Settings, and Print Settings.

NOTE

- Some of the settings may not be displayed depending on the configuration of optional equipment installed on the machine.

<Paper Source Auto Selection>

<Set> ▶ <Function Settings> ▶ <Common> ▶ <Paper Feed Settings>

You can configure the paper source that will be used when printing with <Select Paper> set to <Auto>. This setting also functions when the paper in the current paper source runs out during printing.  **Automatically Selecting the Appropriate Paper Source for a Specific Function (P. 60)**

<Switch Paper Feed Method>

<Set> ▶ <Function Settings> ▶ <Common> ▶ <Paper Feed Settings>

When regularly using paper with logos such as letterheads, while printing in both one-sided and two-sided, you can set this setting to <Print Side Priority> to print the first page on the front side for both one-sided and two-sided, without having to change the paper orientation.  **Loading Preprinted Paper(P. 48)**

IMPORTANT

- The settings for Automatic Paper Selection and Auto Drawer Switching are disabled for paper sources with <Print Side Priority> set. The print speed is also slower when performing one-sided printing.

NOTE

- <Print Side Priority> is only enabled when paper that can be printed on both sides is set ( **Paper Available for Two-Sided Printing(P. 96)**).
- For instructions on loading paper, see  **Loading Preprinted Paper(P. 48)** .

<Suspended Job Timeout>

<Set> ▶ <Function Settings> ▶ <Common> ▶ <Paper Feed Settings>

If this setting is set to <On> and a job is suspended due to a lack of paper, etc., the machine automatically prints the next job after the specified time period.

NOTE

- If a job is suspended because paper has run out during the job, the next job is not processed even after the designated suspension time elapses.
- To automatically delete suspended jobs, see  **<Auto Delete Suspended Jobs>(P. 477)** .

<Job Separator Between Jobs>

<Set> ► <Function Settings> ► <Common> ► <Paper Output Settings>

This enables you to insert the specified paper at the start of each job when multiple jobs are printed consecutively.

<Job Separator Between Copies>

<Set> ► <Function Settings> ► <Common> ► <Paper Output Settings>

This enables you to insert the specified paper each number of copy sets to divide the sets. If you set this, paper is inserted when printing with Collate (Page Order).

 IMPORTANT

- If you are using the Group (Same Pages) mode, you cannot insert job separation sheets between copy sets.

<Print Priority>

<Set> ► <Function Settings> ► <Common> ► <Print Settings>

A job that has a higher set priority can be set to print after the job currently being processed is complete.

NOTE

- If the same printing priority has been specified for multiple functions, printing starts with the first processed print job.
- Priority printing does not take place until the current job is complete. However, if the current job is paused, the printing of another job may start, depending on its settings.

<Auto Delete Suspended Jobs>

<Set> ► <Function Settings> ► <Common> ► <Print Settings>

If this setting is set to <On> and a job is suspended due to a paper jam, etc., the machine automatically deletes the job after the specified time period.

NOTE

- To retain a suspended job without automatically deleting it, see  **<Suspended Job Timeout>(P. 476)** .

<Action When Remaining Toner Is Low>

<Set> ► <Function Settings> ► <Common> ► <Print Settings>

You can set the print operation when the remaining toner in the toner cartridge is low. You can also set whether to display the restock toner message.

NOTE

- When set to <Display Warning Screen>, <Displ Tnr Cart Warning> is set to <On>.

<Printer>

E9SJ-092

This section describes the printer settings.

<Printer Settings>

<Set> ► <Function Settings> ► <Printer>

Specify the printer settings.

For more information, see Setting the Machine (PS/PCL/UFR II Printer).

<Restrict Printer Jobs>

<Set> ► <Function Settings> ► <Printer>

If this setting is set to <On>, you can restrict jobs from the printer driver.

<Switch Paper Source Auto Selection Mode>

<Set> ► <Function Settings> ► <Printer>

You can select which paper to prioritize when both horizontal paper and vertical paper are loaded and set as the target for automatic paper selection.

<Feed from MP Tray When No Paper Source>

<Set> ► <Function Settings> ► <Printer>

If this setting is set to <On>, you can display a message prompting the user to load paper in the multi-purpose tray when the paper specified with automatic paper selection is not found.

<MP Tray Priority for Ppr Src Auto Select>

<Set> ► <Function Settings> ► <Printer>

If this setting is set to <On>, printing on the paper loaded in the multi-purpose tray is prioritized.

<PDL Selection (Plug and Play)>

<Set> ► <Function Settings> ► <Printer>

Select default Page Description Language (PDL).

<Ppr Size Mismatch for Free Size Ppr Src>

<Set> ► <Function Settings> ► <Printer>

When printing on free size paper, the machine detects whether the size of the loaded paper matches the print settings.

<Vertical Printing Priority for Free Size>

<Set> ► <Function Settings> ► <Printer>

You can set the orientation for printing on free size paper.

<PS Password Settings>

<Set> ► <Function Settings> ► <Printer>

You can specify the password that restricts the use of the control command prepared by the PS printer.

NOTE

- <SystemParams Password> is a password that allows changes to the system parameter, and <StartJob Password> is a password that allows startjob, exitserver operator to perform. For more information, check PostScript language specifications.

<Paper Feed Mode When Using PCL Emulation>

<Set> ► <Function Settings> ► <Printer>

You can set the paper source used for the PCL5 PaperSource command.

NOTE

- For details on each setting, see Setting the Machine (PS/PCL/UFR II Printer).

<Send>

E9SJ-093

This section describes how to specify the e-mail print settings.

<Communication Settings>

<Set> ► <Function Settings> ► <Send> ► <E-mail Settings>

You can configure the settings for using the e-mail print function. Other settings related to e-mail printing, such as the settings for a mail server, must be configured from the Remote UI. [▶Configuring E-Mail Print Settings\(P. 143\)](#)

IMPORTANT

- If you set shorter than 10 minutes (excluding '0 min') for <POP Interval>, the machine will not completely enter the Sleep mode.

<Confirm TLS Certificate for POP RX>

<Set> ► <Function Settings> ► <Send> ► <E-mail Settings>

You can check whether the TLS server certificate is valid when receiving with POP. You can verify the validity of the certificate and reliability of the certificate chain, as well as confirm the CN (Common Name).

IMPORTANT

- If you do not verify the certificate, TLS communication is performed, even with an invalid certificate.

NOTE

- If there is a problem with the certificate, POP receiving will fail.

<Receive>

E9SJ-094

This section describes how to specify receive settings.

<Print on Both Sides>

<Set> ► <Function Settings> ► <Receive> ► <Common Settings>

You can select whether to print received documents on both sides of paper.

<Reduce RX Size>

<Set> ► <Function Settings> ► <Receive> ► <Common Settings>

You can select whether to reduce received documents so that the whole document is printed within the printable area of the paper.

NOTE

- If this setting is set to <Off>, the image size of the received file is not reduced to fit the size of the paper. If the size of the image exceeds the printable area, the image is divided into equal sections and printed onto separate sheets of paper.
- If you select <Auto> in <Reduction Mode>, the image size is automatically reduced by a suitable reduction ratio. This ratio can range from the value set for <Reduction Ratio>, up to 100% of the received document size.

<RX Page Footer>

<Set> ► <Function Settings> ► <Receive> ► <Common Settings>

You can select whether to print information, such as reception time and page number, at the bottom of received documents.

NOTE

- When an e-mail without a body is received, the From information and Subject information (up to 24 characters for each) is printed at the top of the first page of the attachment file.

<Access Files>

E9SJ-095

This section describes the settings for printing stored files.

<Change Default Set. (Memory Media Print)>

<Set> ▶ <Function Settings> ▶ <Access Files> ▶ <Common Settings> ▶ <Access Stored Files Settings>

You can change the settings registered as default for the <Access Stored Files> function.

<Use Print Function>

<Set> ▶ <Function Settings> ▶ <Access Files> ▶ <Memory Media Settings>

Specifying this setting enables you to print files in memory media. ▶ **Restricting the Use of Memory Media(P. 325)**

<Select Option When Connecting Mem. Media>

<Set> ▶ <Function Settings> ▶ <Access Files> ▶ <Memory Media Settings>

You can set whether to display the print settings screen when memory media is connected. ▶ **Connecting a USB Memory Device(P. 20)**

<Print>

E9SJ-096

This section describes the print settings.

<Job Storage Period>

<Set> ▶ <Function Settings> ▶ <Print>

Specify the time period for storing jobs.

<Job List Display Settings>

<Set> ▶ <Function Settings> ▶ <Print>

Specify the job types to be included in the job list, and the job type to be selected by default.

<Management Settings>

E9SJ-097

You can configure the settings related to management of users, devices, and data, etc., for secure and efficient use of the machine.

Item	Description
▶<User Management>(P. 486)	You can configure the settings for managing users of the machine.
▶<Device Management>(P. 487)	You can manage information about the hardware and operations, as well as various data required when using the machine functions.
▶<License/Other>(P. 489)	You can register licenses and configure the settings related to the software and system options available for the machine.
▶<Data Management>(P. 491)	You can configure settings for utilizing data such as the machine settings information and initializing data.
▶<Security Settings>(P. 493)	You can configure settings related to system modification.

<User Management>

E9SJ-098

You can configure the settings for managing users of the machine with a user authentication application.

<Set Administrator Password>

<Set> ► <Management Settings> ► <User Management> ► <Authentication Management>

You can change the password used by the Administrator for logging into the Remote UI. When changing the password again, it can only be specified from the Remote UI.

NOTE

- Make sure that you do not forget your password. If you forget your password, contact your dealer or service representative.

<Set Administrator PIN>

<Set> ► <Management Settings> ► <User Management> ► <Authentication Management>

Set whether to require the user to enter a PIN when changing settings that require Administrator privileges from the control panel. The Administrator PIN can also be changed.

NOTE

- Make sure that you do not forget your PIN. If you forget your PIN, contact your dealer or service representative.

<System Manager Information Settings>

<Set> ► <Management Settings> ► <User Management>

Set the System Manager information for the machine. ► **Changing the System Manager ID and PIN(P. 277)**

<Department ID Management>

<Set> ► <Management Settings> ► <User Management>

Select whether to manage users in groups by assigning users to Department IDs. ► **Configuring the Department ID Management Settings(P. 279)**

NOTE

- You can only select whether to use Department ID Management here. The Remote UI must be used to register department IDs or check the usage status of each department ID.

<Device Management>

E9SJ-099

You can specify settings related to the management of the device and optional products.

<Device Information Settings>

<Set> ► <Management Settings> ► <Device Management>

Enter the name and the installation location to identify the machine.

<Display Job Status Before Authentication>

<Set> ► <Management Settings> ► <Device Management>

Select whether to restrict access to the <Status Monitor> screen when using a login service.

<Restrict Access to Other User Jobs>

<Set> ► <Management Settings> ► <Device Management>

Select whether to restrict users from performing operations on the jobs of other users on the <Status Monitor> screen when User Authentication is used.

<Display Job Log>

<Set> ► <Management Settings> ► <Device Management>

Select whether to display job logs on the <Status Monitor> screen. You can also select whether to allow device management software to retrieve job logs from the machine. ► **Basic Screens(P. 150)**

<Save Audit Log>

<Set> ► <Management Settings> ► <Device Management>

Select whether to start log recording. For information on the types of logs, see ► **Management Functions(P. 602)** .

► **Starting Log Recording(P. 352)**

<Retrieve Network Authentication Log>

<Set> ► <Management Settings> ► <Device Management>

Select whether to start log recording for authentication performed when the machine is accessed via the network, such as when printing from a computer.

<Restrict Service Representative Access>

<Set> ► <Management Settings> ► <Device Management>

You can set the machine to restrict changes in user information or security-related settings when the machine is inspected or repaired by your dealer or service representative.

NOTE

- Even when this is not set to <On>, you can check the audit log for past operations if the service representative has changed user information or security-related settings.

<Dsply Cnsmbls Purchase Bttn in Remote UI>

<Set> ► <Management Settings> ► <Device Management> ► <Remote UI/Toner Status Cnsmbls Info Set.>

Select whether to display a button for accessing the website for purchasing toner cartridges on the Remote UI.

<Toner Status Settings>

<Set> ► <Management Settings> ► <Device Management> ► <Remote UI/Toner Status Cnsmbls Info Set.>

Select whether to use the toner cartridge level notification tool. You can also set whether to display a button for accessing the website for purchasing toner cartridges on the toner cartridge level notification tool.

<Prohibit Initialization of Admin. Pswrd.>

<Set> ► <Management Settings> ► <Device Management>

Set whether to restrict the operation of <Initialize Administrator Password> in <Check Counter>.

<Restrict Special Mode Operations>

<Set> ► <Management Settings> ► <Device Management>

Select whether to restrict use of Special Mode, which is provided for the purpose of maintenance by service representatives.

<Canon Genuine Mode>

<Set> ► <Management Settings> ► <Device Management>

This mode is for genuine cartridges.

NOTE

- A service technician may change the settings. If the menu is not displayed, contact the administrator of the machine.

<License/Other>

You can register licenses and configure the settings related to the software and system options available for the machine.

<Register License>

<Set> ► <Management Settings> ► <License/Other>

Enter the license key for a system option that can be used on the machine. [▶Installing System Options\(P. 373\)](#)

<Use TLS>

<Set> ► <Management Settings> ► <License/Other> ► <MEAP Settings>

Select whether to use TLS communication when a MEAP application is used by accessing the machine via a Web browser.

NOTE

- You need to configure the key and certificate before setting this setting to <On>. [▶Configuring the Key and Certificate for TLS\(P. 303\)](#)
- Changes made for this setting are also applied to <Use TLS> in [▶<Remote UI Settings>\(P. 489\)](#) .

<Confirm TLS Certificate Using MEAP App>

<Set> ► <Management Settings> ► <License/Other> ► <MEAP Settings>

Select whether to verify TLS server certificates and their common names (CN) when TLS communication is used for a MEAP application.

<Use DNS Caching>

<Set> ► <Management Settings> ► <License/Other> ► <MEAP Settings>

Select whether to save DNS information from successful searches via a MEAP application to memory. You can also set an expiration date if you choose to save information temporarily.

<Use Proxy Settings of This Device>

<Set> ► <Management Settings> ► <License/Other> ► <MEAP Settings>

Select whether to use the proxy settings of the machine with MEAP applications. [▶Setting a Proxy\(P. 301\)](#)

<Add X-FRAME-OPTIONS to HTTP Header>

<Set> ► <Management Settings> ► <License/Other> ► <MEAP Settings>

When the HTTP server returns a response, it appends X-FRAME-OPTIONS to the header to prevent contents created by other servers from overlapping.

<Remote UI Settings>

<Set> ► <Management Settings> ► <License/Other>

Select whether to use the Remote UI to operate the machine and change settings.

<Remote Operation Settings>

<Set> ► <Management Settings> ► <License/Other>

Select whether to enable the Remote Operation function. This function enables you to specify settings and process jobs from a computer by displaying the screen of the machine on the computer screen.

<Register/Update Software>

<Set> ► <Management Settings> ► <License/Other>

You can install system options/MEAP applications in the machine. ► **Installing System Options(P. 373)**

<Start Setup Guide>

<Set> ► <Management Settings> ► <License/Other>

You can follow the wizard instructions to configure the machine's initial settings. ► **Setting up Using the Setup Guide(P. 104)**

<Data Management>

E9SJ-09C

You can configure settings for utilizing data such as the machine settings information and initializing data.

<Import from USB Memory>

<Set> ► <Management Settings> ► <Data Management> ► <Import/Export>

You can import all the settings information from a USB memory device.

NOTE

- If USB memory is already connected to the machine, that USB memory will be recognized as the media to use for importing, even if you connect new USB memory. Select <Remove Memory Media>, remove the connected USB memory, and then connect the desired USB memory.

<Export to USB Memory>

<Set> ► <Management Settings> ► <Data Management> ► <Import/Export>

You can export all the settings information into a USB memory device.

NOTE

- You cannot select which settings to export when exporting to USB memory. All settings are batch exported.
- If USB memory is already connected to the machine, that USB memory will be recognized as the media to use for exporting, even if you connect new USB memory. Select <Remove Memory Media>, remove the connected USB memory, and then connect the desired USB memory.

<Restrict Import/Export from Web Service>

<Set> ► <Management Settings> ► <Data Management> ► <Import/Export>

Select whether to restrict import and export operations with Web applications other than the Remote UI.

<Initialize Network Settings>

<Set> ► <Management Settings> ► <Data Management>

You can restore all of the network settings to the factory default values.  **Initializing Settings(P. 376)**

<Initialize All Set. without Network Set.>

<Set> ► <Management Settings> ► <Data Management>

You can restore all of the machine settings to the factory default values.  **Initializing Settings(P. 376)**

NOTE

- <Network> is not initialized.

<Initialize All Data/Settings>

<Set> ▶ <Management Settings> ▶ <Data Management>

Select to restore all of the machine settings to the factory default values and completely erase the data stored in the machine. It is not normally necessary to use this setting, but it is useful to erase personal or confidential information when disposing of the machine. ▶ **Initializing Settings(P. 376)**

<Security Settings>

E9SJ-09E

You can configure settings related to system modification.

<Verify System at Startup>

<Set> ► <Management Settings> ► <Security Settings> ► <System Verification Settings>

You can set the machine to verify the integrity of the firmware and applications installed in the machine during startup.

IMPORTANT

- This function restarts the machine not only when the setting is changed from <Off> to <On> but also when <Apply> is selected without changing the setting from <On>. To avoid restarting the machine without changing the setting from <On>, select <No> on the confirmation screen and then navigate from the screen for this function.

NOTE

- When this function is set to <On>, startup takes longer than when it is set to <Off> because system verification is performed.
- The following events and results are recorded to the device management log.  **Managing the Logs(P. 352)**

Event	Firmware verification, Verification of the applications installed in the machine
Result	Success, Failure

- If an error code is displayed on the screen when the machine is started with this setting set to <On>, contact your dealer or service representative.

<Trellix Embedded Control>

<Set> ► <Management Settings> ► <Security Settings> ► <System Verification Settings>

When the machine is operating, the Trellix Embedded Control function is used to prevent unauthorized program modification and the execution of unauthorized programs, for improved system reliability.

NOTE

- To set this function to <On>, it is necessary to set <Verify System at Startup> to <On> in advance.
- When this function is set to <On>, startup takes longer than when it is set to <Off>.

<Recommended Security Set. for Usage Env.>

<Set> ► <Management Settings> ► <Security Settings>

You can now specify all the recommended security settings for your usage environment simply by selecting the machine's environment type. See "Security Settings Navigator" for the available environment types. **Security Settings Navigator**

IMPORTANT

- If any of the machine's security policy settings have been specified, <Recommended Security Set. for Usage Env.> cannot be used.

NOTE

- If you change the machine to the recommended security settings for each type, functions you want to use may become unavailable or other problems may occur. In this case, you can undo the changes and restore the previous security settings.
If you manually changed settings that were changed with <Recommended Security Set. for Usage Env.>, the changes are not retained. The machine returns to the state before executing <Recommended Security Set. for Usage Env.>.

<Output Report>

E9SJ-09F

This section describes settings regarding report output.

<2-Sided Printing>

<Set> ► <Output Report> ► <Default Settings for Output Report>

You can output reports such as the print history and settings list with two-sided printing.

<Consumables Status Report>

<Set> ► <Output Report> ► <Print List>

You can print a report to check the status of the consumables in the machine.

<User Data List>

<Set> ► <Output Report> ► <Print List>

You can check the settings of the machine and their current values in a list.

NOTE

- Network settings are not printed to the user data list.
- Items that have been changed from their default settings are printed with an asterisk (*) next to them.

<Network User Data List>

<Set> ► <Output Report> ► <Print List>

You can check the network settings of the machine and their current values in a list. Information regarding security, such as the address filter and IPSec settings, are also printed.

NOTE

- Items that have been changed from their default settings are printed with an asterisk (*) next to them.
- The following items are automatically generated from unique information of the machine by default and when the settings are initialized, and have an asterisk (*) next to them.
 - IPv4 Host Name
 - IPv6 Host Name
 - mDNS Name (mDNS Settings)
 - Current Transmission Speed (Ethernet Driver Settings)

<Communication Management Report>

<Set> ► <Output Report> ► <Print List>

You can print a report to check the history of the e-mail received with the machine, including the subject and reception date/time.

<Page Count List>

<Set> ► <Output Report> ► <Print List>

You can print a report to check the print count* for each user (department ID) in Department ID Management.

* In this report, the numbers are based on printed sides of the page. For example, the count is 1 if you print on one side of a page, and the count is 2 if you print on both sides of the page.

NOTE

- Department ID Management must be set in order to calculate the Page Count List for each Department ID. Setting the Department ID Management
- With the Remote UI Page Count List, you can check how many pages have been printed by individual user names linked to a Department ID. To display the list, **▶ Starting the Remote UI(P. 329)** ► click [Settings/Registration] ► [User Management] ► [Department ID Management]. However, note that user names will not be displayed if multiple users are allocated to the same Department ID, or if you are using Department ID Authentication as the login service.
- The Page Count List can also be saved as a CSV file using the Remote UI. **▶ Starting the Remote UI(P. 329)** ► click [Settings/Registration] ► [User Management] ► [Department ID Management] ► [Store in CSV Format].

<Counter Report>

<Set> ► <Output Report> ► <Print List>

You can print a report to check the total number of all printed pages.

<Print Log List>

<Set> ► <Output Report> ► <Print List>

The following print history can be checked in a report.

- History of documents printed from a computer
- History of e-mail received and printed
- History of printing setting lists and reports

<IPSec Policy List>

<Set> ► <Output Report> ► <Print List>

You can check a list of the settings for the IPSec policies registered in the machine.

<MEAP System Information>

<Set> ► <Output Report> ► <Print List>

You can check a list of the information for the applications installed in the machine and some system application information.

<Import Result Report>

<Set> ► <Output Report> ► <Print List>

You can check the results of importing in a report.

<Toner Cartridge Log Report>

<Set> ▶ <Output Report> ▶ <Print List>

You can check the usage history of toner cartridges in a report.

<PCL>

<Set> ▶ <Output Report> ▶ <Print List>

You can check the PCL settings of the machine, their current values, and available fonts in a list.

<PS>

<Set> ▶ <Output Report> ▶ <Print List>

You can check the PS settings of the machine, their current values, and available fonts in a list.

Adjusting Print Quality

Adjusting Print Quality	499
Adjusting the Print Position	500
Adjusting the Standard Density	503
Adjusting Density for Specific Paper	504

Adjusting Print Quality

E9SJ-09H

Adjust the settings below if printing results are not satisfactory.

■ Print Position Adjustment

You can adjust the print position when printing is lopsided or protruding from the print range.

▶ Adjusting the Print Position(P. 500)

■ Standard Density Adjustment

If the density does not improve by performing density adjustment, it may be able to be improved by correcting the standard density.

▶ Adjusting the Standard Density(P. 503)

■ Density Adjustment for Specific Paper

When printing become faint on some paper after the toner cartridge is used for a long time, this setting may improve this problem.

▶ Adjusting Density for Specific Paper(P. 504)

Adjusting the Print Position

You can adjust the print position when printing is lopsided or protruding from the print range. The print position can be adjusted for each paper source.



NOTE

- Ensure that the following are set correctly before performing print position adjustment.
 - Setting the paper source to adjust (**Custom Settings(P. 423)** ▶ <Paper Feed> ▶ <Default Paper Feed Source>)
 - Setting the print mode (1-Sided/2-Sided) to adjust (**Custom Settings(P. 423)** ▶ <2-Sided Printing>)
 - Setting the paper type to feed **Specifying Paper Size and Type(P. 51)**
- When performing print position adjustment, set the correct paper type for the paper source, rather than selecting <Free>.

▶ **Step 1: Printing the Current Print Position(P. 500)**

▶ **Step 2: Confirming the Direction and Distance for Adjustment(P. 500)**

▶ **Step 3: Adjusting the Print Position for Each Paper Source(P. 501)**

Step 1: Printing the Current Print Position

You can print a sample print to confirm the direction and distance for adjustment.

- 1** Select <Set> on the <Home> screen. ▶ **<Home> Screen(P. 150)**
- 2** Select <Adjustment/Maintenance> ▶ <Adjust Image Quality> ▶ <Adjust Print Position>.
- 3** Select <Print Sample> ▶ <Yes>, and press **OK**.

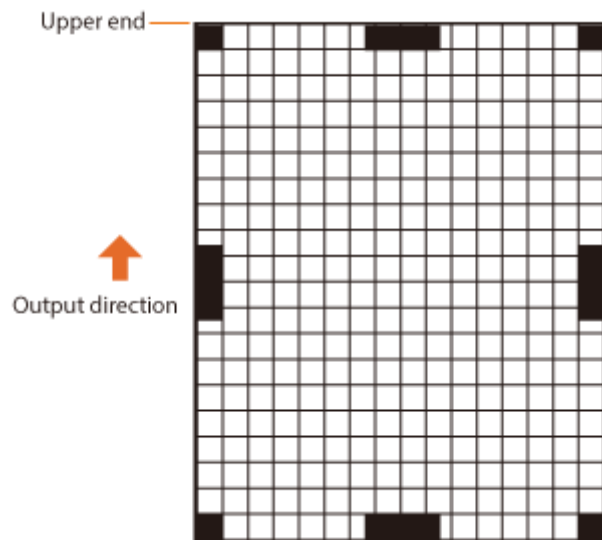
▶▶▶ A sample print is output.

Step 2: Confirming the Direction and Distance for Adjustment

Marks for confirming the print position are printed on the sample print. The position of these marks determines the direction and distance for adjustment. Normally, all marks are printed on the edge of the paper.

Viewing the Sample Print

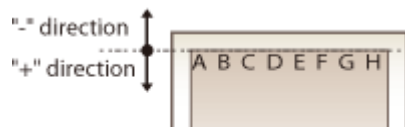
The lead edge of the output paper is the top edge of the sample print. Remember which edge is the top edge when picking up the paper.



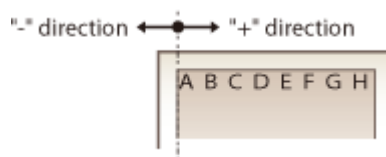
When the Print Position Is Lopsided

Print position adjustment is required when the marks for confirming the print position are lopsided. The direction of the print position can be specified using a positive value (+) or negative value (-), and the distance can be specified in millimeters. To perform vertical adjustment, set a negative value (-) to move the print position up or a positive value (+) to move the print position down. To perform horizontal adjustment, set a negative value (-) to move the print position left or a positive value (+) to move the print position right.

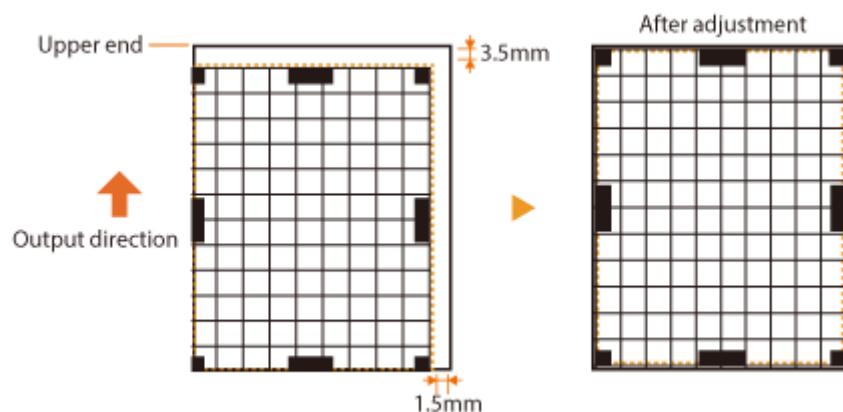
Vertical direction



Horizontal direction



In the following example, because it is necessary to shift the print position 3.5 mm up and 1.5 mm to the right, specify -3.5 mm in the vertical direction and +1.5 mm in the horizontal direction.



Step 3: Adjusting the Print Position for Each Paper Source

Adjust the print position after confirming the direction and distance for adjustment. The print position can be adjusted in the range -3.5 mm to +3.5 mm in both the horizontal and vertical directions, in 0.1 mm increments.

- 1 Select <Set> on the <Home> screen. ➡ <Home> Screen(P. 150)

2 Select <Adjustment/Maintenance> ► <Adjust Image Quality> ► <Adjust Print Position>.

3 Select the paper source to adjust or <Common> to adjust all paper sources.

NOTE:

Print position adjustment in the vertical direction for 2-sided printing

- The print position for the first page (front side) of two-sided printing can be adjusted with <Common>. The print position for the second page (back side) can be adjusted with the setting for each paper source.

■ Example of print position adjustment

First page (front side)	Setting value for <Common> ► <Adj. Vertically (1st Side for 2-Sided)>
Second page (back side)	Setting value for each paper source ► <Adj. Vertically (1-Sd/2nd Sd for 2-Sd)>

4 Select the direction to adjust and the combination of one-sided/two-sided printing, and press **OK**.

5 Set the adjustment value, and press **OK**.

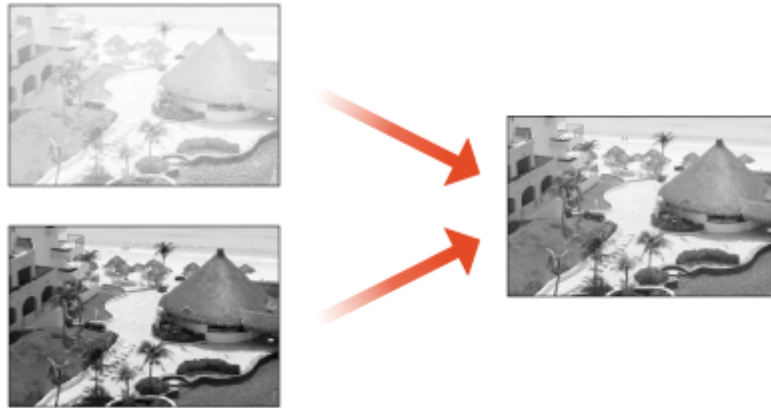
- Enter the value based on the print result of the sample print using ▲/▼.
- For <Adj. Vertically (1st Side for 2-Sided)>, the print position of all paper sources is adjusted with the entered value.
- Repeat steps 3 to 5 to adjust the other positions and paper sources.

6 Output a sample print, and check whether adjustment has been performed correctly. ► **Step 1: Printing the Current Print Position(P. 500)**

Adjusting the Standard Density

E9SJ-0AW

If the density does not improve by performing density adjustment, it may be able to be improved by correcting the standard density.



- 1** Select <Set> on the <Home> screen. ▶<Home> Screen(P. 150)
- 2** Select <Adjustment/Maintenance> ▶ <Adjust Image Quality> ▶ <Adjust Standard Density>.
- 3** Adjust the standard density.
 - The overall density of the printed material, including filled areas, text, lines, and intermediate densities are adjusted. This setting should mainly be used to adjust the maximum density.
- 4** Press **OK**.

Adjusting Density for Specific Paper

E9SJ-0AX

When printing become faint on some paper after the toner cartridge is used for a long time, this setting may improve this problem.

IMPORTANT

- You can use the following paper types.
 - Heavy, Bond, Letterhead 3 to 6, Label, Postcard, Envelope

- 1** Select <Set> on the <Home> screen.  <Home> Screen(P. 150)
- 2** Select <Adjustment/Maintenance> ▶ <Adjust Image Quality> ▶ <Adjust Density for Specific Paper>.
- 3** Adjust the density for specific paper.
 - Set a lower value to reduce the print density and a higher value to increase the print density. Changing this setting also changes the toner consumption.
- 4** Press .

Troubleshooting

Troubleshooting	506
If the Machine Does Not Operate	507
Cannot Print	509
Problems with Printing Results	510
Problems with the Network	521
Problems with Security	525
Other Problems	526
A Message or a Number Starting with "#" (an Error Code) Is Displayed	530
A Message Saying to Contact Your Dealer or Service Representative Is Displayed	531
Countermeasures for Each Message	532
Countermeasures for Each Error Code	550
When a Problem Cannot Be Solved	558

Troubleshooting

E9SJ-09K

If a problem occurs while you are using the machine, check the following items first. If the problem cannot be solved or an inspection is required, contact your dealer or service representative.

■ What kind of problem do you have?



▶ If the Machine Does Not Operate(P. 507)



▶ Cannot Print(P. 509)



▶ Problems with Printing Results(P. 510)



▶ Problems with the Network(P. 521)



▶ A Message or a Number Starting with "#" (an Error Code) Is Displayed(P. 530)



▶ Problems with Security(P. 525)



▶ Other Problems(P. 526)

■ When a paper jam occurs

The procedures for clearing paper jams are described in ▶ Introduction(P. 2) .

If the Machine Does Not Operate

E9SJ-09L

If a problem occurs while you are using the machine, check the following before contacting your dealer or service representative.

- ▶ **Check This First(P. 507)**
- ▶ **If the machine does not respond to computer operations(P. 507)**
- ▶ **When the authentication screen (login screen) is displayed(P. 508)**

Check This First

→ Is a message displayed on the screen?

- A message is displayed on the screen when an error or a problem occurs while operating the machine.
 - ▶ **A Message or a Number Starting with "#" (an Error Code) Is Displayed(P. 530)**

→ Is (Energy Saver) lit?

- If it is lit, press  (Energy Saver) to cancel the Sleep mode.

→ Is the machine connected to a computer correctly?

- Check the network connection of the machine and the computer.
 - ▶ **Setting up the Network Environment(P. 106)**

If the machine does not respond to computer operations

→ Restart the machine.

- If the machine does not respond even though its power is turned ON, turn the power OFF (▶ **Turning OFF the Machine(P. 30)**). Confirm that the power cord is connected correctly, wait 10 or more seconds after the main power is turned OFF, and then turn the power back ON (▶ **Turning ON the Machine(P. 29)**).

→ Check whether the driver is installed correctly.

- For information on installing the driver, see ▶ **Installing Drivers(P. 142)** .

→ Check whether the IP address of the machine is correct.

- Check the IP address settings, and change them if they are incorrect. For information on the settings, see ▶ **Setting up Using the Setup Guide(P. 104)** .

When the authentication screen (login screen) is displayed

→ Log in as a registered user.

- When the authentication screen (login screen) is displayed, you must log in as a registered user to continue operating the machine.
 - ▶ **Logging into the Machine(P. 159)**

Cannot Print

E9SJ-09R

Check This First

→ Is the Processing/Data indicator (on the control panel) flashing or lit?

- If it is flashing or lit, there is a document that is being processed or waiting to be processed. Wait for the processing to finish or select the document that you want to prioritize from the screen for checking the printing status.
 - ▶ **Checking the Printing Status and History(P. 175)**
 - ▶ **Printing Documents that are Forced to be Held in the Machine(P. 180)**

→ Is a message displayed on the screen?

- A message is displayed on the screen when an error or a problem occurs while operating the machine.
 - ▶ **A Message or a Number Starting with "#" (an Error Code) Is Displayed(P. 530)**

→ Is <Auto Select> set to <Off>?

- To switch to the appropriate operation mode, change all items or the items you are using to <Yes>. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual site.

→ Is forced hold printing enabled?

- If it is enabled, documents may not be printed, depending on their settings.
 - ▶ **Configuring the Forced Hold Printing Settings(P. 321)**

→ Are you printing via a print server using the LPR command?

- When continuously printing PDF data using the LPR command, execute one job at a time at the interval set in <Timeout>. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual site.

Problems with Printing Results

E9SJ-09S

- ▶ The printed image is displaced or skewed.(P. 510)
- ▶ Streaks Appear/Printing is Uneven(P. 510)
- ▶ Images are not printed on the intended side of the paper.(P. 511)
- ▶ Images are not printed in the intended size.(P. 511)
- ▶ The orientation does not match on both sides of the paper when using two-sided printing.(P. 512)
- ▶ Smudges Appear on Printouts(P. 513)
- ▶ Toner Smudges and Splatters Appear(P. 514)
- ▶ Afterimages Appear in Blank Areas(P. 514)
- ▶ Printouts are faint or streaks appear(P. 515)
- ▶ White Spots Appear(P. 515)
- ▶ Black Spots Appear(P. 516)
- ▶ Reverse Side of Paper is Smudged(P. 517)
- ▶ Spots like Waterdrops or Streaks Appear(P. 517)
- ▶ The Toner of the Printed Image Peels Off(P. 517)
- ▶ Paper Creases(P. 517)
- ▶ Paper Curls(P. 519)
- ▶ Paper Is Not Fed/Two or More Sheets Are Fed Together(P. 519)

The printed image is displaced or skewed.

→ Are the paper guides misaligned?

- Match the paper guides with the paper loaded in the paper source.

Streaks Appear/Printing is Uneven



→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper.
- ▶ Available Paper(P. 91)
- ▶ Paper Loading Operations(P. 32)

→ Have you cleaned the fixing unit?

- Clean the fixing unit.
- ▶ <Clean Pressure Roller for Fixing>(P. 474)

→ Is the amount remaining in toner cartridge running low?

- Check how much toner is left, and replace the toner cartridge as necessary.

▶ **Replacing the Toner Cartridge(P. 65)**

→ Is it time to replace the toner cartridge?

- Materials inside the toner cartridge may have deteriorated. Replace the toner cartridge.

▶ **Replacing the Toner Cartridge(P. 65)**

→ Are you using the machine in an environment with high humidity?

- Change the settings of [Humid Environment Mode]. Setting to [High Humidity] may improve the problem.

▶ **Paper Type Management Settings(P. 380)**

NOTE:

- Setting to [High Humidity] may cause a printed image or text to be blurred when using in a low humidity environment.

Images are not printed on the intended side of the paper.

→ Is the orientation of the loaded paper correct?

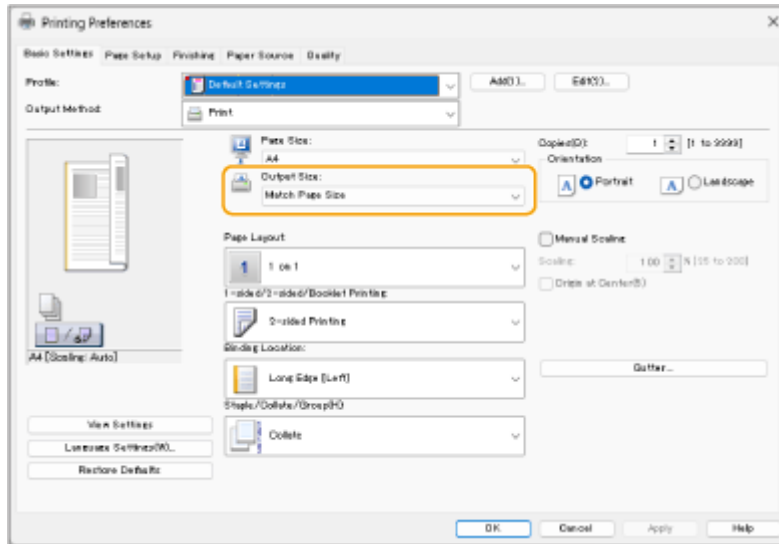
- Check the orientation and side of the paper that is facing up. Load the paper again if it is incorrectly orientated.

▶ **Paper Loading Operations(P. 32)**

Images are not printed in the intended size.

→ Do the original size and size of the paper that is loaded match?

- Replace the paper that is loaded with paper of the size you want to print on.
- Match [Output Size] in the printer driver with the size of paper to print on.

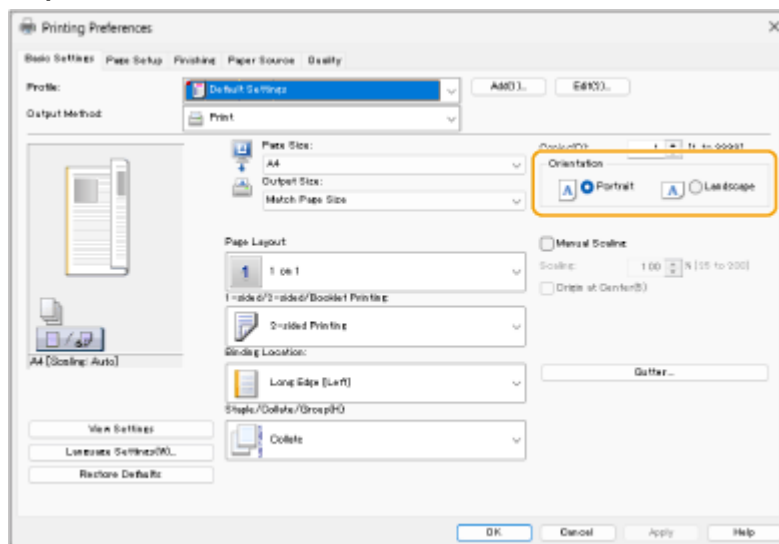


The orientation does not match on both sides of the paper when using two-sided printing.

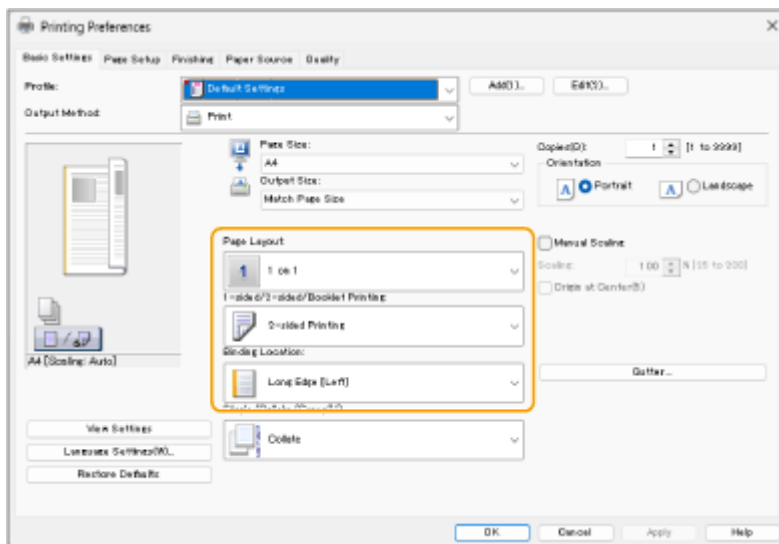
→ Are the settings for two-sided printing correct?

- Follow the procedure below to check the print settings.

- 1 Select the orientation of the original on the print settings screen of the application.
- 2 On the [Basic Settings] screen of the driver, set [Orientation] to the same orientation you set in step 1.



- 3 While checking the print preview, set [Page Layout] ► [Page Order] ► [1-sided/2-sided/Booklet Printing] ► [Binding Location].



NOTE

- [Page Order] is displayed when [Page Layout] is set to [2 on 1] or higher.

Smudges Appear on Printouts



→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper.
- ▶ **Available Paper(P. 91)**
- ▶ **Paper Loading Operations(P. 32)**

→ Do smudges appear on printouts when you use the machine in an environment with low humidity?

- Change the setting for [Humid Environment Mode]. Setting this item to [Low Humidity 1] may solve the problem.
- ▶ **Paper Type Management Settings(P. 380)**

NOTE:

- If you select [Low Humidity 1] and use the machine in an environment with high humidity, the print density may become lighter or uneven.

Toner Smudges and Splatters Appear



→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper.
- ▶ **Available Paper(P. 91)**
- ▶ **Paper Loading Operations(P. 32)**

→ Are you using the machine in a low humidity environment?

- Change the settings of [Humid Environment Mode]. Setting to [Low Humidity 2] may improve the problem.
- ▶ **Paper Type Management Settings(P. 380)**

Afterimages Appear in Blank Areas



→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper.
- ▶ **Available Paper(P. 91)**
- ▶ **Paper Loading Operations(P. 32)**

→ Is the amount remaining in toner cartridge running low?

- Check how much toner is left, and replace the toner cartridge as necessary.
- ▶ **Replacing the Toner Cartridge(P. 65)**

→ Is it time to replace the toner cartridge?

- Materials inside the toner cartridge may have deteriorated. Replace the toner cartridge.
- ▶ **Replacing the Toner Cartridge(P. 65)**

→ Do afterimages appear when you print on large size paper after printing on small size paper?

- Change the setting of <Reduce Ghosting>. Setting to <On> may solve the problem.
- ▶<Adjust Image Quality>(P. 470)

Printouts are faint or streaks appear



→ Is the amount remaining in toner cartridge running low?

- Check how much toner is left, and replace the toner cartridge as necessary.
- ▶Replacing the Toner Cartridge(P. 65)

→ Is it time to replace the toner cartridge?

- Materials inside the toner cartridge may have deteriorated. Replace the toner cartridge.
- ▶Replacing the Toner Cartridge(P. 65)

→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper. Also, specify the paper size and type settings properly.
- ▶Available Paper(P. 91)
- ▶Paper Loading Operations(P. 32)
- ▶Specifying Paper Size and Type(P. 51)

White Spots Appear



→ Are you using paper that has absorbed moisture?

- Replace with appropriate paper.
- ▶Paper Loading Operations(P. 32)

→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper.
- ▶ **Available Paper(P. 91)**
- ▶ **Paper Loading Operations(P. 32)**

→ Is the amount remaining in toner cartridge running low?

- Check how much toner is left, and replace the toner cartridge as necessary.
- ▶ **Replacing the Toner Cartridge(P. 65)**

→ Is it time to replace the toner cartridge?

- Materials inside the toner cartridge may have deteriorated. Replace the toner cartridge.
- ▶ **Replacing the Toner Cartridge(P. 65)**

→ Are you using the machine in a low humidity environment?

- Change the settings of [Humid Environment Mode]. Setting to [Low Humidity 2] may improve the problem.
- ▶ **<Adjust Image Quality>(P. 470)**

→ When performing 2-sided printing, do white spots appear?

- Change the settings of <Waterdrop Pattern Prevention Mode>. Setting to <On> may improve the problem.
- ▶ **<Adjust Image Quality>(P. 470)**

NOTE:

- Setting to <On> decreases the print speed.

Black Spots Appear



→ Have you cleaned the fixing unit?

- Clean the fixing unit.
- ▶ **<Clean Pressure Roller for Fixing>(P. 474)**

Reverse Side of Paper is Smudged



→ Have you loaded paper that is smaller than the size of the print data?

- Check to make sure that the paper size matches the size of the print data.

→ Have you cleaned the fixing unit?

- Clean the fixing unit.
- ▶ **<Clean Pressure Roller for Fixing>(P. 474)**

Spots like Waterdrops or Streaks Appear

→ Does the paper get dirty when printing on both sides?

- Change the settings of <Waterdrop Pattern Prevention Mode>. Setting to <On> may improve the problem.
- ▶ **<Adjust Image Quality>(P. 470)**

NOTE:

- Setting to <On> may decrease the print speed.

The Toner of the Printed Image Peels Off

→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper.
- ▶ **Available Paper(P. 91)**
- ▶ **Paper Loading Operations(P. 32)**

Paper Creases



→ Is paper loaded correctly?

- If paper is not loaded below the load limit line or the load limit guide or is loaded obliquely, it may crease.

▶ **Paper Loading Operations(P. 32)**

→ Are you using paper that has absorbed moisture?

- Replace with appropriate paper.

▶ **Paper Loading Operations(P. 32)**

→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper. Also, specify the paper size and type settings properly.

▶ **Available Paper(P. 91)**

▶ **Specifying Paper Size and Type(P. 51)**

→ Do creases form when you print on thin paper?

- Change the setting of <Reduce Wrinkles (from Humidity)/Streaks>. Selecting <On> may improve the problem.

▶ **<Adjust Image Quality>(P. 470)**

NOTE:

- If you set to <On>, the printing speed will be slower.

→ Do wrinkles appear when printing on thin or plain paper in an environment of high humidity?

- Change the settings of <Paper Wrinkle Correction>. Setting to <On> may improve the problem.

▶ **<Adjust Image Quality>(P. 470)**

NOTE:

- If you set to <On>, the print may be faded or the printing speed may be slower.
- Depending on the environment, paper loaded in a paper drawer may absorb moisture and wrinkles may appear when printing. In that case, reducing the sheets of new paper that will be loaded at the next time may prevent wrinkles.

→ Does this occur when you print on envelopes?

- Change the settings of <Paper Wrinkle Correction>. Setting to <On> may improve the problem.

▶ **<Adjust Image Quality>(P. 470)**

NOTE:

- If you set to <On>, the print may be faded or the printing speed may be slower.

Paper Curls



→ Are you using paper that has absorbed moisture?

- Replace with appropriate paper.
- ▶ **Paper Loading Operations(P. 32)**
- When the current setting of the paper type is <Plain 1>, change it to <Plain 2>.
- ▶ **Specifying Paper Size and Type(P. 51)**

→ Does this problem occur when printing on some types of paper such as plain paper or thin paper?

- Change the setting of <Curl Prevention Mode>. Setting to <On> may solve the problem.
- ▶ **<Adjust Image Quality>(P. 470)**

NOTE:

If you select <On>, the print quality may be reduced.

→ Are you using appropriate paper?

- Check usable paper, and replace with appropriate paper. Also, specify the paper size and type settings properly.
- ▶ **Available Paper(P. 91)**
- ▶ **Paper Loading Operations(P. 32)**
- ▶ **Specifying Paper Size and Type(P. 51)**
- Turn over the paper (front to back) so that the print side is changed, and then reload the paper.

! IMPORTANT:

- Rarely, the symptoms may worsen depending on the type of paper you are using. In that case, get the print side back to original.

Paper Is Not Fed/Two or More Sheets Are Fed Together



→ **Is paper loaded correctly?**

- Fan the paper stack thoroughly so that paper is not stuck together.
- Check whether paper is loaded correctly.
 - ▶ **Available Paper(P. 91)**
 - ▶ **Paper Loading Operations(P. 32)**
- Check whether mixed sizes and types of paper are loaded together.

Problems with the Network

E9SJ-09U

▶ **Problems with Connections(P. 521)**

▶ **Problems with Wireless Connections(P. 522)**

Problems with Connections

→ Cannot set up the network.

- Check whether <Confirm Network Connection> is set to <On>.
▶ **<Confirm Network Connection>(P. 452)**

→ An unintended destination is dialed up.

- If a dial-up router is on the network to which the machine is connected, the machine connects to a destination other than the intended destination, depending on the settings of the machine or dial-up router. This may result in subscriber line charges and call charges. Check the following.
- If the dial-up router does not have to send packets via broadcast, change the router settings to ensure that it sends packets via a method other than broadcast. If it is necessary to allow broadcasting with the dial-up router, check whether an unnecessary destination is set.
- Check whether the host name and IP address of the file server and mail server, etc. set in the machine are correct.
- If the DNS server is on an external server, use the IP address instead of the host name for the destination, even when connecting to devices on the same network as the machine.
- If the DNS server is on the network that the machine is connected to, check whether the information for devices connected to an external network is registered on the DNS server, and whether it is correct.

→ Cannot recognize the machine from a computer.

- If the IP address of the computer where the Remote UI and utility software are executed is not allowed for sending and receiving in <Firewall Settings>, the information for the machine cannot be displayed on the computer. Check whether the settings are correct.
▶ **Specifying IP Addresses in Firewall Settings(P. 289)**
- When using device management software, set [Use Dedicated Community] to [On] and select [Read/Write] for [MIB Access Permission]. Also set [Use Dedicated Port] for [Dedicated Port Settings] to [On].
▶ **Monitoring and Controlling the Machine with SNMP(P. 132)**
- The machine cannot be recognized when utility software is used to access the machine with a community name other than the SNMP community name set in the machine. Check the SNMP community name.
▶ **Monitoring and Controlling the Machine with SNMP(P. 132)**
- If the message "An error has occurred." is displayed in the Web browser and the Remote UI cannot be started, invalid cache data may remain. Clear the cache of the Web browser.
- If the machine enters the Sleep mode, it may not be able to be recognized from a computer. Cancel the Sleep mode or change <Sleep Mode Energy Use> to <High>.
▶ **Energy Consumption in the Sleep Mode(P. 165)**

→ Cannot connect with TLS encrypted communication.

- If you set a TLS version that is not supported by your operating system or software such as the browser, the machine cannot connect to the network using TLS encrypted communication. Upgrade your operating system and software, or lower the TLS version until connections are possible. However, if you lower the TLS version, connections may not be sufficiently secure.
 ▶ **Configuring the Key and Certificate for TLS(P. 303)**

Problems with Wireless Connections

→ Cannot connect wireless LAN and wired LAN at the same time.

- To connect wireless LAN and wired LAN at the same time, set <Select Interface> to the combination of <Wired LAN> and <Wireless LAN>.
 ▶ **<Select Interface>(P. 460)**

→ The Remote UI is not displayed.

- Are <Use HTTP> and <Remote UI Settings> set to <On>?
 ▶ **<Use HTTP>(P. 455)**
 ▶ **Starting the Remote UI(P. 329)**
- If you are connected with wireless LAN, restart the Remote UI after checking whether the IP address is set correctly.
 ▶ **Conducting a Connection Test for an IPv4 Address(P. 121)**
 ▶ **Conducting a Connection Test for an IPv6 Address(P. 123)**
- If you are connected with wired LAN, restart the Remote UI after checking whether the IP address is set correctly and the cable is connected correctly.
 ▶ **Connecting to a Wired LAN(P. 110)**
 ▶ **Starting the Remote UI(P. 329)**
- Are you using a proxy server? If so, add the IP address of the machine in "Exceptions" (addresses to not use a proxy for) in the proxy server settings of the Web browser.
- Is communication with computers restricted in the firewall? If the Remote UI cannot be displayed because the settings are incorrect, set <IPv4 Address Filter>, <IPv6 Address Filter>, or <MAC Address Filter> to <Off> from the control panel of the machine.
 ▶ **Restricting Communication by Using Firewalls(P. 288)**
 ▶ **<Network>(P. 452)** ▶ <IPv4 Address Filter>
 ▶ **<Network>(P. 452)** ▶ <MAC Address Filter>
 ▶ **<Network>(P. 452)** ▶ <IPv6 Address Filter>

→ Cannot connect to the network.

- The IP address may have failed to be set. Set the IP address again.
 ▶ **Setting an IP Address(P. 119)**
- If you are connected with wireless LAN, check whether the machine can connect to the network.
 ▶ **If you cannot connect to a wireless LAN(P. 523)**

→ If you do not know the IP address that was set.

- Press  (Status Monitor) key and check the IP address.

▶ **Control Panel(P. 26)**

- If you want to know the details of the settings or change the settings, select <Set> on the <Home> screen and configure the settings.

▶ **Setting an IP Address(P. 119)**

→ **Cannot change from wired LAN to wireless LAN or wireless LAN to wired LAN.**

- Did you also switch the LAN setting from the control panel of the machine? You cannot change the connection method of the machine unless you do so.

▶ **Selecting the Network Connection Method(P. 108)**

→ **If you do not know the SSID and network key of the wireless LAN router to connect to or the SSID is not displayed on the screen.**

- Check whether the SSID is displayed on the wireless LAN router or its box.

▶ **Checking the SSID and Network Key(P. 118)**

→ **The SSID of the wireless LAN router to connect to is not displayed in the list of access points.**

- Check whether the SSID of the wireless LAN router that you made a note of is correct.
- If the SSID of the wireless LAN router is not disclosed (if it is using the stealth function*), set the wireless LAN router to disclose the SSID.

* This function prevents the SSID of a wireless LAN router from being automatically detected.

- Check whether the machine is connected to the network.

▶ **If you cannot connect to a wireless LAN(P. 523)**

If you cannot connect to a wireless LAN



Check the status of the computer.

- Is setup of the computer and wireless LAN router complete?
- Are any of cables of the wireless LAN router (power cable, LAN cable, etc.) disconnected?
- Is the wireless LAN router turned ON?

If the problem is still not resolved:

- Turn all the devices off, and then on again.
- After waiting a while, check whether you can connect to the network.



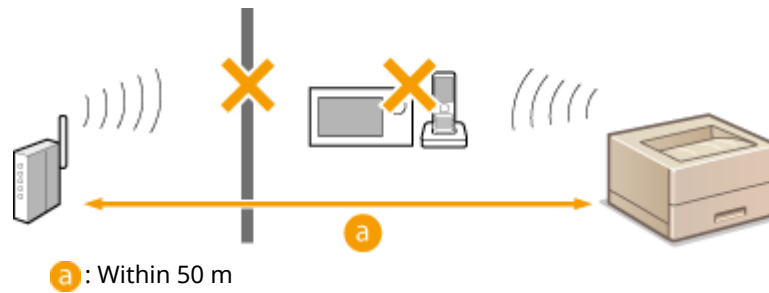
Check whether the machine is turned ON.

If the machine is turned ON, turn it OFF, and then ON again.



Check the installation location of the machine and wireless LAN router.

- Are the machine and wireless LAN router too far away from each other?
- Is there an obstacle such as a wall between the machine and wireless LAN router?
- Are there any devices that emit electromagnetic waves nearby, such as a microwave or digital cordless telephone?



Specify the following settings again.

- ▶ Setting Up the Connection Using WPS Push Button Mode(P. 114)
- ▶ Setting Up the Connection Using WPS PIN Code Mode(P. 115)
- ▶ Setting Up Connection by Selecting a Wireless Router(P. 116)
- ▶ Setting Up a Connection by Specifying Detailed Settings(P. 117)

NOTE

If settings require manual entry

- If the wireless LAN router is set as follows, perform manual entry (▶ Setting Up a Connection by Specifying Detailed Settings(P. 117)):
 - ANY rejection* is enabled.
 - The stealth function is enabled.
- * A wireless LAN router function for refusing connections if the device trying to connect has "ANY" or "blank" set for the SSID.

If it is necessary to change the settings on the wireless LAN router side

- If the wireless LAN router is set as follows, change the settings on the router side:
 - MAC address filtering is set.
 - When communicating with IEEE 802.11n only, the encryption method for WPA/WPA2 is set to TKIP.

Problems with Security

▶ The settings in <Set> are not restored even though the check box is deselected in the security policy settings. (P. 525)

▶ Cannot import security policy settings.(P. 525)

▶ A security administrator password entry screen is displayed even though no password is set.(P. 525)

The settings in <Set> are not restored even though the check box is deselected in the security policy settings.

- Items changed with security policy settings applied are not restored simply by deselecting the check box. Deselect the check box, and change the corresponding settings from [Settings/Registration] in the Remote UI.
▶ **Security Policy Setting Items(P. 236)**

Cannot import security policy settings.

- Have you set a different security policy password from the source device? Remove the password in the destination device or set the same password as the source device.
▶ **Using a Password to Protect the Security Policy Settings(P. 232)**

A security administrator password entry screen is displayed even though no password is set.

- If you import security policy settings, the same password is set for the destination device if a security policy password is set in the source device. Check the password of the source device.

Other Problems

- ▶ Cannot press a button, select an item, or an item is not displayed.(P. 526)
- ▶ Some settings imported from another device are not reflected.(P. 526)
- ▶ Log files are garbled.(P. 526)
- ▶ Log events are not recorded even though log collection was started.(P. 526)
- ▶ The setting for K-size paper is not displayed.(P. 526)
- ▶ Viewing the Network Connection Information of the Computer(P. 527)

Cannot press a button, select an item, or an item is not displayed.

- Some settings can only be used by the administrator. They cannot be used by general users.
 - ▶ **Settings/Registration(P. 386)**
- The system administrator limits the functions that general users can use to prevent unauthorized use, and restricts the use of functions.
- The functions that can be used with User Authentication are managed by the administrator. These functions can be used by logging in using an ID with access privileges.
 - ▶ **Logging into the Machine(P. 159)**
- Functions cannot be used because the optional equipment or system options that they require are not installed.
- The settings are managed with security policy settings. To change the settings, it is necessary to log in to the Remote UI with administrator privileges.
 - ▶ **Configuring the Security Policy Settings(P. 234)**

Some settings imported from another device are not reflected.

- If a security policy is set, settings that violate the security policy cannot be imported.

Log files are garbled.

- When opening CSV files with Microsoft Excel, the content may not be recognized as text strings and may become garbled as a result. If this happens, open the files with a CSV file editor or text editor.

Log events are not recorded even though log collection was started.

- Results may not be reflected in a log file if it is retrieved immediately after log collection is started. Since it takes some time to collect logs, retrieve the log file again after waiting a while.

The setting for K-size paper is not displayed.

- You can use K-size paper by changing the machine settings. For more information, contact your dealer or service representative.

Viewing the Network Connection Information of the Computer

▶ When Using Windows(P. 527)

▶ When Using macOS(P. 528)

■ When Using Windows

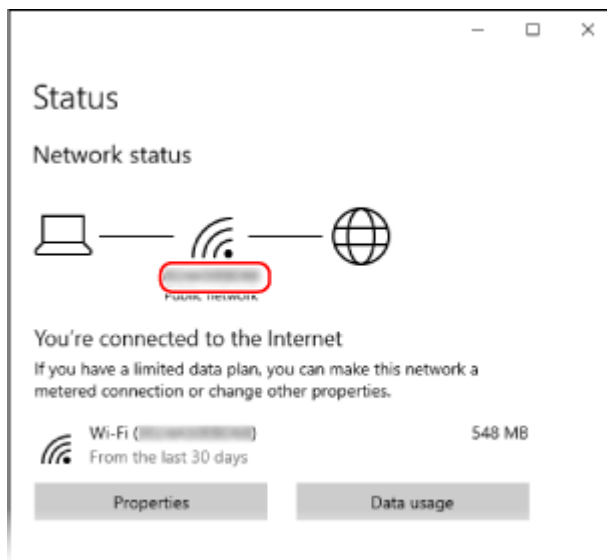
1 Right-click [] (Start), and click [Network Connections].

⇒ The [Status] screen is displayed.

2 View the network connection information.

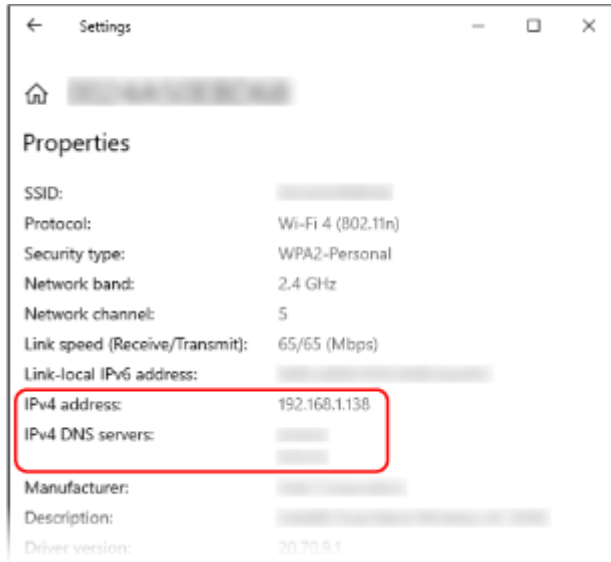
■ Viewing the SSID of the Wireless LAN

View the SSID in [Network status].



■ Viewing the IP Address and DNS Server

- 1 Click [Properties] for the connected network.
- 2 In [Properties], view the IP address and DNS server.



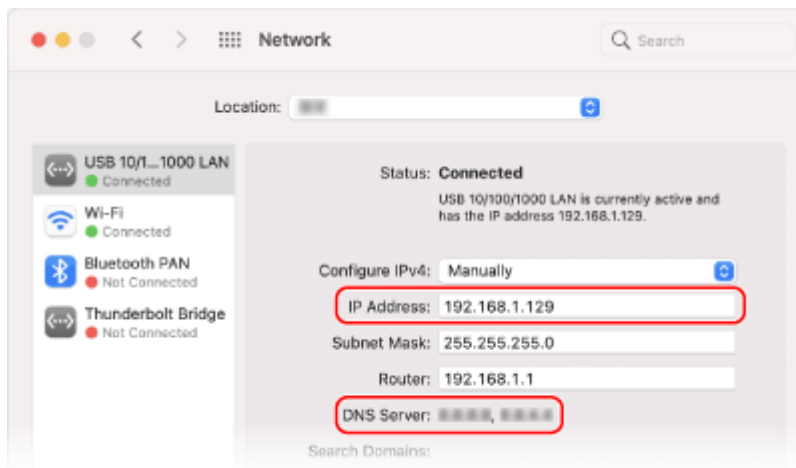
■ When Using macOS

1 Click [] ► [System Preferences] ► [Network].

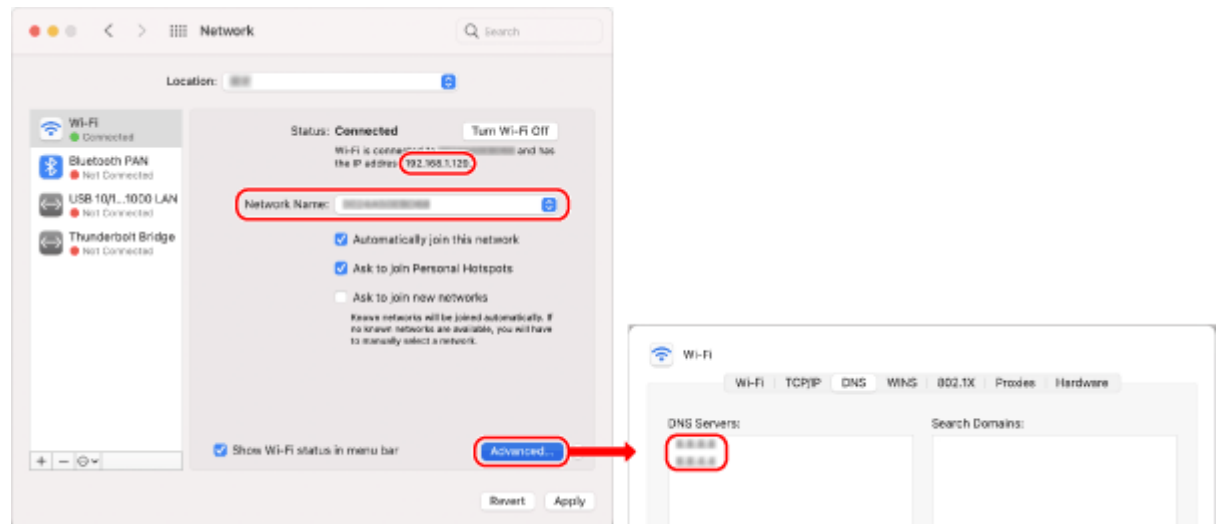
⇒ The [Network] screen is displayed.

2 View the IP address, DNS server, and other information.

■ For Wired LAN



■ For Wireless LAN



- View the SSID in [Network Name].
- View the IP address in [Status].
- Click [Advanced], and view the DNS server on the [DNS] tab.

A Message or a Number Starting with "#" (an Error Code) Is Displayed

E9SJ-09Y

If a message is displayed on the screen of the machine or the Remote UI, or a number starting with "#" (an error code) is displayed on the details screen for job log or a communication management report, refer to the following to check the remedy.

- ▶ **A Message Saying to Contact Your Dealer or Service Representative Is Displayed(P. 531)**
- ▶ **Countermeasures for Each Message(P. 532)**
- ▶ **Countermeasures for Each Error Code(P. 550)**

A Message Saying to Contact Your Dealer or Service Representative Is Displayed

E9SJ-0A0

If the machine cannot operate normally due to a problem, a message is displayed on the touch panel display. Check the reference according to the displayed message.

▶ **When a message saying to contact a your dealer or service representative is displayed(P. 531)**

When a message saying to contact a your dealer or service representative is displayed

1 Restart the machine.

- Press the power switch to turn the power OFF (▶ **Turning OFF the Machine(P. 30)**), wait for longer than 10 seconds, and then turn the power ON again (▶ **Turning ON the Machine(P. 29)**).

IMPORTANT:

- Note that data waiting to be processed is erased when you turn the power OFF.

2 If the message is still displayed, prepare the following information.

- Product name
- The dealer or service representative where you purchased the machine
- The problem (the specific operation you performed and the result and symptom, etc.)
- Code displayed on the screen

3 Turn the power of the machine OFF, pull out the power plug, and contact your dealer or service representative.

WARNING

- Do not connect or disconnect the power cord with wet hands, as this may result in electrical shock.

CAUTION

- Always grasp the power plug when disconnecting the power cord. Pulling on the power cord may expose or snap the core wire, or otherwise damage the power cord. If the power cord is damaged, this could cause current to leak, resulting in a fire or electrical shock.

Countermeasures for Each Message

E9SJ-0A1

If an error occurs during printing, or if a problem occurs with the network connection or settings, a message appears on the machine display or the Remote UI screen. For details about each message and solutions to the problems, refer to the messages below.

23 MEMORY FULL

There is insufficient memory to register overlay forms and external characters, etc.

- Cancel printing (**▶Canceling Printing(P. 173)**), initialize the printer to increase the free memory, and then try printing again. However, note that initializing the printer will erase all the print data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.
- Select <Skip Error>, and continue printing. However, the data that could not be registered due to a lack of memory will not be printed.

27 JOB REJECT

The specified emulation does not exist.

- Specify emulation that the machine supports. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.
- Select <Skip Error> to skip the printing that an error occurred for. You can perform the following printing.

33 WORK FULL

Could not print because the dedicated work memory was insufficient.

- Cancel printing (**▶Canceling Printing(P. 173)**), initialize the printer to increase the free memory, and then try printing again. However, note that initializing the printer will erase all the data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.
- Select <Skip Error>, and continue printing. However, the data for which an error was displayed will not be printed correctly. Also note that registered data such as overlay forms and macros may be deleted.

52 IMAGEMODE REJECT

Data that cannot be processed was sent while printing an image.

- Select <Skip Error> to skip the printing that an error occurred for. However, the data for which an error was displayed will not be printed.
- Perform printing again using a printer driver that supports the data format of the image.

An unsupported wired LAN adapter has been connected.

The USB-LAN adapter is not connected, or the USB-LAN adapter which is not available for the machine is connected.

- Check the Connection of the USB-LAN Adapter.
▶Connecting to a Wired LAN(P. 110)
- For details about the USB-LAN adapter which is available for the machine, contact your dealer or service representative.

Could not verify the CRL.

Could not confirm the CA certificate of the certificate authority that issued the certificate revocation list (CRL).

- Register the CA certificate of the certificate authority that issued the certificate revocation list (CRL).
➤Registering a CA Certificate(P. 338)

D1 Replot Buffer Full

Could not redraw because data could not be registered to the replot buffer.

- Select <Skip Error>, and continue printing. However, the data that caused the error will not be printed correctly. For information on the replot buffer, see Setting the Machine (PS/PCL/UFR II Printer).

D1 Div. Print. Bffr Full

Could not perform divided printing because data could not be registered to the buffer for divided printing.

- Cancel printing (**➤Canceling Printing(P. 173)**), set <Divide Mode> to <Off> and <Enlarge/Reduce> to <Auto> in the HP-GL setup menu, specify the output paper size, and perform printing again. However, the data will be enlarged/reduced when printed. For more details, see Setting the Machine (PS/PCL/UFR II Printer).
- Select <Skip Error>, and continue printing. However, the data that could not be registered will not be printed correctly. For information on divided printing, see Setting the Machine (PS/PCL/UFR II Printer).

D1 Polygon Buffer Full

Could not draw because data could not be registered to the polygon buffer.

- Select <Skip Error>, and continue printing. However, the data that caused the error will not be printed correctly. For information on the replot buffer, see Setting the Machine (PS/PCL/UFR II Printer).

D0-nn error (nn is two alphanumeric characters)

The printer stopped operating normally due to an unknown problem.

- Restart the machine. Press the power switch to turn the power OFF (**➤Turning OFF the Machine(P. 30)**), wait for longer than 10 seconds, and then turn the power ON again (**➤Turning ON the Machine(P. 29)**). If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FF FONT FULL

Could not register font information in the font table because there were too many fonts to register.

- Cancel printing (**➤Canceling Printing(P. 173)**), initialize the printer to increase the free memory, and then try printing again. However, note that initializing the printer will erase all the data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.
- Select <Skip Error>, and continue printing. However, the data that could not be registered will not be printed correctly.

FM DL SIZE ERROR n (n is a single alphanumeric character)

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM DL SCALE ERROR n (n is a single alphanumeric character)

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM DL FONT MEMORY FULL

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM FILE ACCESS ERROR

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM SC WORK MEM. ERROR n (n is a single alphanumeric character)

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM ALIGNMENT ERROR

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM FONT PARSE ERROR

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM FONT MEMORY FULL

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

FM WORK MEMORY ERROR

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

IEEE 802.1X error. Set correct auth. info.

The client authentication information is not set correctly.

- Check whether the authentication method and authentication information (key and certificate, user name and password, and CA certificate) are set correctly.

IEEE 802.1X error. No reply from the destination.

An error occurred while communicating with the authenticator.

- Check whether the authenticator (LAN switch) and RADIUS server are set correctly.

IEEE 802.1X error. Cannot analyze cert.

Failed to analyze the server certificate sent from the RADIUS server.

- Check the content of the server certificate of the RADIUS server.

IEEE 802.1X error. Cert. is incorrect.

An error occurred when using the server certificate sent from the RADIUS server as a CA certificate for validation.

- Check the content of the server certificate of the RADIUS server and the CA certificate registered in the machine.
 **Registering a CA Certificate(P. 338)**

IEEE 802.1X error. Auth srvr cert expired

The server certificate sent from the RADIUS server has expired.

- Check the expiration date of the server certificate of the RADIUS server.

IEEE 802.1X error. Change the authentication password.

The password has expired.

- Set a new password.

IEEE 802.1X error. Check the authentication settings.

The authentication method set in the machine and the authentication method set in the RADIUS server do not match.

- Check the authentication method set in the machine and the RADIUS server, and set the correct authentication method.

Cannot delete the default key because it is in use by TLS or other settings. Check the settings.

The key and certificate you are trying to delete is being used in TLS encrypted communications.

- Set all TLS settings to <Off> to stop TLS encrypted communication.

TCP/IP Error

Could not automatically retrieve the address with DHCP and Auto IP.

- If the address cannot be automatically retrieved with DHCP and Auto IP, <IP Address> in <IPv4 Settings> is set to 0.0.0.0. Set the correct IPv4 address. In addition, if <Sub Line> is set to a setting other than <Off> in <Select Interface>, correctly configure the IPv4 address of the sub line.

➤ **Setting an IPv4 Address(P. 120)**

➤ **<IP Address Settings>(P. 452)** (<Sub Line Settings>)

0.0.0.0 is set as a fixed IPv4 address in <IP Address> in <IPv4 Settings>.

- Set the correct IPv4 address.
- **Setting an IPv4 Address(P. 120)**
- **<IP Address Settings>(P. 452)** (<Sub Line Settings>)

The IPv6 address is not set correctly.

- Check the following. It may take several minutes until the stateless address is decided.
- Check whether <Use IPv6> is set to <On> in <IPv6 Settings>.
- When using a stateless address or DHCPv6, check whether each address has been retrieved.
- If the address has not been retrieved, check the settings of the router and the DHCPv6 server.

➤ **Setting an IPv6 Address(P. 122)**

The address of the DNS server is not set correctly.

- Check whether the address of the DNS server is set correctly in <IPv4> or <IPv6>.
- **Making DNS Settings(P. 128)**

Could not send to the TCP/IP protocol stack.

- Check whether the IPv4 address or IPv6 address is set correctly in <IPv4 Settings> or <IPv6 Settings>. In addition, if <Sub Line> is set to a setting other than <Off> in <Select Interface>, correctly configure the IPv4 address of the sub line.

➤ **Setting an IPv4 Address(P. 120)**

➤ **Setting an IPv6 Address(P. 122)**

Check the TCP/IP.

The TCP/IP of the machine is not operating.

- Check the IP address, DHCP, and Auto IP settings in <TCP/IP Settings>.
- **Setting an IPv4 Address(P. 120)**
- If <Sub Line> is set to a setting other than <Off> in <Select Interface>, check the settings for the IP address and DHCP in <Sub Line Settings>.
- **<IP Address Settings>(P. 452)** (<Sub Line Settings>)

Check the TCP/IP settings. (Main Line)

The IP address of the main line is set to "0.0.0.0".

- Set a different IP address.

▶Setting an IPv4 Address(P. 120)

Check the TCP/IP settings. (Sub Line)

The IP address of the sub line is set to "0.0.0.0".

- Set a different IP address.
- ▶Setting the IPv4 Address of the Sub Line(P. 124)

Universal Print: Srvr. communication error

The machine is not connected to the network correctly.

- Check the machine and network settings, and try connecting again.

Could not communicate because a server error occurred.

- Check whether the server is operating normally.

Communication with the server is blocked due to firewall settings.

- Configure the firewall settings to allow communication.

Universal Print: Srvr. authentication error

An error has occurred during server authentication.

- Restart the machine. If the message still appears after restarting the machine, make a note of the message and contact your dealer or service representative.

Universal Print: Certificate expired.

The expiration date of the certificate has expired.

- Delete this machine from Microsoft Entra ID and the computer, re-register the machine, and then update the certificate.

Universal Print: Internal error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message still appears after restarting the machine, make a note of the message and contact your dealer or service representative.

Universal Print: Printer not registered

This machine was deleted from Microsoft Entra ID and could not be communicated with.

- Re-register this machine in Microsoft Entra ID.

Chk. wired LAN adapter connected to USB port.

Multiple USB-LAN adapters are connected, or the USB-LAN adapter is not connected/recognized.

- Check the connection of the USB-LAN adapter.
- ▶Connecting to a Wired LAN for the Sub Line(P. 110)
- If you reconnected the USB-LAN adapter, restart the machine.
- ▶Front Side(P. 19)

XPS Print Range Error

There are no pages that can be processed in the specified range for printing.

- Specify a correct page range.

XPS Image Data Error

Failed to extend the image data.

- Replace the image data in the XPS file and try printing again.

XPS Spool Memory Full

There is insufficient memory to process the XPS data.

- Restart the machine and try printing again. If you still cannot print, divide the pages into multiple files and print them separately.

XPS Data Error

An invalid command is specified due to corrupt data, etc. and processing cannot continue.

- Perform printing again using XPS data in a format supported by the machine.

XPS Unsupport Image Error

An unsupported data format is included.

- Convert the data to the TIFF or JPEG format and try printing again.

XPS Font Error

Failed to analyze the font data.

- Replace the font data in the XPS file and try printing again.

XPS Page Data Error

Cannot generate pages because the descriptions are incorrect.

- Perform printing again using XPS data in a format supported by the machine.

XPS Memory Full

There is insufficient memory to process the XPS data.

- Select <Skip Error>, and continue printing. However, pages that include the data that caused the error may not be printed correctly.

Cannot find the access point.

The access point could not be found.

- Check the wireless LAN settings.
 ▶ **Check the settings and information of the wireless LAN(P. 112)**

Could not delete authentication information because an error occurred.

The authentication information could not be deleted because an unknown error occurred.

- Contact your dealer or service representative.

Could not set authentication information because an error occurred.

The authentication information could not be set because an unspecified error occurred.

- Contact your dealer or service representative.

An error occurred. Contact the system manager.

The selected user has already been deleted.

- Log in as the Administrator and register the button again.

An unexpected system error occurred.

- Check the operations and log in again. If you still cannot log in, consult your system administrator.

Reconsider your usage environment for recmnd. security settings.

The usage environment was checked in the Recommended Security Settings for Usage Environment, or the recommendation result changed due to a change in the connection environment.

- It Is Recommended That You Check the Recommended Usage Environment and Change to That Security Setting, As Needed.

* If you do not intend to change the security settings and you want to prevent this message from appearing, disable the notification for when the recommended usage environment is updated.

▶<Recommended Security Set. for Usage Env.>(P. 493)

Check the remaining toner in the toner cartridge. Printing is possible if there is still toner left in the toner cartridge.

A toner cartridge needs to be replaced soon. Make sure that you have a replacement toner cartridge ready.

- Replace the toner cartridge if you see this message before you start to print a large job. This message is displayed when <Action When Remaining Toner Is Low> is set to <Display Warning Screen>.

▶<Action When Remaining Toner Is Low>(P. 477)

An error occurred during verification.

The certificate is invalid.

- Register the correct certificate and specify the settings again.
 - ▶Configuring the Key and Certificate for TLS(P. 303)
 - ▶Registering a Key and Certificate for Network Communication(P. 337)

This CRL is invalid.

The certificate revocation list (CRL) may be corrupt, or a signing algorithm not supported by the machine may be used.

- Register the correct certificate revocation list (CRL).
 - ▶Registering a Certificate Revocation List (CRL)(P. 340)

This CRL has expired.

The start date for the certificate revocation list (CRL) may be set to a date in the future.

- Check the start date of the certificate registered in the machine. If the start date is set to a date in the future, use the certificate on a day after that date.
 ▶ **Registering a Certificate Revocation List (CRL)(P. 340)**

The date and time set on the machine may be incorrect.

- Check the date and time setting of the machine.
 ▶ **Setting the Date/Time(P. 105)**

Cannot register because the algorithm of this key is not supported.

You tried to register the key and certificate file of an unsupported encryption algorithm.

- Register the key and certificate file of a supported encryption algorithm.
 ▶ **Registering a Key and Certificate(P. 337)**
 ▶ **System Specifications(P. 598)**

Cannot set this key as the default key because it is corrupted or invalid.

The key specified for the machine cannot be set because it is corrupted.

- Register the key again.
 ▶ **Registering a Key and Certificate for Network Communication(P. 337)**
 ▶ **Registering a Key and Certificate(P. 337)**

This certificate has been revoked.

The certificate is included in the certificate revocation list (CRL).

- Register a new certificate.
 ▶ **Registering a Key and Certificate for Network Communication(P. 337)**

This certificate is invalid.

The certificate is invalid.

- Register the correct certificate and specify the settings again.
 ▶ **Configuring the Key and Certificate for TLS(P. 303)**
 ▶ **Registering a Key and Certificate for Network Communication(P. 337)**

This certificate has expired.

The certificate may have expired.

- Check the expiration date of the certificate registered in the machine. If the certificate has expired, register a valid certificate.
 ▶ **Registering a Key and Certificate for Network Communication(P. 337)**

The date and time set on the machine may be incorrect.

- Check the date and time setting of the machine.
 ▶ **Setting the Date/Time(P. 105)**

The appropriate paper size, A4, is not available.

Paper of the optimal size selected with Automatic Paper Selection has not been loaded.

- Load paper of the displayed size.

<Paper Source Auto Selection> is set to <Off>.

- Specify the paper drawer manually.
 - Set a paper source loaded with the optimal paper size to <On> in <Paper Source Auto Selection>.
- **<Paper Source Auto Selection>(P. 476)**

Paper of a type that cannot be selected with Automatic Paper Selection is loaded.

- Specify the paper drawer manually.

Subnet Mask Conflict

The network addresses of the main line and sub line conflict.

- Check the IP address and subnet mask settings of the main line and sub line.
- **Setting an IP Address(P. 119)**

The default key is not set.

The key and certificate (TLS server certificate) are not registered.

- To use TLS encrypted communication, first register the key to be used.
- **Configuring the Key and Certificate for TLS(P. 303)**

An unusable wired LAN adapter was connected.

A USB-LAN adapter that cannot be used with the machine is connected.

- For information on the USB-LAN adapters that can be used, contact your dealer or service representative.
- **Connecting to a Wired LAN for the Sub Line(P. 110)**

Could not verify the certificate.

The CA certificate of a certificate authority could not be confirmed.

- Register a CA certificate issued by a certificate authority.

Cannot change the settings because the selected key is being used.

The key and certificate you are trying to delete is being used in TLS encrypted communications.

- Set all TLS settings to <Off> to stop TLS encrypted communication.

Session timed out. Wait a moment, then try to access the database again.

The session timed out because the specified length of time elapsed.

- Try accessing again after waiting a while. If the session continues to time out, restart the machine.

Direct Connection ended due to an error.

Failed to connect to the mobile device, or no data was sent or received between the machine and the connected mobile device for a certain period of time.

- Check the connection between the machine and the mobile device.

Cannot print because a non-Canon or counterfeit toner cartridge may be in use.

A toner cartridge for which the print quality cannot be guaranteed may be installed.

- It is recommended to replace the toner cartridge.

IMPORTANT:

- Printing cannot continue while this message is displayed.
 **<Canon Genuine Mode>(P. 488)**

Could not register because the number of registered users has reached the limit.

Cannot register the user because the number of users has exceeded the upper limit.

- Delete any unnecessary users.

The entered PIN is incorrect.

An incorrect PIN was entered.

- Enter the PIN again.
- If you do not know the correct PIN, contact the administrator.

The authentication server is not running. Contact the system manager.

The LAN cable is disconnected.

- Connect the LAN cable.

The Active Directory server is not running.

- Start the Active Directory server.

The KDC service of Active Directory is stopped.

- Follow the procedure below to check the status of the service.
 1. Start the "Service" management tool of Active Directory.
 2. Check whether the Active Directory server is operating normally.

Communication with the Active Directory * server is blocked by the firewall.

- Stop blocking the default port 88.

* If Active Directory is set as the login destination, communication is normally performed with the UDP protocol using port 88, but the data may be processed with the TCP protocol if it exceeds a certain size.

Cannot find the authentication server. Contact the system manager.

The LAN cable is disconnected.

- Connect the LAN cable.

The primary/secondary DNS server settings of the machine are incorrect or not set.

- Check and adjust the DNS server settings of the machine.

The DNS server specified in the machine is not running or its service is stopped.

- Follow the procedure below to check the status and settings of the DNS server.
 1. Check whether the DNS server specified in the machine is running.
 2. Start the "Service" management tool of the DNS server.
 3. Check the status in [DNS Server], and if [Enable] is not displayed, right-click and select [Enable].

Check whether the host record exists in the DNS server.

- Check whether a host record exists in the DNS server, and whether the forwarder settings are correct.

Anonymous access to auth. server is not allowed. Contact the system manager.

Anonymous access is not allowed on the LDAP server.

- On the information input screen of the LDAP server, select [Use Authentication Information of Each User], and then specify the user name and password according to what is registered in the LDAP server.
 - ▶ **Registering Server Information(P. 262)**

Account info needed to log in to auth. server is invalid. Contact sys manager.

The user name or password is not set correctly.

- Confirm the authentication user ID and password, and whether the user has administrator privileges.

The attributes specified in the server settings are not set correctly.

- Confirm that the attributes are correct. Also, make sure that the fields (attribute names) do not contain invalid values.
 - ▶ **Registering Server Information(P. 262)**

The administrator account information specified in the server settings is not set correctly. Alternatively, the user could not log in as an administrator.

- Specify the correct administrator account information.

The information for the server settings is insufficient.

- Confirm that the attributes necessary for logging in are set correctly.
 - ▶ **Registering Server Information(P. 262)**

IP address conflict detected.

The IPv4 address set for the machine already exists in the same network as the machine.

- Change the IP address of the machine in <IP Address> in <IPv4 Settings> so that it does not conflict with the IP address of another device.
 - ▶ **Setting an IPv4 Address(P. 120)**

An IP address conflict was detected on the network. (Main Line)

The IPv4 address set for the main line of the machine already exists on the same network as the machine.

- Change the IP address of the main line of the machine so that it does not conflict with the IP address of another device.
 - ▶ **Setting an IPv4 Address(P. 120)**

An IP address conflict was detected on the network. (Sub Line)

The IPv4 address set for the sub line of the machine already exists on the same network as the machine.

- Change the IP address of the sub line of the machine so that it does not conflict with the IP address of another device.
 **Setting the IPv4 Address of the Sub Line(P. 124)**

Check the network connection.

The cable is not connected to the machine correctly.

- Check whether the LAN cable is connected correctly. If you had to connect it again, restart the machine.
 **Connecting to a Wired LAN(P. 110)**

The machine is not connected to the network.

- If you want to use the machine without connecting to a network, set <Confirm Network Connection> to <Off>.
 **<Confirm Network Connection>(P. 452)**

Check the network connection.(Main Line)

The machine and the LAN cable of the main line are not connected correctly.

- Check whether the LAN cable is connected correctly. If you had to connect it again, restart the machine.
 **Connecting to a Wired LAN(P. 110)**

The machine is not connected to the network.

- If you want to use the machine without connecting to a network, set <Confirm Network Connection> to <Off>.
 **<Confirm Network Connection>(P. 452)**

Check the network connection. (Sub Line)

The machine and the LAN cable of the sub line are not connected correctly.

- Check whether the LAN cable is connected correctly. If you had to connect it again, restart the machine.
 **Front Side(P. 19)**

The machine is not connected to the network.

- If you want to use the machine without connecting to a network, set <Confirm Network Connection> to <Off>.
 **<Confirm Network Connection>(P. 452)**

Cannot log in because an authentication error occurred in Department ID Management. Contact the system manager.

When using User Authentication, Department ID Management is enabled but Department IDs have not been assigned to users.

- If you are a general user, ask your administrator to assign you a Department ID.
- If you are an administrator user, ask the Department ID Management administrator to assign you a Department ID. If no administrator users can log in, contact your dealer or service representative.

PDL Invalid DLG Input

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL DLG Rendering Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL DLG Unknown Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL DLG Memory Full

The work memory was insufficient when the system was processing data (in particular, graphic processing and text processing).

- Select <Skip Error>, and continue printing. However, pages that include the data that caused the error may not be printed correctly.

PDL DLG Mem. Alloc. Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL GL Orig. Pt Unknown

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL GL Coord.Result

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL Invalid GL Input

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL GL Range Check

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL GL Memory Full

The work memory was insufficient when the system was processing data (in particular, graphic processing and text processing).

- Select <Skip Error>, and continue printing. However, pages that include the data that caused the error may not be printed correctly.

PDL GL Mem. Alloc. Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL IMG Refer. Data Error

The TIFF or JPEG data includes data that cannot be processed with the machine.

- Cancel printing (**▶Canceling Printing(P. 173)**), initialize the printer to increase the free memory, and then try printing again. However, note that initializing the printer will erase all the data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.

PDL IMG Initial. Error

The memory for printing the TIFF or JPEG data was insufficient.

- Cancel printing (**▶Canceling Printing(P. 173)**), initialize the printer to increase the free memory, and then try printing again. However, note that initializing the printer will erase all the data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.

PDL IMG Process. Error

An unknown problem occurred while processing the TIFF or JPEG data.

- Cancel printing (**▶Canceling Printing(P. 173)**), initialize the printer, and try printing again. However, note that initializing the printer will erase all the data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.

PDL IMG Invalid Data

The TIFF or JPEG data includes data that cannot be processed with the machine.

- Cancel printing (**▶Canceling Printing(P. 173)**), and check the TIFF or JPEG data.
- Select <Skip Error>, and continue printing. However, the data that caused the error will not be printed.

Data that cannot be processed by the machine because the machine has the same IP address as another device, etc. was sent.

- Cancel printing (**Canceling Printing(P. 173)**), check the IP address in <TCP/IP Settings>, and change the IP address if necessary.
Setting an IP Address(P. 119)

PDL IMG Work Memory Full

The memory for processing the TIFF or JPEG data was insufficient.

- Cancel printing (**Canceling Printing(P. 173)**), initialize the printer to increase the free memory, and then try printing again. However, note that initializing the printer will erase all the data in the memory of the machine. For more details, see Setting the Machine (PS/PCL/UFR II Printer) via the online manual Web site.
- Select <Skip Error>, and continue printing. However, the data that caused the error will not be printed.

PDL nn Rendering Error (nn is the module name)

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL PDF Error

PDF data that cannot be processed with the machine was sent.

- Cancel printing (**Canceling Printing(P. 173)**), optimize the PDF using Adobe Acrobat, and try printing again.
- Cancel printing (**Canceling Printing(P. 173)**), open the PDF file in an application, and try printing again using the printer driver.
- If the above-mentioned remedies do not solve the problem, make a note of the message and contact your dealer or service representative.

PDL PDF Data Decode Error

The password for printing the PDF file is incorrect.

- Enter the correct password, and try printing again.

Printing is not allowed in the security settings of the PDF file.

- Change the PDF file to allow printing in an application for editing PDF files.

If the PDF file is linked with a policy server, the policy server cannot be accessed.

- Check whether the policy server is turned on.
- Check whether the machine, policy server, and network are operating normally.

PDL PDF Memory Full

There is insufficient memory to process the PDF data.

- Cancel printing (**Canceling Printing(P. 173)**), optimize the PDF by adjusting settings such as the image resolution using Adobe Acrobat (to reduce the size of the data to print at one time), and perform printing again.
- Cancel printing (**Canceling Printing(P. 173)**), divide the pages of the PDF data in Adobe Acrobat into multiple files, and try printing again.

- Cancel printing ( **Canceling Printing(P. 173)**), open the PDF file in an application, and try printing again using the printer driver.

PDL RIP Process. Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL XPS Error

An undefined error occurred.

- Restart the machine and try again. If the message is still displayed, make a note of the message and contact your dealer or service representative.

PDL XPS Initialize Error

An unknown error such as not being able to retrieve memory during initialization occurred.

- Restart the machine and try again. If the message is still displayed, make a note of the message and contact your dealer or service representative.

PDL XPS Rendering Error

An error occurred in the rendering system.

- Restart the machine and try again. If the message is still displayed, make a note of the message and contact your dealer or service representative.

PDL Image Comp. Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL Rendering Timeout

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL Data Transfer Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

PDL Reg. Access Error

The printer stopped operating normally due to an unknown problem.

- Restart the machine. If the message is still displayed after restarting the machine, make a note of the message and contact your dealer or service representative.

The password does not meet the policy requirements. Change the password.

The entered password violates the password policy.

- Enter a password that complies with the password policy. If you do not know the password policy, consult your system administrator.

A toner cartridge that cannot be used with this device has been inserted, so printing is currently unavailable.

A toner cartridge that can be used with the machine has not been loaded.

- Load the toner cartridge that can be used with the machine. For instructions on checking the model number of the toner cartridge, see **Replacement Parts(P. 70)** .

! IMPORTANT:

- Printing cannot continue while this message is displayed.

Timer settings for this device and the authentication server may not be synchronized. Contact the system manager.

The date and time settings of the machine and the authentication server are different.

- Synchronize the date and time settings of the machine and the authentication server.

No Paper

The paper in the paper source has run out.

- Load paper in the paper source displayed on the screen.
Paper Loading Operations(P. 32)

The paper guides in the paper source are in the wrong position.

- Adjust the paper guides according to the edges of the paper. Depending on the cut edge of the paper, multiple sheets of paper may be fed together when printing, which can cause paper jams. This can be reduced by changing the orientation of the loaded paper.

The paper settings differ from the paper that is loaded.

- Press  (Status Monitor) ► select <Device Status> ► <Paper Information> to check the paper setting. If the paper settings are incorrect, match them with the paper that is loaded. The paper loaded in the paper drawers and multi-purpose tray can be set in <Paper Settings> on the <Home> screen.
Specifying Paper Size and Type(P. 51)

The paper settings of the driver or application differ from the paper that is loaded.

- Check the paper settings on the [Printing Preferences] screen of the printer driver, and if the paper settings are incorrect, match them with the paper that is loaded.

Countermeasures for Each Error Code

E9SJ-0A2

When printing is not completed normally, a number starting with "#" (an error code) is displayed on the details screen for job log or a communication management report ( **Printing Reports and Lists(P. 379)**). Perform the countermeasure required for the error code.

NOTE

- Some error codes may not be displayed, depending on your machine.

#001 to #800

-  #009(P. 550)  #010(P. 550)  #037(P. 551)  #099(P. 551)  #701(P. 551)
 #749(P. 551)  #752(P. 551)  #753(P. 551)  #755(P. 552)  #772(P. 552)

#801 to #999

-  #801(P. 552)  #802(P. 552)  #810(P. 552)  #813(P. 553)  #816(P. 553)
 #818(P. 553)  #819(P. 553)  #820(P. 553)  #821(P. 553)  #822(P. 553)
 #825(P. 554)  #827(P. 554)  #828(P. 554)  #829(P. 554)  #831(P. 554)
 #837(P. 554)  #843(P. 554)  #844(P. 555)  #851(P. 555)  #852(P. 555)
 #853(P. 555)  #856(P. 555)  #857(P. 555)  #858(P. 555)  #860(P. 555)
 #861(P. 556)  #862(P. 556)  #863(P. 556)  #865(P. 556)  #866(P. 556)
 #919(P. 556)  #923(P. 556)  #934(P. 557)  #939(P. 557)  #995(P. 557)

■ #009

Paper has run out.

- Load paper.
 **Paper Loading Operations(P. 32)**

The paper drawer is not inserted correctly.

- Insert the paper drawer in all the way.
 **Basic Paper Loading Method(P. 33)**

■ #010

Paper has run out.

- Load paper.
 **Paper Loading Operations(P. 32)**

■ #037

Data containing more than 1,000 pages was received.

- The machine deletes any pages after the 999th page, and prints the remaining 999 pages. Tell the other party to send the 1,000th and subsequent pages again.

■ #099

The operation was canceled before it was complete.

- Perform the operation again.

■ #701

The Department ID does not exist, or the PIN was changed.

- If you are using User Authentication, assign Department IDs to users. If you are using Department ID Authentication, enter the new Department ID and PIN to log in again.

The reception setting in [Printer Jobs with Unknown IDs] is set to [Reject].

- Set [Printer Jobs with Unknown IDs] in [Department ID Management] to [Allow].
 **Setting the Department ID Management(P. 276)**

■ #749

The operation could not be performed because a service call message is displayed.

- Turn the main power OFF, and turn the main power ON again. If the operation still cannot be performed correctly, turn the main power switch OFF, remove the power plug from the outlet, and contact your dealer or service representative.
 **Turning OFF the Machine(P. 30)**
 **Turning ON the Machine(P. 29)**

■ #752

The server is not running or the network is disconnected.

- Check whether the SMTP server is operating normally.
- Check the status of the network.

The SMTP server name setting for e-mail is incorrect or the e-mail address or domain name is not set.

- Check the SMTP server name, e-mail address, and domain name settings in <Communication Settings>.
 **Configuring E-Mail Print Settings(P. 143)**

■ #753

A TCP/IP error (Socket or Select error, etc.) occurred when receiving an e-mail.

- Check the status of the network cable and connector. If there is still a problem, restart the machine.
 **Turning ON the Machine(P. 29)**

■ #755

The IP address is not set.

- Check <TCP/IP Settings> in <Preferences>.
 - ▶ <Network>(P. 452) ▶ <TCP/IP Settings>
- If <Sub Line> is set to a setting other than <Off>, also check <Sub Line Settings> in <Preferences>. When the machine was turned ON, an IP address was not assigned to the machine by DHCP or Auto IP.
 - ▶ <Network>(P. 452) ▶ <Sub Line Settings>

When the machine was turned ON, an IP address was not assigned to the machine by DHCP or Auto IP.

- Check <TCP/IP Settings> in <Preferences>.
 - ▶ <Network>(P. 452) ▶ <TCP/IP Settings>
- If <Sub Line> is set to a setting other than <Off>, also check <Sub Line Settings> in <Preferences>.
 - ▶ <Network>(P. 452) ▶ <Sub Line Settings>

■ #772

The network is disconnected.

- Check the status of the network.

■ #801

A timeout error occurred due to a problem on the mail server side when communicating with the SMTP server to receive an e-mail.

- Check whether the SMTP server is operating normally.
- Check the status of the network.

An error was returned from the SMTP server when connecting with SMTP. The address setting is incorrect. An error occurred due to a problem on the server side when sending to a file server.

- Check whether SMTP is operating normally, the status of the network, the destination settings, and the status and settings of the file server.

■ #802

The SMTP server name specified in <Communication Settings> is incorrect.

- Check the SMTP server name set in <Communication Settings>.
 - ▶ <Configuring E-Mail Print Settings>(P. 143)

The DNS server address specified in <DNS Settings> is incorrect.

- Check the DNS server address specified in the DNS settings.
 - ▶ <Making DNS Settings>(P. 128)

Connection to the DNS server failed.

- Check that the DNS server is functioning normally.

■ #810

A POP server connection error occurred when an e-mail was received.

- Check the POP server settings in <Communication Settings>.

► **Configuring E-Mail Print Settings(P. 143)**

- Check whether the POP server is operating correctly. Check the status of the network.

An error was returned from the POP server when connecting to the POP server. Alternatively, a timeout error occurred on the server side.

- Check the POP server settings in <Communication Settings>.

► **Configuring E-Mail Print Settings(P. 143)**

- Check whether the POP server is operating correctly. Check the status of the network.

■ #813

A POP server authentication error (user account error or password error) occurred when an e-mail was received.

- Check the POP server settings in <Communication Settings>.

► **Configuring E-Mail Print Settings(P. 143)**

■ #816

Printing could not be performed because the maximum number of prints set in Department ID Management was exceeded.

- Contact your System Manager.

■ #818

The received data was in a file format that cannot be printed.

- Tell the other party to change the file format and send again.

■ #819

Data that cannot be handled was received. The MIME information is invalid.

- Tell the other party to check the settings and send again.

■ #820

Data that cannot be handled was received. The BASE64 or uuencode is invalid.

- Tell the other party to check the settings and send again.

■ #821

Data that cannot be handled was received. A TIFF analysis error occurred.

- Tell the other party to check the settings and send again.

■ #822

Data that cannot be handled was received. The image cannot be decoded.

- Tell the other party to check the settings and send again.

■ #825

The Department ID and PIN of a job being executed or a reserved job were deleted, or the PIN was changed.

- Execute the job again using the changed Department ID and PIN.

■ #827

Data that cannot be handled was received. Unsupported MIME information was included.

- Tell the other party to check the settings and send again.

■ #828

HTML data was received.

- Tell the other party to change to a format other than HTML and send again.

■ #829

Data containing more than 1,000 pages was received.

- The machine deletes any pages after the 999th page, and prints the remaining 999 pages. Tell the other party to send the 1,000th and subsequent pages again.

■ #831

An e-mail document could not be received using SMTP because of the Receive Filter setting in Firewall Settings.

- Reset the Receive Filter setting in Firewall Settings.
 **Specifying IP Addresses in Firewall Settings(P. 289)**

■ #837

A connection request was received from a host whose connection is restricted by the Receive Filter settings in Firewall Settings.

- Check the Receive Filter settings in Firewall Settings. This may also represent a hacking attempt via unauthorized access.
 **Specifying IP Addresses in Firewall Settings(P. 289)**

■ #843

There is a great difference between the time of the KDC (Key Distribution Center) server and the time set in the machine.

- Adjust the current date and time in <Date/Time Settings>.
 **Setting the Date/Time(P. 105)**
- Adjust the current time set in the KDC (Key Distribution Center) server.

■ #844

Sending could not be performed because a validation error occurred when validating the TLS server certificate when communicating with the POP server because <Confirm TLS Certificate for POP RX> is set to <On>.

- Use the Remote UI to check whether the CA certificate used to sign the TLS server certificate on the POP server side is registered in the machine.
- Check whether the TLS server certificate on the POP server side is correct.
- Check whether the TLS server certificate is a self-signed certificate.

■ #851

The printer job could not be stored because the memory is full.

- Check the amount of available memory, and execute the job again.

■ #852

The power was turned OFF while the job was being executed.

- Check that the power cable and plug are securely connected, and execute the job again.

■ #853

The memory is full.

- Reduce the number of pages or check that the number of jobs waiting to be processed has decreased, and execute the job again.

■ #856

The executed operation was canceled because the storage area used for temporarily saving data is full.

- Contact your administrator.

■ #857

Printing was canceled due to the job being canceled while being received, or due to timeout.

- If timeout has occurred, check the status of the network.

■ #858

The data is invalid.

- Check that the print protocol is supported by the machine, as well as the print settings.

■ #860

Recovery failed after a paper jam, or an incompatible page description language or settings which cannot be combined were included.

- Check the paper or job settings.

■ #861

An error occurred while processing the print data or image data.

- Check the image size and paper size, as well as the color specification settings.

■ #862

Settings are included which are not supported, cannot be combined, or otherwise exceed the limits of the machine.

- Check the job settings.

■ #863

The job was canceled because initialization operations were performed while the print data was being processed.

- Execute the job again.

■ #865

The required functions for printing are currently restricted.

- Check the machine and the job settings.

■ #866

The job was canceled by the security related settings.

- If you are executing a job from the printer driver, use the user information of the appropriate privileges.
- If you are executing a job from the control panel, login as a user with the appropriate privileges.

NOTE

The security related settings are as follows.

- [Remote job without user authentication] is selected.

■ #919

A syntax error or a PostScript error that exceeds device restrictions, etc. was detected.

- Set <Print PS Errors> (Set) to <On>, submit the job again, confirm the contents of the PostScript error, then execute the job after resolving the error. For more details, see "Setting the Machine (PS/PCL/UFR II Printer)" via the online manual site.

■ #923

Could not print on the specified side of the cover, or body.

- Change to a paper type that is compatible with two-sided printing, and execute the job again.

■ #934

An error occurred for a print job, and the job was deleted because the specified time period elapsed.

- Resolve the error and execute the job again.
- You can also change the time period before deletion or disable automatic deletion from <Auto Delete Suspended Jobs> (Set).
 <Auto Delete Suspended Jobs>(P. 477)

■ #939

Printing was canceled due to an error that occurred while processing the image data.

- Execute the job again.

■ #995

Reserved communication jobs were cleared.

- Perform the operation again, as necessary.

When a Problem Cannot Be Solved

E9SJ-0A3

If you cannot solve a problem by referring to the information in this chapter, contact your dealer or service representative or the Canon help line.

IMPORTANT

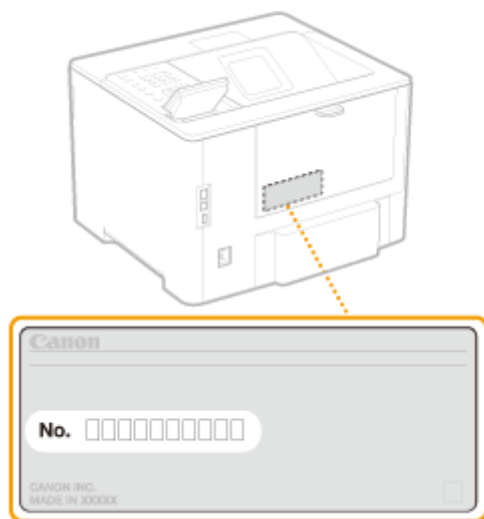
Do not disassemble or repair the machine yourself

- If you disassemble or repair the machine yourself, it may not be covered by warranty.

■ When Contacting Canon

When contacting us, have the following information ready:

- Product name (imageCLASS LBP335x)
- Dealer where you purchased the machine
- Details about your problem (such as what you did, what happened as a result, and displayed messages)
- Serial number (found on the label on the back side of the machine)



NOTE

Checking the serial number from the control panel

- You can also check by  (Status Monitor) ► <Device Status> ► <Serial Number>.

Implementing Security Measures

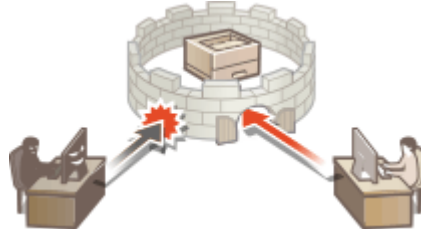
Implementing Security Measures	560
Various Security Functions	561

Implementing Security Measures

E9SJ-0A4

Saving important data to the machine and sharing information via the machine enable the machine to be used more effectively. It also raises the value the machine provides as an information asset.

The machine provides various functions for enhancing security, such as preventing information leaks, preventing unauthorized access, and protecting confidential information. Using these security functions together enables you to use the machine securely.



► **Various Security Functions(P. 561)**

Various Security Functions

E9SJ-0A5

Do you feel uneasy about the following problems?

- Unattended output
- Unauthorized access
- Forgetting to erase confidential data on the machine

The machine provides various security functions for minimize the risk of information leakage and unauthorized access. This section describes functions that are effective in certain situations.

- ▶ **Preventing Documents Leaks(P. 561)**
- ▶ **Preventing Unauthorized Access to the Network(P. 562)**
- ▶ **Preventing Leaks of Confidential Information during Operation of the Machine(P. 562)**

! IMPORTANT

- Implementing security measures does not guarantee that all information will be protected.

NOTE

- Using the Import All function enables multiple devices to be managed with the same settings. ▶ **Importing/Exporting the Setting Data(P. 357)**

Preventing Documents Leaks



When managing confidential documents, it is necessary to handle problems such as leaks and loss. The machine has a security function that prohibits printing until the user logs in at the device, in order to prevent the leakage or loss of documents.

Use the following functions as security measures for preventing document leaks.

Force Hold

To avoid leaving printed material, accidental information leakage, misprinting, etc., the administrator can set to store the document before printing. ▶ **Printing Documents that are Forced to be Held in the Machine(P. 180)**

Only Allow Encrypted Print Jobs

By using Encrypted Secure Printing, you can send encrypted printing data to a machine from your computer. This enables you to reduce the risk of information leaks when sending printed data, and to print more safely. ▶ **Only Allow Encrypted Print Jobs(P. 323)**

Preventing Unauthorized Access to the Network



Although Cloud services have made it easier to exchange data via the Internet, communication can still be intercepted or modified by malicious third parties due to network vulnerabilities. The machine provides various measures for increasing network security, such as only allowing communication with specific IP addresses and encrypting data for communication.

Use the following functions as security measures for preventing unauthorized network access, etc.

Firewall Settings

Unauthorized access by third parties, as well as network attacks and breaches, can be blocked by only allowing communication with devices that have a specific IP address. ➤ **Restricting Communication by Using Firewalls(P. 288)**

Proxy Settings

You can provide greater security by using a proxy server for connections outside the network. ➤ **Setting a Proxy(P. 301)**

TLS Settings

TLS is a protocol for encryption for data sent over a network and is often used for communication via a Web browser or an e-mail application. TLS encrypted communication enables secure network communication when accessing the machine using the Remote UI. ➤ **Configuring the Key and Certificate for TLS(P. 303)**

IPSec Settings

While TLS only encrypts data used on a specific application, such as a Web browser or an e-mail application, IPSec encrypts the whole (or payloads of) IP packets. This enables IPSec to offer a more versatile security system than TLS. ➤ **Configuring the IPSec Settings(P. 310)**

IEEE 802.1X Settings

If a device tries to connect and start communicating on an 802.1X network, the device must go through user authentication in order to prove that the connection is made by an authorized user. Authentication information is sent to and checked by a RADIUS server, which permits or rejects communication to the network depending on the authentication result. If authentication fails, a LAN switch (or an access point) blocks access from the outside of the network. The machine can connect to an 802.1X network as a client device. ➤ **Configuring the IEEE 802.1X Authentication Settings(P. 317)**

Preventing Leaks of Confidential Information during Operation of the Machine



The machine generates value as an information asset by storing important data. Preventing confidential information from remaining on the machine after disposal is another important security measure. The machine provides various measures for increasing security of operation, such as preventing unregistered users from operating the machine, and completely erasing temporary job data when the machine is started.

Use the following functions as security measures for preventing leaks of confidential information during operation of the machine.

Verify System at Startup

The integrity of the firmware, system, and MEAP applications in the machine are verified during startup. [▶<Verify System at Startup>\(P. 493\)](#)

Trellix Embedded Control

When the machine is operating, the Trellix Embedded Control function is used to prevent unauthorized program modification and the execution of unauthorized programs, for improved system reliability. [▶<Trellix Embedded Control>\(P. 493\)](#)

Personal Authentication Management

A user name and password can be used to perform personal authentication of users. Preventing unauthorized access by third parties and setting usage restrictions can maintain a higher level of security and enable more efficient operation of the machine. [▶Managing Users\(P. 241\)](#)

Encrypting the Data in the Storage

You can automatically encrypt the data in the storage to prevent information leaks caused by the removal of the storage. [▶Managing Storage Device Data\(P. 375\)](#)

Initialize All Data/Settings

You can restore all of the machine settings to the factory default values. Since data remaining in the memory is overwritten with meaningless values, this prevents external leaks of confidential data when disposing of the machine. [▶Initializing Settings\(P. 376\)](#)

Security Policy Settings

A security policy describes company-wide rules regarding information security. With this machine, multiple settings related to a security policy can be set together. [▶Applying a Security Policy to the Machine\(P. 231\)](#)

Allow Use of Default Password for Remote Access

You can set the machine to not allow users to log in to the Remote UI using the default password (7654321) of the "Administrator" user for security reasons. [▶Setting an Authentication/Password Policy\(P. 283\)](#)

Appendix

Appendix	565
Feature Highlights	566
Productivity	567
Image Quality	568
Manageability	569
Building a Dual Network Environment	570
Reliability	573
Office Compatibility	574
MEAP	575
Installing MEAP Applications	577
Managing MEAP Applications	580
Managing MEAP Application Licenses	585
Changing Login Services	588
Basic Windows Operations	592
System Specifications	598
Printer Functions	599
Management Functions	602
System Environment	607
Network Environment	608
System Options	610

Appendix

E9SJ-0A6

This chapter provides useful information and items that customers should be aware of, such as the machine's system specifications and functions for more effective use of the machine. Read this chapter as necessary.

■ System Specifications

See this section when you want to check the specifications of the print function or the network environment, and so on.



▶ **System Specifications(P. 598)**

■ Enhancing Functions of the Machine

Refer to this section when you use the MEAP application, the dedicated application for enhancing functions.



▶ **MEAP(P. 575)**

■ Additional Information

Read this chapter to learn useful information on using the machine.



▶ **Feature Highlights(P. 566)**

▶ **Basic Windows Operations(P. 592)**

Feature Highlights

E9SJ-0A7

This section highlights five ways in which you can use the machine to its fullest potential.

Superior productivity to help your business' daily operations run more smoothly

▶ **Productivity(P. 567)**

Clearer images thanks to high-quality image printing and corrective functions

▶ **Image Quality(P. 568)**

Expanded capabilities and easier management

▶ **Manageability(P. 569)**

Convenience and peace of mind

▶ **Reliability(P. 573)**

An energy-saving design that's environmentally friendly

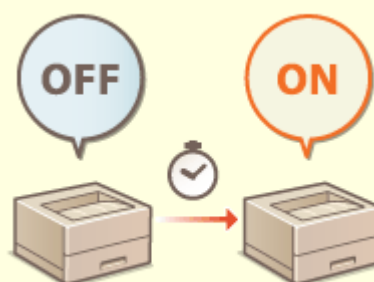
▶ **Office Compatibility(P. 574)**

Productivity

E9SJ-0A8



This section describes how to use the machine's superior productivity to help your daily business operations run more smoothly.



Using the Machine Immediately after Turning it ON (Quick Startup)

Specifying <Quick Startup Settings for Main Power> reduces the time required for the machine to start up after turning the main power ON, enabling smoother operations.

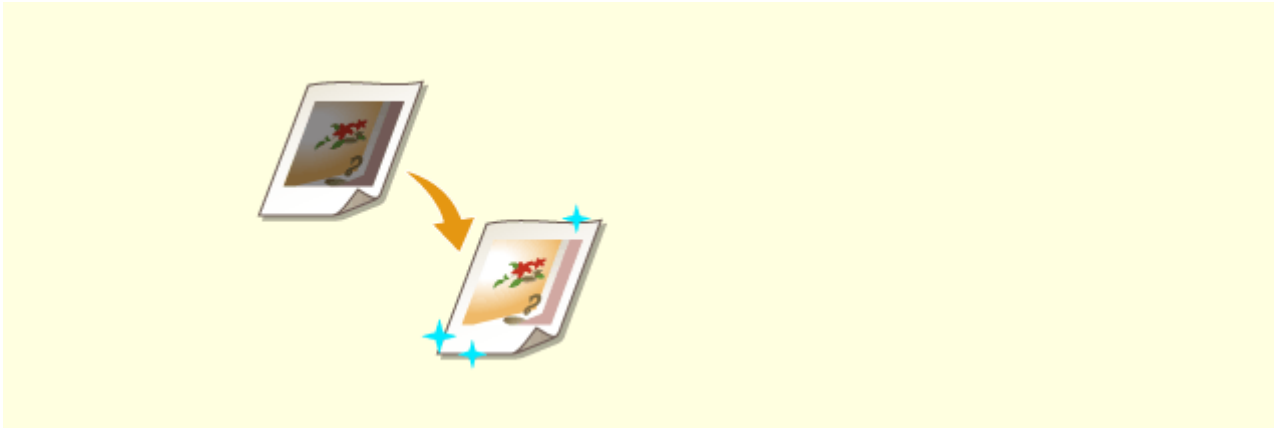
▶<Quick Startup Settings for Main Power>(P. 448)

Image Quality

E9SJ-0A9



This section describes functions that help to produce crisp and clear images, such as high-quality image printing and corrective functions.



Adjusting the Quality of Printing and Finishing

You can achieve more satisfying print results by using corrective functions.

▶ **Adjusting Print Quality(P. 499)**

Manageability

E9SJ-0AA



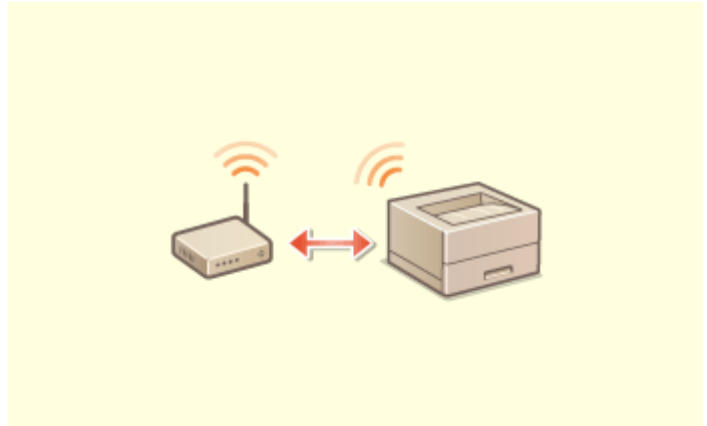
This section describes how to expand the capabilities of the machine and make management easier.



Dual Network Environment

A dual network environment using wired LAN and wireless LAN or wired LAN and another wired LAN can be used.

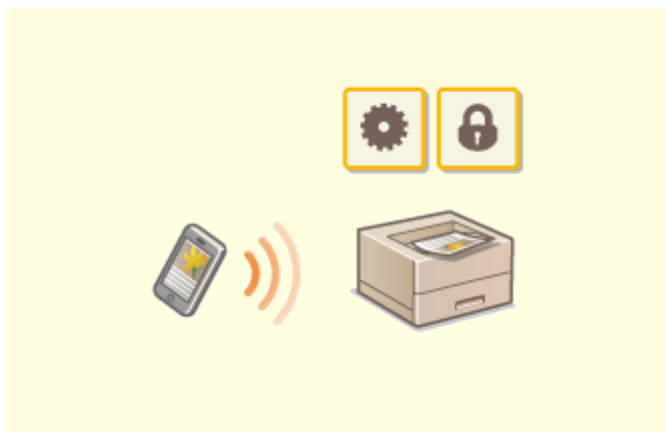
► **Building a Dual Network Environment(P. 570)**



Connecting to the Wireless LAN

A wireless LAN is built into the machine, enabling you to connect a computer or mobile device to the machine, as well as install it in a separate location.

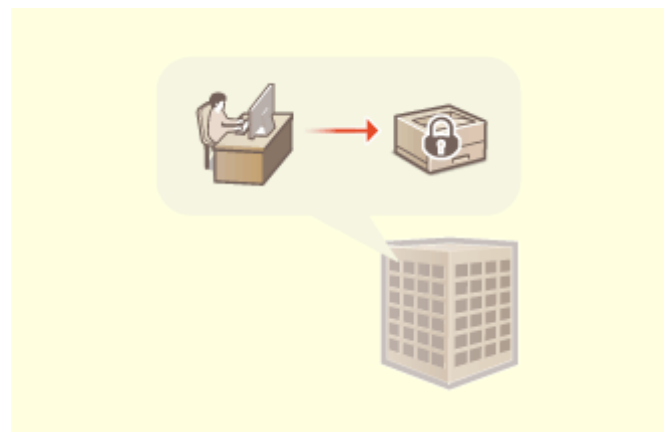
► **Connecting to a Wireless LAN(P. 112)**



Linking with Mobile Devices

You can directly print data saved in a mobile device from the machine. You can also use your mobile device to specify settings for forced hold printing in the machine.

► **Linking with Mobile Devices(P. 208)**



Operating an Office Security Policy

A security policy describes company-wide rules regarding information security. With this machine, multiple settings related to a security policy can be set together.

► **Applying a Security Policy to the Machine(P. 231)**

Building a Dual Network Environment

E9SJ-0AC

Do you have separate machines in each department or floor of the same office for security purposes?

In addition to single connections with a wired LAN or wireless LAN, this machine enables dual network environments with both a wired LAN and wireless LAN or a wired LAN and another wired LAN via a USB-LAN adapter*. This makes it easy to build network environments where employees use the main line and customers use a sub line with restricted functionality. It also contributes to reduced costs as it is not necessary to install a machine for each network environment.

* For information on the supported USB-LAN adapters, contact your dealer or service representative.



On the machine and in the User's Guide (this manual), the primary line used in a dual network is called the "main line," and the secondary line is called the "sub line."

▶ **Flow of Settings Required for a Dual Network(P. 570)**

▶ **Cautions When Using the Sub Line(P. 571)**

Flow of Settings Required for a Dual Network

In a dual network, the main line and sub line have separate settings. This section describes the settings required for the sub line network.

NOTE

- Specify the wired LAN/wireless LAN settings common to the main and sub lines, as required.
 - ▶ **Connecting to a Wired LAN(P. 110)**
 - ▶ **Connecting to a Wireless LAN(P. 112)**

Step 1

▶ **Selecting the Network Connection Method(P. 108)**

- Select the network connection method.



Step 2

▶ **Setting the IPv4 Address of the Sub Line(P. 124)**

- Specify the IPv4 address settings from <IP Address Settings> in <Sub Line Settings>. When using static routing, also set a gateway address.

**Step 3****▶ Making Ethernet Settings(P. 126) ***

- Set this when using a wired LAN via a USB-LAN adapter for the sub line.
* Specify the required settings according to your environment.

**Step 4****▶ Configuring the Firewall in IP Addresses of the Sub Line(P. 295) ***

- Register the port numbers of the functions to use/restrict in the firewall settings of the sub line.
* Specify the required settings according to your environment.

**Step 5****▶ Setting Static Routing(P. 136) ***

- Set static routing when connecting to another network via a router.
* Specify the required settings according to your environment.

**Step 6****▶ Configuring System Data Communication(P. 140) ***

- Set this when performing specific system data communication, such as accessing a firmware distribution server in environments where DNS name resolution or network connections via a proxy cannot be used.
* Specify the required settings according to your environment.



Cautions When Using the Sub Line

The network functions set in the machine can all be used for the main line. However, the functions that can be used with the sub line are limited.



- The DNS server and WINS server settings cannot be used at the same time as the main line.
- <DNS Server Address Settings> and <Proxy Settings> in <Settings for System Data Communication> can only be used for specific system data communication, such as using the sub line to access a firmware distribution server. When using a DNS server or proxy server for the sub line for applications other than system data communication, register the addresses and port numbers to use with the sub line in the settings of the main line.

▶ **Making DNS Settings(P. 128)**

▶ **Setting a Proxy(P. 301)**

■ Functions Restricted for the Sub Line

The following network functions cannot be used with the sub line.

- IPv6 address settings
- IEEE802.1X authentication
- IPSec
- NetBIOS
- FTP (ACTIVE mode)
- DHCP Option Settings
- DNS Dynamic Update Settings
- Multicast Discovery Settings
- Setting the IP address via AutoIP
- Browsing using the SMB protocol

The following functions and services cannot be used, due to the above limitations.

- Building a printing/accounting system that connects to a server via a MEAP application
- Building an authentication system for an Active Directory server
- File sending using DNS name resolution or NetBIOS name resolution from the SMB or WebDAV protocol*1
- Automatic discovery of other printers/multifunction machines on the sub line side using multicast discovery*1
- Functions such as the following that use the IP address of the main line
 - [Security Policy Settings]
 - Batch importing/batch exporting
- Universal Print

*1 Specify the IP address directly.

Reliability

E9SJ-0AE



This section describes how to use the machine with greater convenience and peace of mind.



Preventing Information Leaks from the Storage

You can automatically encrypt the data in the storage to prevent information leaks caused by the removal of the storage.

▶ **Managing Storage Device Data(P. 375)**

Office Compatibility

E9SJ-0AF



This section describes how to use the machine in an environmentally-friendly manner.



Using the Sleep Mode to Save Power During Standby

The machine saves power by switching to the Sleep mode when not in use. Users can also save power by only starting up the functions they require when the machine recovers from the Sleep mode.

▶ **Entering Sleep Mode(P. 164)**

▶ **<Timer/Energy Settings>(P. 448)**

MEAP

E9SJ-0AY

MEAP (Multifunctional Embedded Application Platform) is a framework for enhancing and optimizing various functions installed on the machine such as "Authentication" and "Output." For instance, user management using IC cards and collaboration with software which streamlines file processing becomes possible through MEAP. To enhance functions as stated before, you are required to install a dedicated application called a "MEAP application" on the machine. You can install MEAP applications and check their usage status by displaying the SMS (Service Management Service) from the Remote UI. In order to install a MEAP application, you are required to log in as an administrator ([▶Logging into the Machine\(P. 159\)](#)).



NOTE

- SMS will always use encrypted TLS communications, regardless of the setting of <Use TLS> in <MEAP Settings>. Therefore, if the default key for SSL is not set in advance, you cannot log in to SMS. [▶Configuring the Key and Certificate for TLS\(P. 303\)](#)
- Multiple users cannot log in to SMS at the same time.

■ Installing MEAP Applications

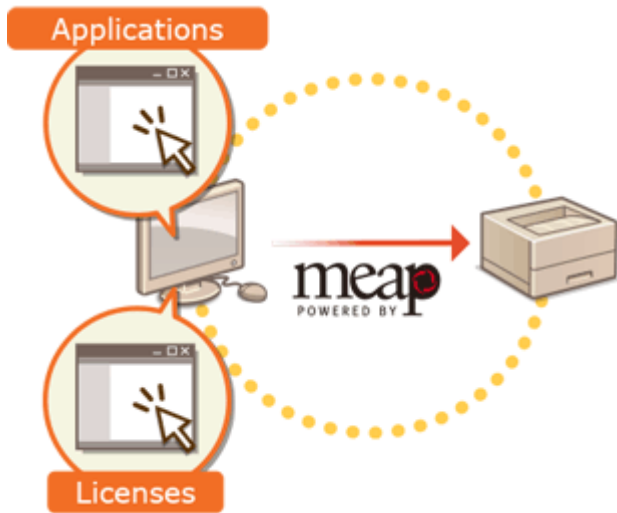
You can install MEAP applications and configure the necessary settings to use the MEAP applications.



[▶Installing MEAP Applications\(P. 577\)](#)

■ Managing MEAP Applications

This section describes how to check the MEAP applications you installed, how to uninstall the applications, and how to manage the licenses.



- ▶ Managing MEAP Applications(P. 580)
- ▶ Managing MEAP Application Licenses(P. 585)

Installing MEAP Applications

E9SJ-0C0

Before installing a MEAP application, you must acquire the "license file" using a computer. After acquiring the license file, display the SMS from the Remote UI to install the MEAP application.



▶ **Acquiring the License File(P. 577)**

▶ **Installing the Application(P. 578)**

NOTE

- You can check the number of applications installed and the storage device space being used. ▶ **Managing MEAP Applications(P. 580)**
- If your MEAP application does not come with a License Access Number, your license file will be provided by your MEAP Application provider. The license key and license file described in this section are not required. For more information, see the manual provided with each MEAP application.
- Depending on the MEAP application, it may require a specific condition for installation. For more information, see the user's manual for the MEAP application to be used.
- The maximum number of MEAP applications that can be installed on this machine is 20.

Acquiring the License File

! IMPORTANT

The following information is required for acquiring a license file.

- The license access number attached to the package of the MEAP application
- Serial number* of the machine displayed in <Check Device Configuration> in <Check Counter>

* You can also check the serial number through the SMS screen. ▶ **Managing MEAP Applications(P. 580)**

1 Open a Web browser to access <http://www.canon.com/lms/license/>

2 Follow the on-screen instructions to acquire the license file.

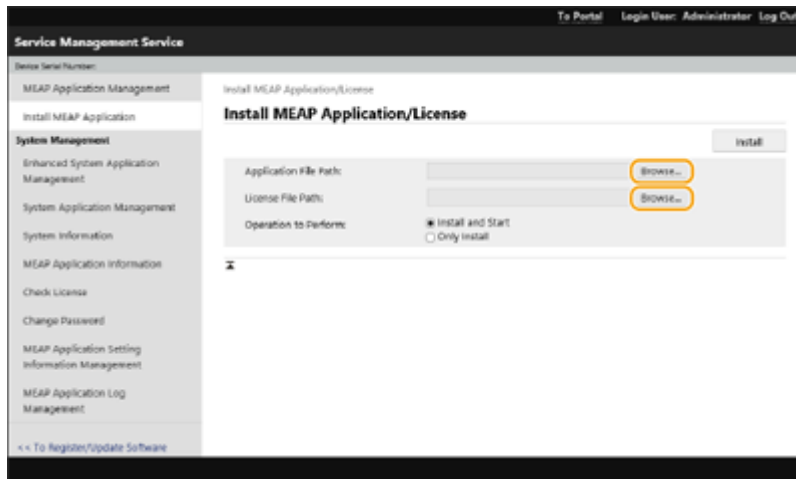
➡ After acquiring the license file, display the SMS to install the MEAP application.

Installing the Application

- 1 Log in to the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Service Management Service] on the portal page.
- 3 Click [Install MEAP Application].

Resource Name	Amount Used	Remaining	Percent Used
Storage	5700 KB	1462716 KB	0%
Memory	600 KB	77124 KB	1%
Threads	5	191	3%
Sockets	0	128	0%
File Descriptors	10	118	8%

- 4 Click [Choose File], specify the application file and the license file, and click [OK].



- Files with a ".jar" extension are application files.
- Files with an ".lic" extension are license files.

5 Select the operation to perform after installation.

- To start the application after installation, select [Install and Start]. If you do not want to start the application after installation, select [Only Install].

6 Click [Install] ► [Yes].

- When the licensing screen is displayed, confirm the contents and click [I Accept].
 ► When installation is complete, the MEAP Application Management screen is displayed.

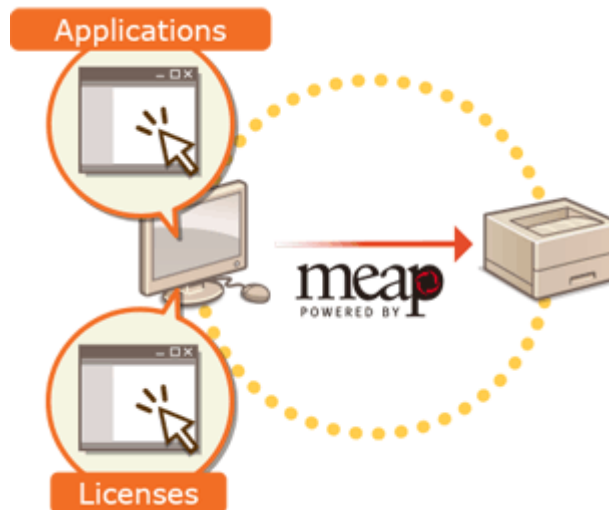
NOTE

- Depending on the MEAP application, the user's manual or related software can be downloaded from the following URL. <http://canon.com/fau/downloads>
- You can upgrade the MEAP application version in the same procedure as the installation. Stop the MEAP application on the SMS screen before installing. ► **Managing MEAP Applications(P. 580)**
- The maximum amount of storage device that applications can use is approximately 1,434 MB.
- If the machine is performing its shutdown process while an application is being installed, an error message may be displayed on the Install page for SMS, and the installation may be cancelled. In this case, try installing the MEAP application again after restarting the machine (turn the main power switch Off, and then On). For instructions on turning On/Off the machine, see ► **Turning OFF the Machine(P. 30)** , ► **Turning ON the Machine(P. 29)** .

Managing MEAP Applications

E9SJ-0C1

In addition to checking details and changing settings, you can upgrade MEAP applications or uninstall applications by using the SMS from the Remote UI.



! IMPORTANT

- While you are operating on the SMS screen, do not use the [Back] button on your Web browser, the SMS screen may not operate properly.

1 Log in to the Remote UI. ▶ **Starting the Remote UI(P. 329)**

2 Click [Service Management Service] on the portal page.

3 Configure the settings on the SMS screen.

Application Name	Updated	Status	License
LoginContextViewer	1.90.01 2022/11/01 19:15:06	Stopped	Start Uninstall Not Installed
Accounting Manager for MEAP SPP	3.6.5-JP 2022/11/01 19:14:25	Started	Stop Uninstall Installed

Resource Name	Amount Used	Remaining	Percent Used
Storage	46900 KB	1422115 KB	3%
Memory	3000 KB	72224 KB	7%
Threads	22	174	11%
Sockets	9	119	7%
File Descriptors	36	82	28%

a [Device Serial Number: <Serial Number>]

The machine's serial number is displayed. Use this number when acquiring a license file. ▶ **Acquiring the License File(P. 577)**

b Menu

If you click an item, the management page for the item appears.

- [MEAP Application Management]: The management of installed MEAP applications is mainly performed on this page.
- [Install MEAP Application]: A page for the installation and update of MEAP applications is displayed. ▶ **Installing MEAP Applications(P. 577)**
- [System Management]: A page for managing applications and information related to the MEAP system is displayed.

[Enhanced System Application Management]	Installs, uninstalls, and manages system applications that can be enhanced. You can change the login service from this page. ▶ Changing Login Services(P. 588)
[System Application Management]	Starts and stops the usage of installed system applications. Changing the SMS login method is performed from this page.
[System Information]	Displays the version and the operation status of a system application.
[MEAP Application Information]	Displays a list of applications (excluding system applications) currently installed and already uninstalled.
[Check License]	Displays the detailed information of license files before installation.
[Change Password]	Normally, it is not necessary to change this setting. You must enter between 8 and 32 alphanumeric characters for the password.
[MEAP Application Setting Information Management]	Displays or deletes information related to MEAP application settings. If there is setting information that is shared between the applications, [Shared Setting Information of Applications] is displayed. It can be deleted in the same way as other items.
[MEAP Application Log Management]	Downloads or deletes log data such as the usage history of MEAP applications.

c [Resource Information]

Displays the usage amount, remaining amount, and the usage rate of storage device space as well as memory that is used by a MEAP application and system applications.

d [MEAP Application Management]

Displays a MEAP application name and its version, the date of update, operation status, and the license status.

- If you click a MEAP application name, detailed information such as the company's name and the memory usage amount for each application is displayed. License management is performed from here. ▶ **Managing MEAP Application Licenses(P. 585)**
- For the operation status, one of the following is displayed.

[Installed]	The MEAP application has been installed, but it is not ready for use. Even if you restart the machine after stopping the use of the MEAP application, [Installed] is displayed.
[Started]	The MEAP application is ready for use.
[Stopped]	The MEAP application is not ready for use.
[Starting]	The MEAP application is starting.
[Stopping]	The MEAP application is stopping.

- If you click the [Start] / [Stop] button located on the right side of the operation status, you can start/stop the use of the MEAP application.
- If you click [Uninstall], the MEAP application is uninstalled.
- For the license status, one of the following is displayed.

Depending on the MEAP application, the license file may have a term of validity. In addition, the maximum number (counter) for printing is predetermined.

[Installed]	The valid license is installed.
[Not Installed]	Unable to use the MEAP application as the license file is not installed or is disabled.
[Over Limit]	Some counters set for the MEAP application exceed the maximum value.
[Invalid]	The validity for the license file has expired or all counters set for the MEAP application exceed the maximum value.
[Unnecessary]	You can use the MEAP application even if you do not have a license file.

NOTE

If [Over Limit] or [Invalid] appears

- If the validity of the license file expires or a counter exceeds the maximum value, the MEAP application cannot be used. By adding a license, you can extend the validity or increase the counter's maximum value.
- **Managing MEAP Application Licenses(P. 585)**

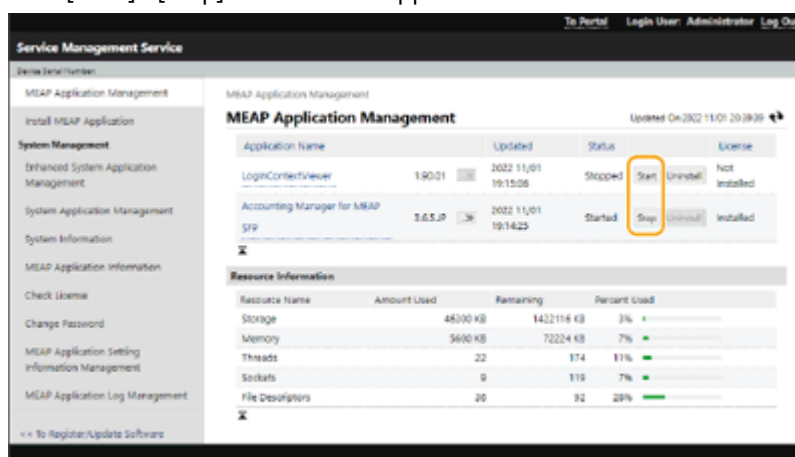
e [To Portal]/[Log Out]

Click to display the portal page of the Remote UI or the login screen of the Remote UI.

■ Starting or stopping the use of a MEAP application

If you selected [Only Install] in the installation of the MEAP application, you need to start the MEAP application. When you update a MEAP application, stop the MEAP application.

- 1 Click [MEAP Application Management].
- 2 Click [Start] / [Stop] for the MEAP application to be used.



NOTE:

- Depending on the MEAP application, you need to restart the machine. Follow the on-screen instructions and restart the machine.
- When the resources required for memory, threads, sockets, or file descriptors has run out, the application will not start, even if you click [Start].

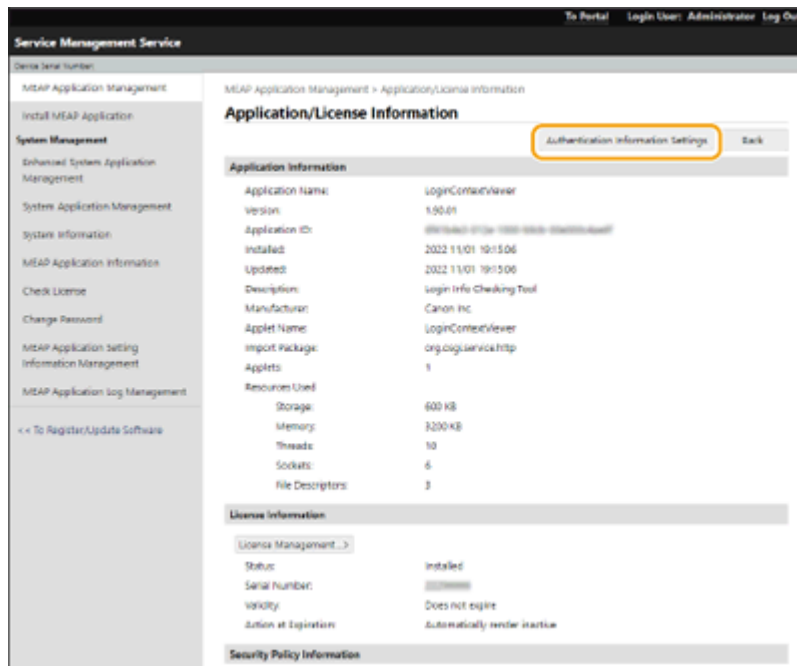
■Configuring the MEAP application's authentication information

Depending on the MEAP application, you may need to configure authentication information.

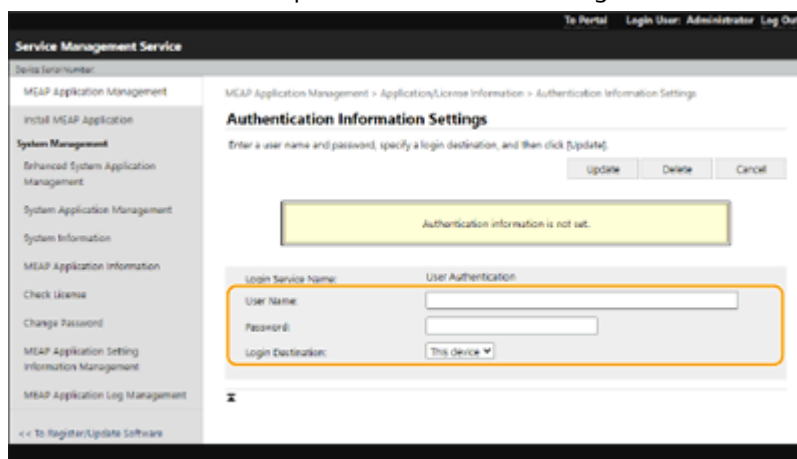
NOTE

- If the login application is changed, reconfirm the authentication information in [Set MEAP Authentication]. It may be necessary to re-enter the authentication information.

- 1 Click [MEAP Application Management] ► click an application to set the authentication information.
- 2 Click [Authentication Information Settings].



- 3 Enter the user name and password and select the login destination.



- 4 Click [Update].
- ▮▮▮▮ The [Authentication information has been set. Department ID: <ID>] message is displayed.

NOTE:

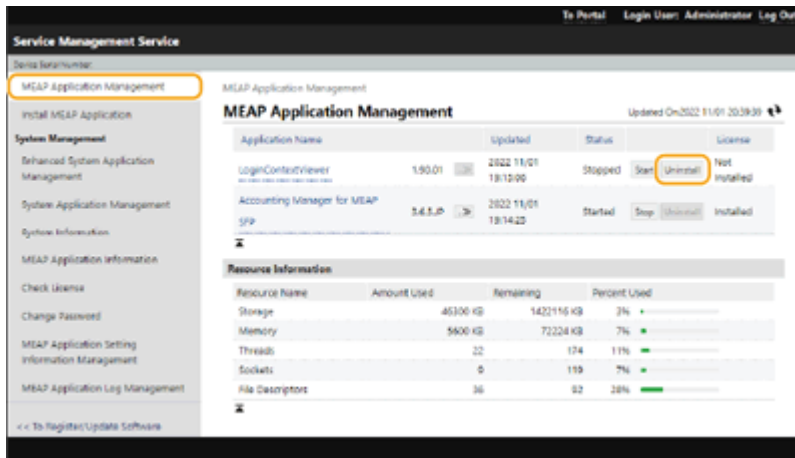
To cancel authentication information

- Click [Delete] ► [Yes] on the authentication information page in step 3.

■ Uninstalling a MEAP application

When uninstalling a MEAP application, you need to delete the corresponding license files in advance. **▶ Managing MEAP Application Licenses(P. 585)**

- 1 Click [MEAP Application Management] ▶ [Uninstall] for the application to be uninstalled.



- 2 Click [Yes].

- If you uninstall a MEAP application, you may be required to restart the machine. Follow the on-screen instructions to restart the machine.

! IMPORTANT:

- If the "Export Package of this application will be unavailable." message is displayed, the MEAP application you are uninstalling is linked with other applications. If this MEAP application is uninstalled, other applications may not be able to be used.

- 4 When you finish the operation, click [Log Out].

! IMPORTANT:

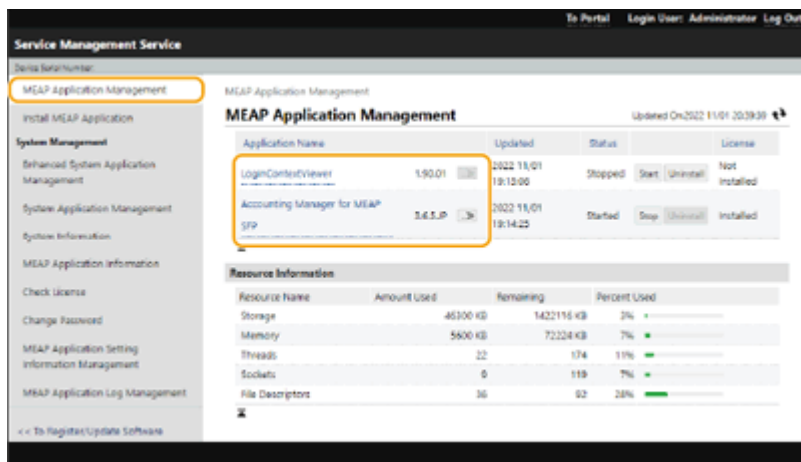
- When you close the SMS, make sure to log out. If you close the Web browser without logging out, you cannot use the SMS for some time.

Managing MEAP Application Licenses

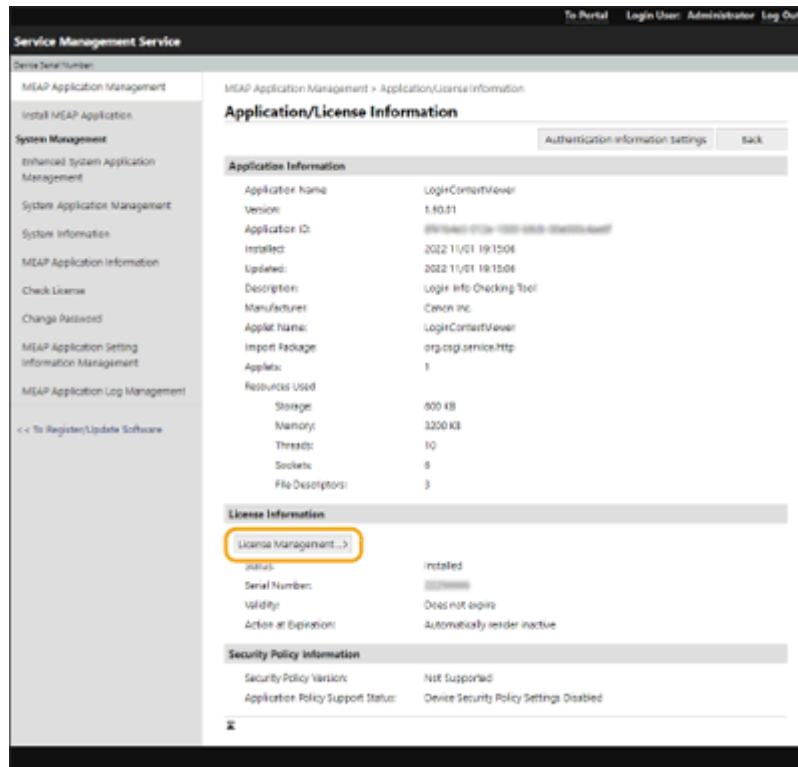
E9SJ-0C2

License file operation may be required at times other than installing a MEAP application. For example, even when the licensed counter value or usage period is exceeded or has expired, you can continue to use the MEAP application by adding a license file. In addition, if you want to delete a MEAP application, you are required to delete the license file in advance.

- 1 Log in to the Remote UI. ▶ Starting the Remote UI(P. 329)
- 2 Click [Service Management Service] on the portal page.
- 3 Click [MEAP Application Management], and click the application to manage the license.



- 4 Click [License Management] and perform the intended operation.



■ Adding a license file

- 1 Click [Choose File], select the license file to install, and click [OK].
 - 2 Click [Install] ► [Yes].
- Installation starts.

NOTE:

- Depending on the MEAP application, you may need to restart (stop and start) the application. ►
- Managing MEAP Applications(P. 580)**

■ Saving the license file on a computer

You can save a backup file on your computer before deleting the license file. If you want to save, you are required to disable the license file in advance.

- 1 Click [Disable] ► [Yes].
- 2 Click [Download], and specify the location to save the license file.

NOTE:

- The disabled license file and the license file saved on your computer can be installed on the same machine again.

■ Deleting the license file

Before deleting the license file, you are required to disable the license file in advance.

- 1 Click [Disable] ► [Yes].
- 2 Click [Delete] ► [Yes].



IMPORTANT:

- Once you have deleted the disabled license file, you cannot download it from the machine.

Changing Login Services

E9SJ-0C3

The application to implement user authentication is called the "Login Service." The machine is set to use "User Authentication (personal authentication management)" for the login service by default. To use a login service other than User Authentication, change the login service in SMS.

▶ **Changing the Login Service(P. 588)**

▶ **Settings when Using a Login Service Other Than User Authentication(P. 589)**

Changing the Login Service

- 1 Log in to the Remote UI. ▶ Starting the Remote UI(P. 329)**
- 2 Click [Service Management Service] on the portal page.**
- 3 Click [Start] for [SMS Installer Service (Password Authentication)] in [System Application Management], as required.**
 - ⇒ The status becomes [Started].
- 4 Click [Enhanced System Application Management] ▶ [Switch] for the login service to use.**
 - ⇒ The status becomes [Start after Restart].
- 5 Restart the machine. ▶ Restarting the Machine(P. 336)**
 - ⇒ The machine restarts and the changed settings are reflected.

IMPORTANT

When a login service other than User Authentication is started

- When the URL for SMS (<https://<IP address of the machine or host name>:8443/sms/>) is entered directly in a browser, the SMS login screen is displayed. For security purposes, the machine is configured not to permit login with the default password dedicated for SMS. Start the Remote UI ▶ select [Settings/Registration] ▶ [Security Settings] ▶ [Authentication/Password Settings] ▶ [Edit] for [Password Settings] ▶ temporarily select [Allow Use of Default Password for Remote Access].
- After logging in to SMS with the default password, restore the security level by changing the default password then deselecting [Allow Use of Default Password for Remote Access].
- "MeapSmsLogin" is set as the login password dedicated for SMS. If you log in with "MeapSmsLogin," the screen for changing the password is displayed. For security purposes, follow the on-screen instructions to change the password.
- The password for SMS can be changed with [Change Password] in [System Management].
- Make sure that you do not forget your password. Otherwise, you will not be able to access SMS. In this case, contact your dealer or service representative.

Return to User Authentication

- Select [Enhanced System Application Management] ► [User Authentication], click [Switch], and restart the machine. If you will not use SMS Installer Service (Password Authentication), after restart of the machine select [System Application Management] ► [SMS Installer Service (Password Authentication)], and click [Stop].

Settings when Using a Login Service Other Than User Authentication

When using Department ID Management with a login service other than User Authentication, make sure that the administrator (System Manager) manages the Department IDs and PINs. To enhance security, make sure to log in with the System Manager ID immediately after starting to use the login service other than User Authentication and change the System Manager ID and PIN.

Which users become administrator or general users depends on whether Department ID Management and System Manager Settings are set, as indicated in the table below.

Department ID Management	System Manager Settings	Administrator	General Users
On	Set	System Manager	Users authenticated with a Department ID and PIN not for the System Manager
	Not Set	Users authenticated with a Department ID and PIN	None
Off	Set	System Manager	Users other than the System Manager
	Not Set	All users	None

■ Changing the System Manager ID and PIN

- 1 Select <Set> on the <Home> screen.  **<Home> Screen(P. 150)**
- 2 Enter the ID and PIN in <System Manager ID> and <System Manager PIN>, and press .
 - Immediately after the login service has started, both the System Manager ID and PIN are set as "7654321."
 - You cannot register a Department ID or PIN consisting only of 0s, such as "00" or "0000000".
 - Even if you enter fewer than seven digits, zeros are added to the start of the number, and a seven digit number is set. However, the zeros at the start of the number can be omitted when logging in. For example, even if you enter <2>, <02>, or <002>, the PIN is set as <0000002>. However, you can log in by entering <2>, <02>, or <002>.
- 3 Select <Management Settings> ► <User Management> ► <System Manager Information Settings> ► <System Manager ID and PIN>.
- 4 Enter the necessary information and press .
 - Enter the same PIN again for confirmation, and press .

■ Enabling Department ID Management

To enable Department ID Management, you need to register the Department ID and PIN.

- 1 Start the Remote UI. **Starting the Remote UI(P. 329)**
- 2 Select [Settings/Registration] ► [User Management] ► [Department ID Management] ► click [Edit].
- 3 Select [Enable Department ID Management], and click [OK].
 - If you want to manage only with the System Manager ID and PIN without implementing Department ID Management, deselect [Enable Department ID Management].

! IMPORTANT:

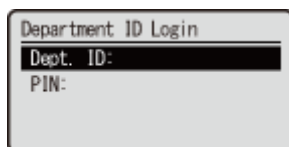
- If you want to return the login service to User Authentication and use Department IDs, follow the procedure below to enable Department ID Management.
 - 1 Deselect [Enable Department ID Management] for the login service other than User Authentication.
 - 2 Start User Authentication.
 - 3 Assign Department IDs to users.
 - 4 Select [Enable Department ID Management] for User Authentication.
- 4 Click [Register New Department].
- 5 Enter the ID and PIN in [Department ID] and [PIN], and click [OK].
 - Enter the same PIN again in [Confirm] for confirmation.
 - You cannot register a Department ID or PIN consisting only of 0s, such as "00" or "0000000".
 - Even if you enter fewer than seven digits, zeros are added to the start of the number, and a seven digit number is set. However, the zeros at the start of the number can be omitted when logging in. For example, even if you enter <2>, <02>, or <002>, the PIN is set as <0000002>. However, you can log in by entering <2>, <02>, or <002>.
 - If you do not set a PIN, you can use the machine by entering only the Department ID.

■ Login Operation When Department ID Management is Enabled

When Department ID Management is enabled, you need to log in to use the machine.

Logging in from the control panel

Enter the ID and PIN in <Department ID> and <PIN> ► press **OK**.



NOTE

When Department ID Management is not implemented

- When only the System Manager ID and PIN are set without Department ID Management, you need to log in to the machine only when you want to configure the settings that require the administrator's authority. Enter the ID and PIN in <System Manager ID> and <System Manager PIN>, and press **ID**.

Logging in from the Remote UI

The login method may differ from that for Department ID Management, depending on the login service you are using. For details, see the instruction manual for the login service.

■ Implementing Function Restrictions and User Management

Configure the settings as necessary.

Checking page totals



Start the Remote UI ► select [Settings/Registration] ► [User Management] ► [Department ID Management] ► check the counter information.

Setting the maximum number of pages for print



Start the Remote UI ► select [Settings/Registration] ► [User Management] ► [Department ID Management] ► select the Department ID ► select [Total Prints] for [Page Limit] ► enter the total page count ► click [OK].

Deleting Department IDs



Start the Remote UI ► select [Settings/Registration] ► [User Management] ► [Department ID Management] ► click [Delete] for the Department ID to delete.

Blocking printer jobs when Department ID is unknown



Start the Remote UI ► select [Settings/Registration] ► [User Management] ► [Department ID Management] ► [Edit] ► deselect [Allow Printer Jobs with Unknown IDs] ► click [OK].

Blocking black and white printer jobs when Department ID Management is enabled



Start the Remote UI ► select [Settings/Registration] ► [User Management] ► [Department ID Management] ► [Edit] ► deselect [Allow Black & White Printer Jobs] ► click [OK].

LINKS

🔗 **Configuring the Personal Authentication Management Settings(P. 243)**

Basic Windows Operations

E9SJ-0AH

- ▶ **Displaying the Printer Folder(P. 592)**
- ▶ **Displaying Shared Printers in the Print Server(P. 592)**
- ▶ **Checking the LPR/RAW Printer Port(P. 594)**
- ▶ **When Printing from the Microsoft Store App(P. 595)**
- ▶ **Registering Application on Microsoft Entra ID(P. 595)**

NOTE

- Depending on the computer that you use, the operation may differ.

■ Displaying the Printer Folder

Windows Server 2012 R2

Right-click [Start] ▶ select [Control Panel] ▶ [View devices and printers].

Windows 10 /Windows Server 2016/Windows Server 2019/Windows Server 2022/Windows Server 2025

[

Windows 11

Right-click [

■ Displaying Shared Printers in the Print Server

1 Open Windows Explorer.

Windows Server 2012 R2

Right-click [Start] ▶ select [File Explorer].

Windows 10 /Windows Server 2016/Windows Server 2019/Windows Server 2022/Windows Server 2025

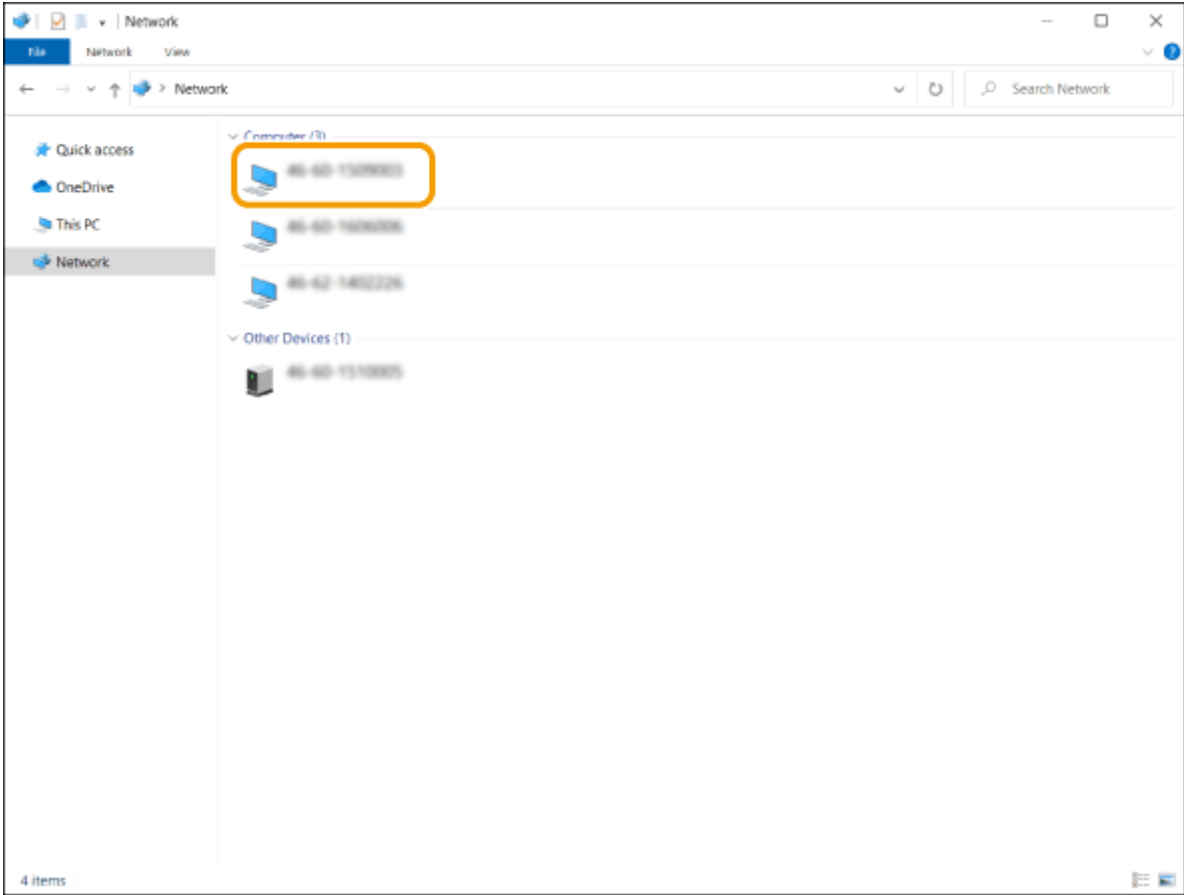
Right-click [

Windows 11

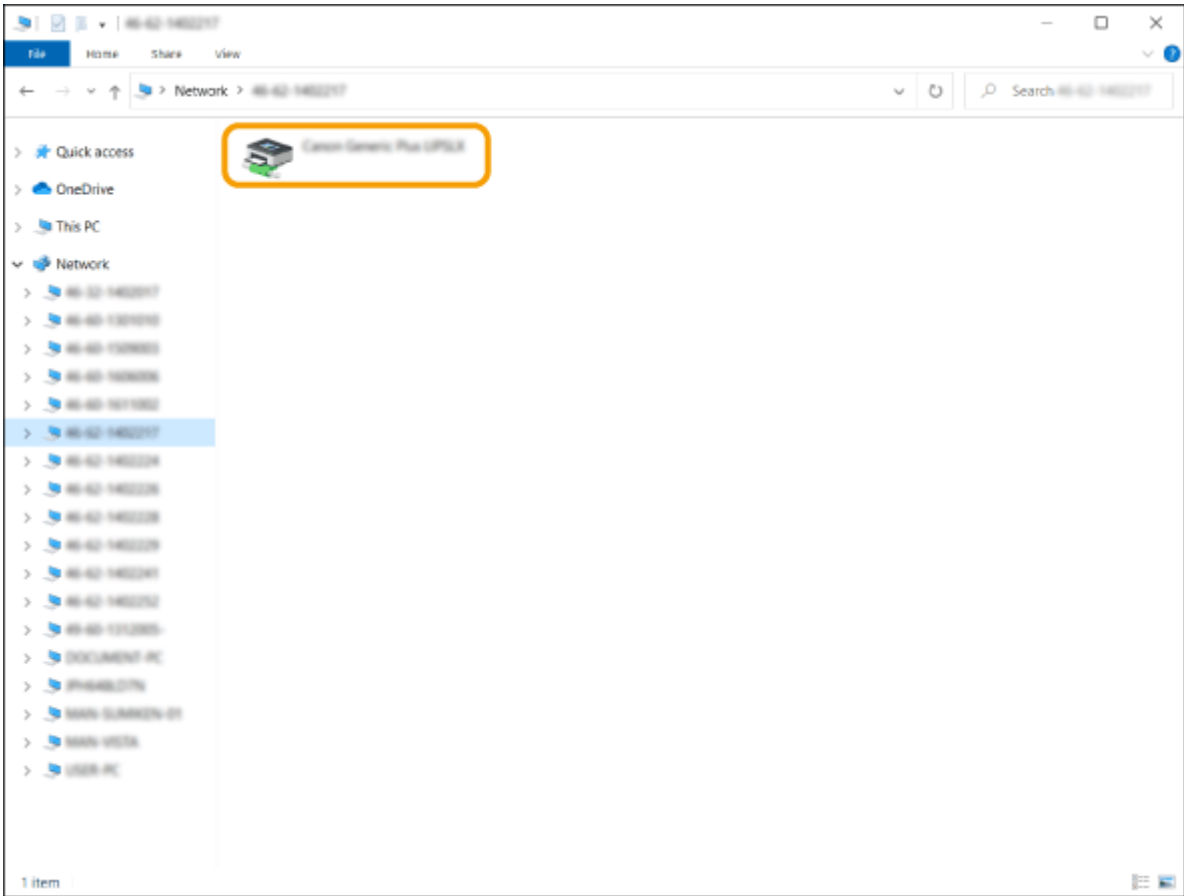
Right-click [

2 Select the print server from [Network].

- To view computers on the network, you may need to turn on network discovery or search the network for computers.



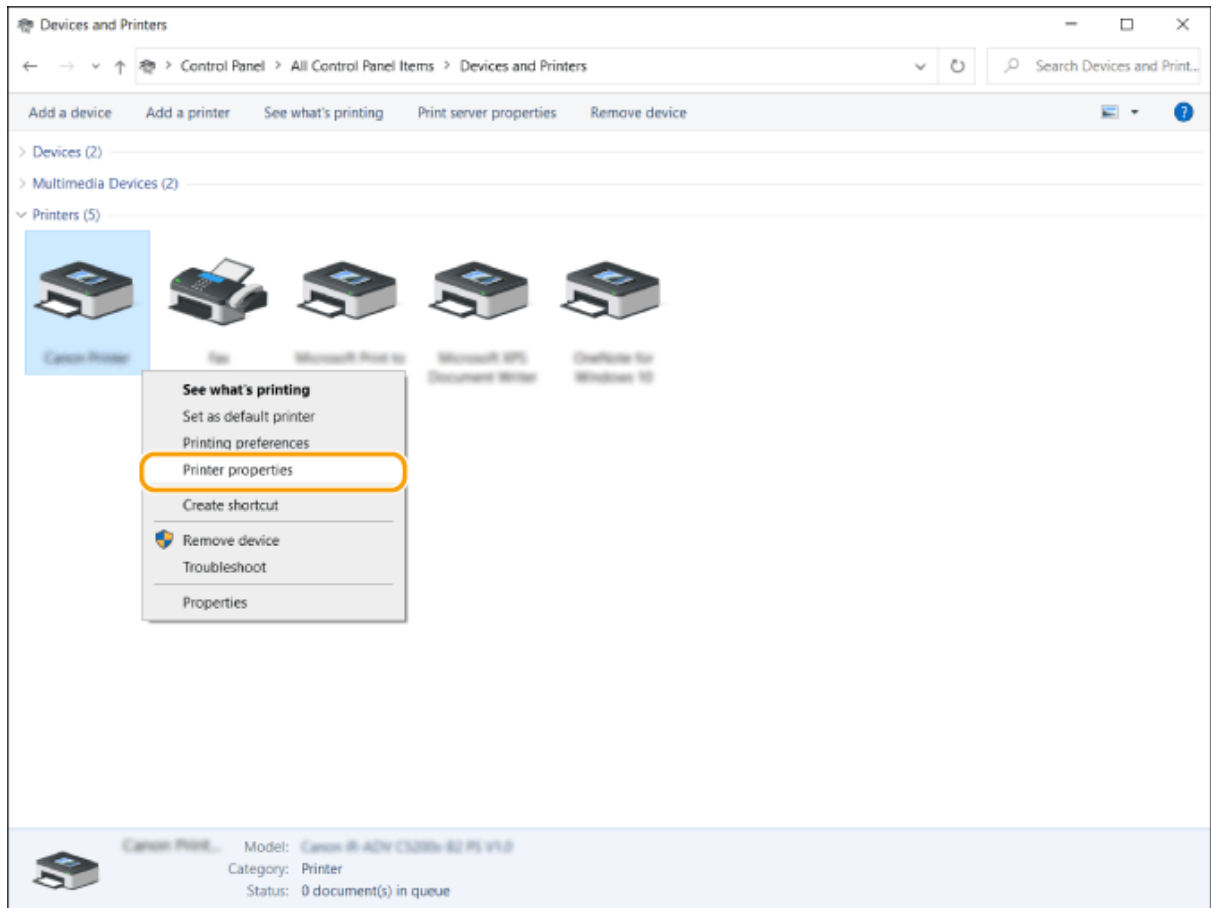
⇒ The shared printer is displayed.



■ Checking the LPR/RAW Printer Port

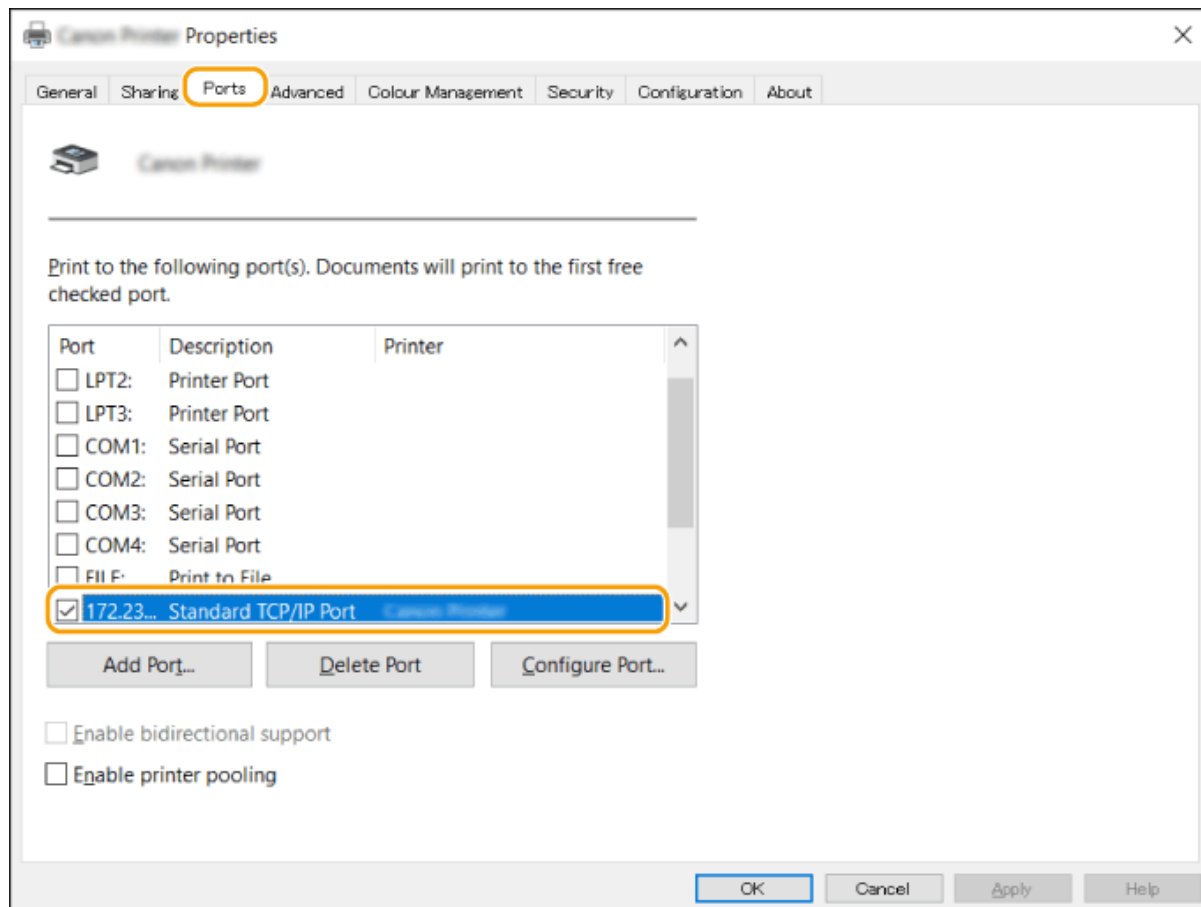
1 Open the printer folder. ▶ Displaying the Printer Folder(P. 592)

2 Right-click your printer icon of the machine and click [Printer properties].



3 Check the port settings.

- Click the [Ports] tab.
- Make sure that the correct port is selected for the printer.



■ When Printing from the Microsoft Store App

Windows Server 2012 R2

Display the charms on the right side of the screen ► Tap or click [Devices] ► [Print] ► The driver that you use ► [Print].

Windows 10

Tap or click [Print] on the application ► The driver that you use ► [Print].

NOTE

- If you print using this method, only a limited number of print settings are available.
- If the message [The printer requires your attention. Go to the desktop to take care of it.] is displayed, go to the desktop and follow the instructions in the displayed dialog box. This message appears when the machine is set to display the user name during printing and similar instances.

■ Registering Application on Microsoft Entra ID

- 1** Login to Microsoft Entra admin center.
- 2** Click Microsoft Entra ID on the navigation menu.
- 3** Click where you can register an application on the navigation menu.

4 Click where you can start registering a new application.

5 Enter the name of the application.

You can enter any name you want. (Example: Canon "Printer name" Login)

6 Select the type of the account.

7 Click where you can finish your registration.

⇒ A client ID for the application is issued.

Copy the client ID on a text editor to store it.

8 Issue a secret or register a certificate.

■ Issuing a Secret

- 1 Click where you can manage a certificate and a secret on the navigation menu.
- 2 Click where you can manage a new client secret.
- 3 In the dialog for adding a client secret, enter the description and the valid period of the new client secret and click where you can complete adding the new client secret.

⇒ A secret ID and a secret value are issued.

Copy the secret value on a text editor to store it. The secret ID is not used.

! IMPORTANT:

- The client secret value will not be displayed again. If you have not stored the client secret value, issue a new client secret.

■ Registering a Certificate

If you want to register a certificate, it is necessary to export the certificate of the machine beforehand. ▶
Specifying the domain of Microsoft Entra ID(P. 266)

- 1 Click where you can manage a certificate and a secret on the navigation menu.
 - 2 Click where you can upload a certificate.
 - 3 Select a certificate file and click where you can start adding the certificate.
- ⇒ After uploading is complete, copy the thumbprint value to a text editor to store it.

9 On the navigation menu, click where you can add permissions for a registered application to access API.

10 Click where you can add access permissions.

11 Select Microsoft Graph from listed API names from which you can request access permissions.

12 Select Delegated permissions among the access permission types and assign the following access permissions.

- User.Read.All
- Group.Read.All
- GroupMember.Read.All

13 Select Application permissions among the access permission types and assign the following access permissions.

- User.Read.All
- User.ReadWrite.All (When you want to register or delete an IC card from the machine)
- Group.Read.All
- GroupMember.Read.All

NOTE

- Access permissions are used when IC Card authentication is used or when you cannot login to the machine due to an error of multi-factor authentication. Access permissions are not needed depending on used functions or environments.

14 Click where you can grant admin consent and select Yes.

- ➡ Admin consent is assigned to access permissions that are selected under Delegated permission or Application permissions.

System Specifications

E9SJ-0AJ

This section presents the system specifications for this product. Specifications are subject to change without notice for product improvement or future release.

NOTE

- To check the specifications of the main unit and optional equipment for this product, see **▶Hardware Specifications(P. 88)** .

■ Functional Specifications

▶Printer Functions(P. 599)

▶Management Functions(P. 602)

■ Environment To Use the Machine

▶System Environment(P. 607)

▶Network Environment(P. 608)

▶System Options(P. 610)

Printer Functions

E9SJ-0AK

■ UFR II Printer Function

Type	Internal
Print Size	▶ Available Paper(P. 91)
Print Speed	Same as "Print Speed" in "Main Unit" ▶ Main Unit(P. 89)
Data Processing Resolution	600 dpi x 600 dpi, 1200 dpi x 1200 dpi
Page Description Language (PDL)	UFR II
Protocol Supported	TCP/IP (LPD/Port9100/IPP/IPPS/FTP/WSD)
Compatible OS	- Windows 10/Windows 11/Windows Server 2016/Windows Server 2019/Windows Server 2022/Windows Server 2025 - macOS (10.15 or later)
Resident Fonts	None
Interface	USB 2.0High-Speed, 1000Base-T/100Base-TX/10Base-T (IEEE 802.3 compliant), Wi-Fi (IEEE 802.11b/g/n)

■ PCL Printer Function

Type	Internal
Print Size	▶ Available Paper(P. 91)
Print Speed	Same as "Print Speed" in "Main Unit" ▶ Main Unit(P. 89)
Data Processing Resolution	- PCL5: 600 dpi x 600 dpi - PCL6: 600 dpi x 600 dpi, 1200 dpi x 1200 dpi
Page Description Language (PDL)	PCL5, PCL6
Protocol Supported	TCP/IP (LPD/Port9100/IPP/IPPS/FTP/WSD)
Compatible OS	Windows 10/Windows 11/Windows Server 2016/Windows Server 2019/Windows Server 2022/Windows Server 2025

Resident Fonts	93 Roman, 10 Bitmap fonts, 2 OCR fonts, Andalé Mono WT J/K/S/T* ¹ (Japanese, Korean, Simplified Chinese, and Traditional Chinese) , Barcode fonts* ²
Interface	USB 2.0High-Speed, 1000Base-T/100Base-TX/10Base-T (IEEE 802.3 compliant), Wi-Fi (IEEE 802.11b/g/n)

*1 Requires optional PCL International Font Set

*2 Require optional Barcode Printing Kit

■ PS Printer Function

Type	Internal
Print Size	➡ Available Paper(P. 91)
Print Speed	Same as "Print Speed" in "Main Unit" ➡ Main Unit(P. 89)
Data Processing Resolution	600 dpi x 600 dpi, 1200 dpi x 1200 dpi
Page Description Language (PDL)	Adobe PostScript 3
Protocol Supported	TCP/IP (LPD/Port9100/IPP/IPPS/FTP/WSD)
Compatible OS	Driver - Windows 10/Windows 11/Windows Server 2016/Windows Server 2019/Windows Server 2022/Windows Server 2025 - macOS (10.15 or later) PPD - Windows 10/Windows 11 - macOS (10.15 or later)
Resident Fonts	136 Roman
Interface	USB 2.0High-Speed, 1000Base-T/100Base-TX/10Base-T (IEEE 802.3 compliant), Wi-Fi (IEEE 802.11b/g/n)

■ E-Mail Print Function

Compatible Mail Receiving Server Software	- Microsoft Exchange Server 2016 - Microsoft Exchange Server 2019 - Qpopper 4.1.0 - Microsoft Exchange Online - Google Workspace
Protocol Supported	POP3 (receive* ¹), SMTP (receive* ²)

Appendix

Supported Attachment File Decoding Formats	uuencode, x-uuencode, base64
Printable Format of Attached Image Files	TIFF

*1 Supports APOP and encrypted (TLS) communication when receiving POP.

*2 Supports encrypted (TLS) communication when SMTP is received.

Management Functions

E9SJ-0AL

■ Information Registered in User Authentication

Up to 5,001 users can be registered.

■ Registering Department IDs

Up to 1,000 Department IDs can be registered.

■ Authentication Functions

- When an Active Directory server is specified as an authentication server, the following system environment is required.

Software (operating system):	Windows Server 2016 ^{*1} /Windows Server 2019 ^{*1} / Windows Server 2022 ^{*1} /Windows Server 2025 ^{*1*2}
-------------------------------------	---

^{*1} Users cannot log in with Active Directory authentication if Kerberos Armoring is enabled for KDC-related policies (group policies). Make sure to disable Kerberos Armoring.

^{*2} In Windows Server 2025 or later OS, LDAP/LDAPS communication is not possible with the default settings of Windows Server. Install a server certificate on Windows Server and communicate with LDAPS (TLS).

- Kerberos encryption methods for the Active Directory authentication supported by the current version of User Authentication are as follows.

Encryption method	- AES (Advanced Encryption Standard) 128 bit - AES (Advanced Encryption Standard) 256 bit - DES (Data Encryption Standard) - RC4
--------------------------	---

NOTE

- The available encryption methods may vary, depending on the Active Directory settings.
 - Of the available encryption methods, the one with the highest cipher strength is automatically selected.
- When specifying an Active Directory server as an authentication server, use the following ports^{*1} on the server.

To communicate with a DNS server:	port number 53
To communicate with a KDC (Key Distribution Center):	port number 88

To communicate with a server for LDAP directory service (can be changed to an arbitrary port number for the LDAP service):	port number 389
---	-----------------

*1 The above port numbers are default values. These numbers may vary depending on the selected settings.

- When specifying an LDAP server as an authentication server, the following system environment is required.

Software:	OpenLDAP
Operating system:	Requirements are pursuant to the product specifications of the LDAP server.

- When specifying an LDAP server as an authentication server, use the following ports*1 on the server.

To communicate with the LDAP server using LDAP (when TLS is enabled):	port number 636
To communicate with the LDAP server using LDAP (when TLS is disabled):	port number 389

*1 The port numbers can be changed according to the LDAP server settings.

■ Firewall Settings

- When specifying IP addresses in firewall settings, up to 16 IP addresses (or ranges of IP addresses) can be specified for both IPv4 and IPv6.
- When specifying MAC addresses in firewall settings, up to 100 MAC addresses can be specified.
- The exception addresses and exception port numbers that can be used for communication using the sub line and are registered by default are indicated below.

Exception addresses:	0.0.0.1 to 255.255.255.255
Exception port numbers:	53, 67, 68, 80, 161, 443, 515*, 631*, 3702, 5353, 5357, 5358, 8000*, 8080, 8443*, 9013, 9100*, 10443*, 20010*, 47545

* Inbound filter only

■ Registration of Keys and Certificates

- If you install a key or CA certificate from a computer, make sure that they meet the following requirements:

Format	Key: PKCS#12*1*2 CA certificate: X.509 DER format/PEM format
File extension	Key: ".p12" or ".pfx" CA certificate: ".cer" or ".pem"
Public key algorithm (and key length)	- RSA (512 bits, 1024 bits, 2048 bits, 4096 bits) - DSA (1024 bits, 2048 bits, 3072 bits)*1 - ECDSA (P256, P384, P521)
Certificate signature algorithm	RSA: SHA-1*1, SHA-256, SHA-384*3, SHA-512*3, MD2*1, MD5*1

	• DSA: SHA-1*1 • ECDSA: SHA-1*1, SHA-256, SHA-384, SHA-512
Certificate thumbprint algorithm	SHA-1

*1 Available only when installed by using the Remote UI.

*2 Requirements for the certificate contained in a key are pursuant to CA certificates.

*3 SHA384-RSA and SHA512-RSA are available only when the RSA key length is 1024 bits or more.

■ Registration of Certificate Revocation Lists (CRL)

Up to 50 certificate revocation lists (CRL) can be registered. Note, however, that CRL cannot be registered in the following cases.

- The data size of the CRL exceeds 1 MB.
- An unsupported signature algorithm is being used.
- The number of revoked certificates registered in one CRL file exceeds 10,000.

■ Definition of "Weak Encryption"

When <Prohibit Use of Weak Encryption> is selected, the use of the following algorithms is prohibited.

Hash:	MD4, MD5, SHA-1
HMAC:	HMAC-MD5
Common key cryptosystem:	RC2, RC4, DES
Public key cryptosystem:	RSA encryption (512 bits/1024 bits), RSA signature (512 bits/1024 bits), DSA (512 bits/1024 bits), DH (512 bits/1024 bits)

NOTE

- Even when <Prohibit Use of Key/Certificate with Weak Encryption> is selected, the hash algorithm SHA-1, which is used for signing a root certificate, can be used.

■ FIPS 140 Standard Algorithm

When <Format Encryption Method to FIPS 140> is selected, the following algorithms are prohibited from use.

Hash:	MD4, MD5, SHA-1 (for a purpose other than TLS)
Common key cryptosystem:	RC2, RC4, DES, PBE
Public key cryptosystem:	RSA encryption (512 bits/1024 bits), RSA signature (512 bits/1024 bits), DSA signature (512 bits/1024 bits), DH (512 bits/1024 bits)

■ Log Management

- The following types of logs can be managed on the machine. Collected logs can be exported in the CSV file format.

Log Type	Number Indicated as "Log Type" in the CSV File	Description
User Authentication Log	4098	This log contains information related to the authentication status of user authentication (login/logout and user authentication success/failure), the registering/changing/deleting of user information managed with User Authentication.
Job Log	1001	This log contains information related to the completion of print jobs.
Receive Log	8193	This log contains information related to reception.
Machine Management Log	8198	This log contains information related to the starting/shutting down of the machine and changes made to the settings using <Set>. The Machine Management Log also records changes in user information or security-related settings when the machine is inspected or repaired by your dealer or service representative.
Network Authentication Log	8200	This log is recorded when IPSec communication fails.
Export/Import All Log	8202	This log contains information related to the importing/exporting of the settings by using the Export All/Import All function.
Application/Software Management Screen Operation Log	3101	This is an operation log for software registration/updates, and MEAP application installers, etc.
Security Policy Log	8204	This log contains information related to the setting status of the security policy settings.
System Maintenance Log	8206	This log contains information related to firmware updates and backup/restoration of the MEAP application, etc.
Authentication Print Log	8207	This log contains information and the operation history related to the forced hold print jobs.
Log for Audit Log Management	3001	This log contains information related to the starting and ending of this function (the Audit Log Management function), as well as the exporting of logs, etc.

NOTE

- Logs can contain up to 40,000 records. When the number of records exceeds 40,000, they are deleted, with the oldest records first.

■ Import/Export of the Setting Data

See  **Settings/Registration(P. 386)** .

■ SCEP Server Support

Only the Network Device Enrollment Service (NDES) of Windows Server 2012 R2/2016/2019/2022/2025 is supported.

System Environment

E9SJ-0AR

System requirements for the Remote UI *1	Windows • Microsoft Edge • Google Chrome Mac OS • Safari 11 or later • Google Chrome
---	--

*1 Before changing the settings of the machine, set your Web browser to enable all cookies and use JavaScript.

Network Environment

E9SJ-0AS

■ Wired LAN Specifications

Interface (Primary line/Secondary line)	10Base-T/100Base-TX/1000Base-T (RJ-45)
Protocol Supported	TCP/IP • Frame type: Ethernet II • Print applications: LPD/Raw/IPP/IPPS/FTP/WSD/Mopria/AirPrint/Windows 10 Mobile Print/Universal Print/IPP Everywhere

NOTE

- For precautions related to the sub line, see [▶ Cautions When Using the Sub Line\(P. 571\)](#) .

■ Wireless LAN Specifications

Standard	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Transmission Scheme	• IEEE 802.11b (Modulation system: DS-SS) • IEEE 802.11g (Modulation system: OFDM method) • IEEE 802.11n (Modulation system: OFDM method)
Security (encryption method)	Infrastructure Mode • WPA-PSK (AES-CCMP) • WPA2-PSK (AES-CCMP) • WPA3-SAE (AES-CCMP) • WPA-EAP (AES-CCMP) • WPA2-EAP (AES-CCMP) • WPA3-EAP (AES-CCMP) Access Point Mode WPA2-PSK (AES-CCMP) Wi-Fi Direct Mode WPA2-PSK (AES-CCMP)
Connection Method	WPS (Wi-Fi Protected Setup), Manual setup

Port Numbers Available for Direct Connection

Type	Port Number	Protocol
TCP	515	LPD

Appendix

	9100	RAW
	80, 8000, 8080	HTTP
	631	IPP
	443, 10443	IPPS
	443, 8443	HTTPS
	9013	CPCA (unique Canon protocol)
	5357, 5358	WSD
UDP	161	SNMP
	5353	mDNS
	67, 68	DHCPv4
	3702	WSD
	47545	CPCA (unique Canon protocol)

System Options

E9SJ-0AU

By installing system-related options, you can further enhance the performance of the machine.

■ Barcode Printing Kit

This option enables you to print barcodes. For more details, see Bar Code Printing via the online manual site.

■ PCL International Font Set

This option enables you to add the following fonts for a PCL printer. As a result, you can output using multiple languages in a SAP Unicode environment.

- Andale® and WorldType® Collection J (Japanese Version)
- Andale® and WorldType® Collection K (Korean Version)
- Andale® and WorldType® Collection S (Simplified Chinese Version)
- Andale® and WorldType® Collection T (Traditional Chinese Version)

In order to support differences in character design depending on the region, four font versions are enabled.

■ PCL Asian Font Set

This option enables you to add the asian fonts for a PCL printer. As a result, you can output using asian languages.

This Font Software is licensed under the SIL Open Font License, Version 1.1.
This license is copied below, and is also available with a FAQ at:
<https://openfontlicense.org>

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components,

in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.