P C375

User Guide



For safe and correct use, be sure to read Safety Information separately provided before using the machine.

TABLE OF CONTENTS

1. Introduction and Basic Operations 5

About This Manual 5
Abbreviated Names of Options 5
Basic Operation of the Machine 6
Turning On and Off the Power 6
Guide to Names and Functions of Components 9
Names and Functions of the Control Panel 14
Names and Functions of the Operation Screen 15
How to Use the Selection Keys 16
User Authentication 17
Logging In from the Control Panel 17
Loading Paper 18
Loading Paper into the Paper Tray 18
Operating or Configuring the Machine from Computer (Web Image Monitor) 28
What You Can Do on the Web Image Monitor 29
Accessing to Web Image Monitor 30
Web Image Monitor Screen 31
Specifying Web Image Monitor Help 32

2. Printer 35

Basic Printing 35
Basic Procedure for Printing Documents 35
Printing on Both Sides of Paper 39
Combining and Printing Multiple Pages on a Single Sheet of Paper 40
Printing on Envelopes 41
Printing from a Storage Media 45
Printing from a USB Flash Memory Device Directly 45

3. Maintenance 47

Replacement and Replenishment of Consumables 47
Replacing the Print Cartridge 47
Replacing the Waste Toner Bottle 50
Replacing the Drum Unit 53
Replacing the Transfer Unit 56
Replacing the Fusing Unit 58

4. Troubleshooting 59
Getting Started 59
Alert Sounds 59
Checking the Indicators, Icons, and Messages on the Control Panel 59
When Messages Appear 62
Status Messages 62
Alert Messages that Appear on the Control Panel 63
Alert Messages that Are Printed on Error Logs and Reports 66
5. Security 75
Introduction 75
Taking Measures to Prevent Security Threats 75
Registering Administrators 78
Using the Supervisor Privilege 86
Usable Characters for User Names and Passwords 89
Preventing Unauthorized Accesses 91
Taking Measures to Prevent Unauthorized Access 91
Verifying Users to Operate the Machine (User Authentication) 92
Registering/Changing/Deleting User Codes 97
Preparing the Server to Use for User Authentication 98
Limiting Available Functions 103
Executing a Print Job with Authentication Information Only 104
Specifying the Policy on Login/Logout 106
Access Control 110
Encrypting Network Communication 120
Preventing Information Leaks 129
Taking Measures to Prevent Information Leaks 129
Preventing Data Leaks from Printed Sheets 130
Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine 132
Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator 136
6. Specifications 139
Paper Specifications 139
Recommended Paper Sizes and Types 139
Thick Paper Recommended Status 144

Envelope Orientation and Recommended Status 144
Loading Orientation-fixed Paper or Two-sided Paper 145
Machine and Options Specifications 147
Model-Specific Information 147
List of Specifications 148
Printable Area and Margin 153
Machine Options 154
Functions Requiring Optional Configurations 155
Legal and Contact Information 157
Environmental Regulations 157
Notes for wireless LAN 161
Trademarks (User Guide) 161
7. Setup **165**
Setting Up the Printer 165
Installing Options 165
8. Driver Installation Guide **171**
Installing the Printer Driver 171
Installing the Printer Driver by Using Device Software Manager Installer 171
Installing the Printer Driver for Network Connection (Windows) 173
Installing the Printer Driver for Network Connection (macOS) 179
9. How to use this manual **185**

1. Introduction and Basic Operations

About This Manual

Abbreviated Names of Options

In the manuals, the abbreviated names of options are used. The abbreviated names and corresponding product names are as follows:

Options that can be attached to the machine differ depending on the machine type.

page 154 "Machine Options"

Abbreviated names of externally attached options

Abbreviated name	Product name
Caster table	Caster Table Type M57
Lower paper tray	Paper Feed Unit PB1210

Abbreviated names of internal options

Abbreviated name	Product name
PostScript 3 unit	PostScript3 Unit Type P24
Device server option	Device Server Option Type P24
Wireless LAN board	IEEE 802.11a/b/g/n/ac Interface Unit Type M57

Basic Operation of the Machine

1

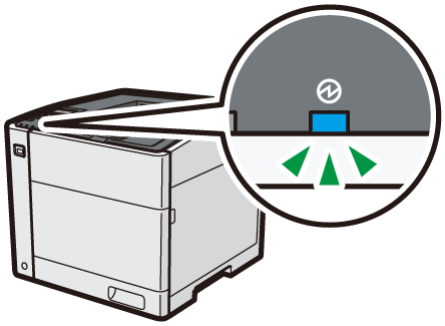
Turning On and Off the Power

To turn the machine on and off, press the power switch on the front left side of the machine.

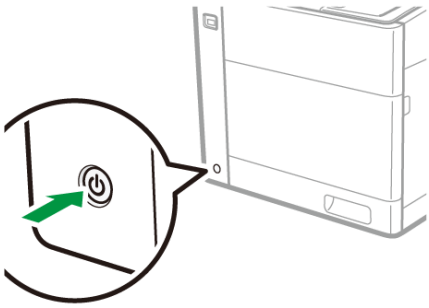
Turning On the Power

Important

- **Do not press the power switch repeatedly. When you turn the power on or off, wait at least 10 seconds after confirming that the power indicator on the control panel has turned on or off.**



1. **Make sure the power cord is firmly plugged into the wall outlet.**
2. **Push the power switch on the front left side of the main unit.**



The power indicator on the control panel turns on.

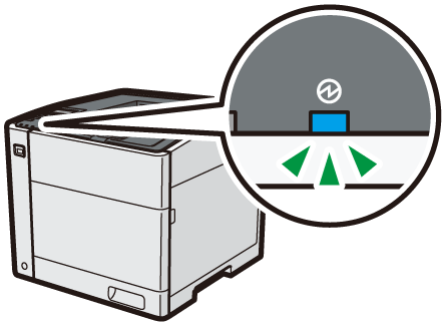
Note

- When the power is turned on, the screen may show that the machine is performing an auto restart. Do not turn off the power while the machine is processing. The machine takes up to seven minutes to restart.

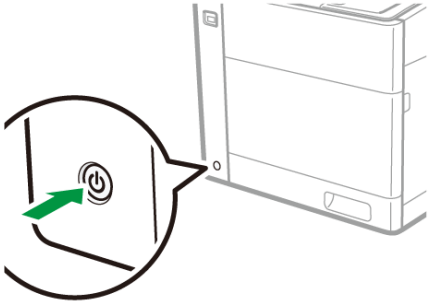
Turning Off the Power

Important

- **Do not turn off the power while the machine is in operation. To turn the power off, confirm that the operation is finished.**
- **Do not hold down the power switch while turning off the power. Doing so forcibly turns off the machine's power and may damage the internal storage or memory and cause malfunctions.**
- **Do not press the power switch repeatedly. When you turn the power on or off, wait at least 10 seconds after confirming that the power indicator on the control panel has turned on or off.**



1. **Push the power switch on the front left side of the main unit.**



The power indicator on the control panel turns off. The main power turns off automatically after the machine has shut down properly.

Energy Saving Mode

When the machine is not operated for a specified period of time, the machine enters the "Energy Saving mode" automatically. "Energy Saving mode" has two modes, "Fusing Unit Off mode" and "Sleep mode", and the machine enters the Fusing Unit Off mode first. In the factory default, the machine is configured to use both modes.

Fusing Unit Off Mode

In this mode, the power indicator is lit. Because the heater of the fusing unit is turned off but the screen of the control panel is still displayed, the power consumption decreases, but you can start operation promptly. If you do not operate

the machine for a specified period of time, the machine emits a clicking sound and enters Fusing Unit Off mode.

- You can specify whether to enable the Fusing Unit Off mode and the time to wait before the machine enters Fusing Unit Off mode under [Fusing Unit Off Mode (Energy Saving) On/Off].

  See System, User Guide in English.

Sleep Mode

In this mode, the display of the control panel turns off and the power indicator blinks slowly. Power consumption is minimized. The machine enters Sleep mode when no operation is performed for the specified period of time.

- You can specify the amount of time that the machine waits before entering Sleep mode under [Sleep Mode Timer].

  See System, User Guide in English.

- The machine recovers from Sleep mode when you perform one of the following:
  - Press any key on the control panel.

Note

- The energy saving functions are disabled when an error occurs or while an operation is in progress.
- The energy saving functions will not operate in the following cases:
  - When fixed warm-up is in progress
  - When operations are suspended during printing
  - When a warning message appears (The machine enters Fusing Unit Off mode unless the cover is open.)
  - When paper is jammed (The machine enters Fusing Unit Off mode except when the cover is open.)
  - When the Data In indicator is lit or flashing (The machine enters Fusing Unit Off mode except when the Data In indicator is lit or flashing due storing documents.)
- The machine does not enter Sleep mode in the following cases:
  - During communication with external equipment
  - When the internal storage is active
  - When the service call message appears
  - When the "Add Toner" message appears
  - When toner is being replenished
  - When one of the following screens is displayed:
    - System
    - Counter

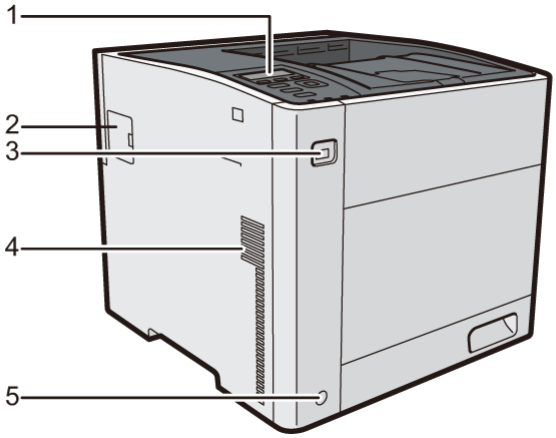
    - Paper Input
- When data is being processed
- When the sample print, locked print, hold print, or stored print screen is displayed
- When the internal cooling fan is active
- When accessing the machine using Web Image Monitor

Guide to Names and Functions of Components

⚠CAUTION

- Do not obstruct the machine's vents. Doing so can result in fire as the internal components are overheated.

Front and Left View



1. **Control panel**

   page 14 "Names and Functions of the Control Panel"
2. **Slot Cover**

   Remove this cover when you attach the wireless LAN board.
3. **Media slots**

   Insert an USB flash memory device. You can print the file stored on the media.

    - Use the media formatted in FAT16 or FAT32.
    - Certain types of USB flash memory devices such as one that supports encryption may not be used on the machine.
    - A USB extension cable, hub, or card reader cannot be used.

- If the power of the machine is turned off or the media is removed from the machine while the machine is reading the data in the media, check the data in the media.

4. **Vents**

   Prevent overheating.

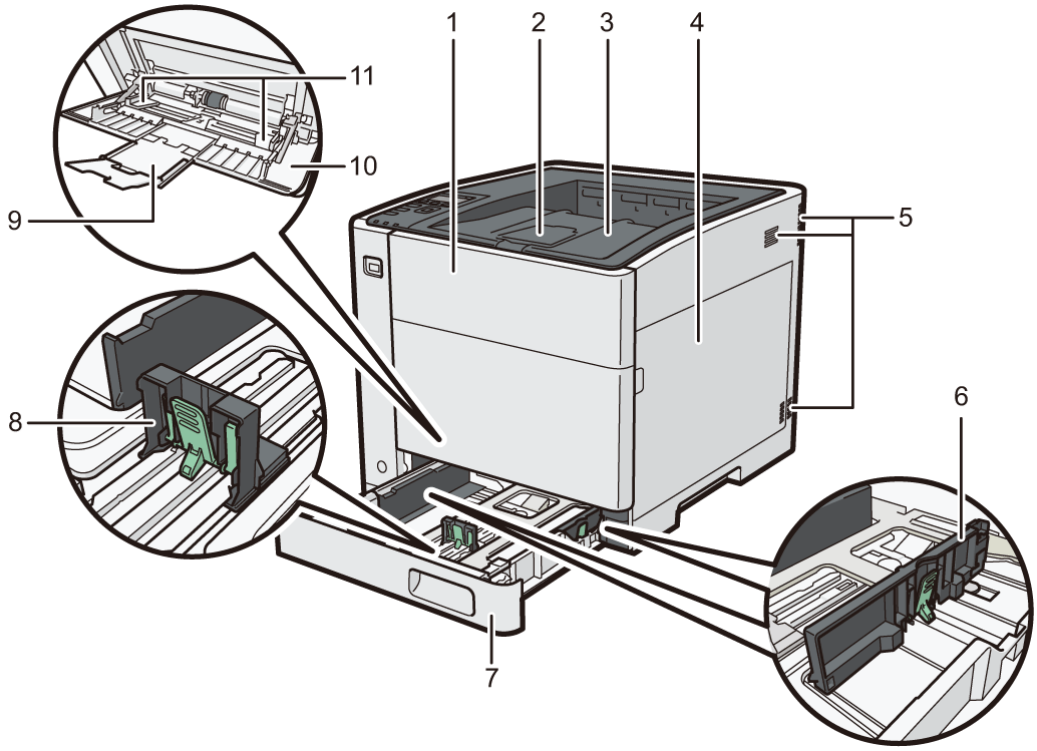
   After large-volume printing, the ventilation fan may continue to work to lower the temperature inside the machine.

5. **Power switch**

   To turn the power on and off, press the power switch.

   page 6 "Turning On and Off the Power"

Front and Right View



1. **Front cover**Open this cover when replacing the print cartridge.
2. **Paper stopper**

   Raise this stopper to prevent paper to fall from the tray when you print a large number of sheets at one time.

3. **Internal tray**

   The machine ejects the output paper onto this tray.

4. **Right cover/Waste toner bottle**

   Collects the excess toner produced in the print process.

page 50 "Replacing the Waste Toner Bottle"

5. **Vents**

   Prevent overheating.

   After large-volume printing, the ventilation fan may continue to work to lower the temperature inside the machine.

6. **Side fences**

   Slide them until they are aligned with each edge of paper when you place the paper on the tray.

7. **Paper tray (Tray 1)**

   Standard paper trays. Load paper here.

   page 18 "Loading Paper into the Paper Tray"

8. **End fence**

   Slide the it until it is aligned with bottom edge of paper when you place the paper on the tray.

9. **Bypass tray extension guide**

   Pull this out when loading paper on the bypass tray.

10. **Bypass cover/Bypass tray**

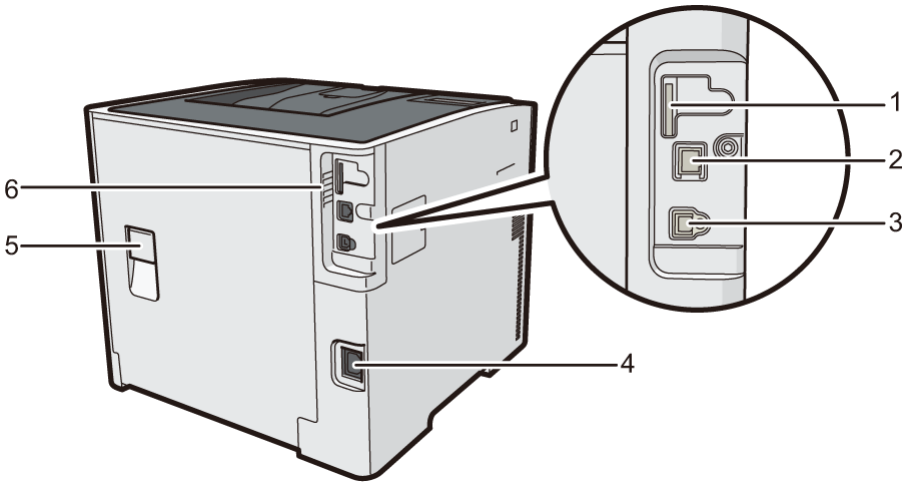
    Use to print on adhesive labels or paper that cannot be loaded in the paper trays.

    page 23 "Loading Paper into the Bypass Tray"

11. **Paper guides**

    When loading paper in the bypass tray, align the paper guides flush against the paper.

Rear View



1. **Slot for the Expansion SD Card**

   Insert the expansion SD card into this slot.

2. **Ethernet interface**

   Used the port to connect the machine to the network or to use the remote management service (@Remote) over the Internet.

3. **USB2.0 interface Type B**

   Use the port to connect the machine and the computer with the USB cable.

4. **Power socket**

   Plug the machine end of the power cable into this socket.

5. **Rear cover open lever**

   The rear cover opens when you pull this lever.

6. **Vents**

   Prevent overheating.

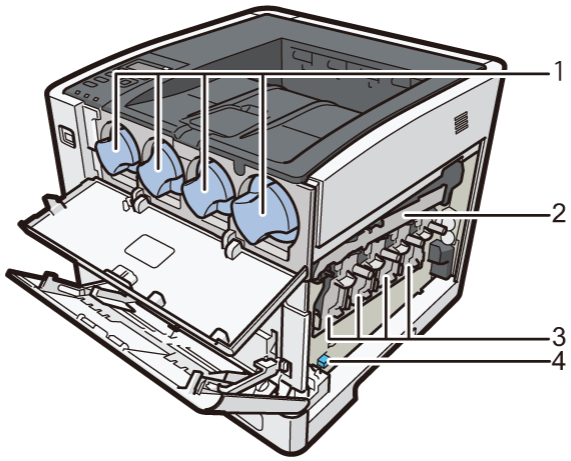
   After large-volume printing, the ventilation fan may continue to work to lower the temperature inside the machine.

Note

- Region A (mainly Europe)

  When touching the machine, you may experience a static shock which is harmless to humans. For details, refer to the following : https://www.ricoh-europe.com/support/environmental-health-safety-product-information/ricoh-static-shock

Interior: Front View



1. **Print cartridge**

   Set the print cartridge in the machine, in the order of yellow (Y), magenta (M), cyan (C), and black (K) from left to right. Messages appear on the screen when print cartridges need to be replaced, or new ones need to be prepared.

   page 47 "Replacing the Print Cartridge"

2. **Transfer unit (Intermediate transfer unit)**

   Transfers the image that is rendered on the transfer unit onto the paper. A message appears on the screen when you need to replace the transfer unit or to prepare a replacement for the unit.

   page 56 "Replacing the Transfer Unit"

3. **Drum unit**

   From the front to back, set the drum units in the following order: yellow (Y), magenta (M), cyan (C), and black (K). A message appears on the screen when the drum Unit needs to be replaced, or a replacement for the unit needs to be prepared.

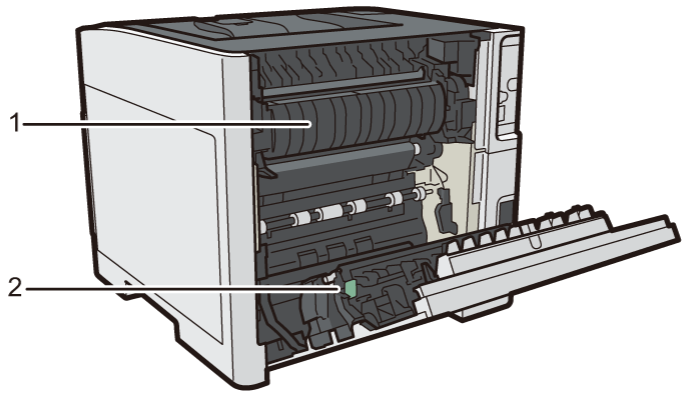
   page 53 "Replacing the Drum Unit"

4. **Cleaning rod**

   Remove it from the machine when you clean the dustproof glass.

   See Cleaning the Dustproof Glass, User Guide in English.

Interior: Rear View



1. **Fusing unit**

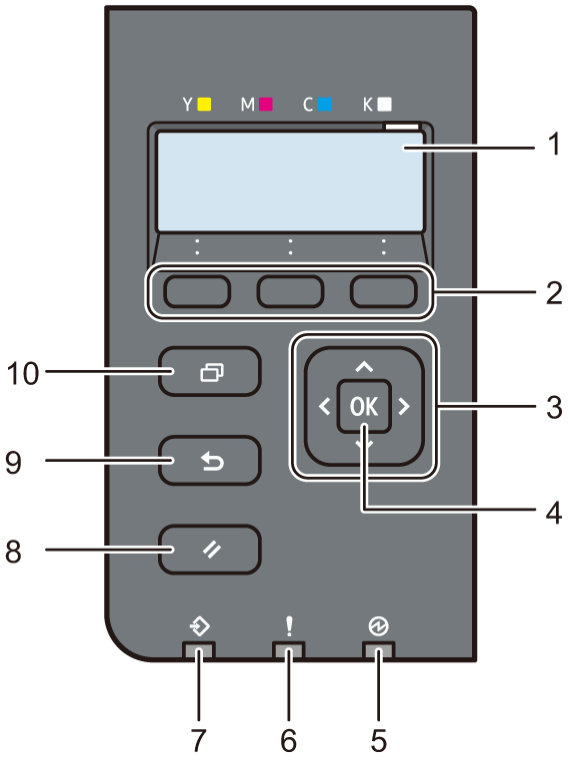
   Fixes the toner on the paper. You may need to handle the unit to check the location of, or resolve a problem when a paper jam occurs.

2. **Transfer unit (Transfer roller)**

   A message appears on the screen when the Transfer unit needs to be replaced, or a replacement for the unit needs to be prepared.

   page 56 "Replacing the Transfer Unit"

Names and Functions of the Control Panel



1. **Display**

   Displays current printer status and error messages.

   Entering energy saver mode turns off the back light.

   page 7 "Energy Saving Mode"

2. **Selection keys**

   Correspond to the function items at the bottom line on the display.

   page 16 "How to Use the Selection Keys"

3. **Scroll keys**

   Press these keys to move the cursor in each direction.

   When the [▲] [▼] [◀] [▶] keys appear in this manual, press the applicable key for the direction that you want to move the cursor.

4. **[OK] key**

   Use this key to confirm settings or setting values, or move to the next menu level.

5. **Power indicator**

   Lights up when the printer is ready to receive data from a computer. Flashes when the printer is warming up or receiving data. It is unlit when the power is off or when the printer is in energy saver mode.

6. **Alert indicator**

   Lights up or flashes when a printer error occurs.

Steady red: printing is not possible, or is possible but print quality cannot be ensured.

Flashing yellow: the printer will soon require maintenance or a replacement consumable such as print cartridge.

Follow the instructions that appear on the display.

7. **Data in indicator**

   Flashes when the printer is receiving data from a computer. The data in indicator is lit if here is data to be printed.

8. **[Job Reset] key**

   Press to cancel the current print job.

9. **[Escape] key**

   Press this key to cancel an operation or return to the previous display.

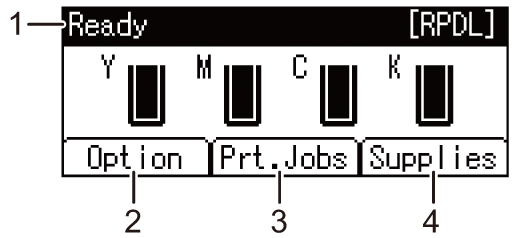
10. **[Menu] key**

    Press this key to configure and check the current printer settings.

    Press to change the default settings to meet your requirements.

    See Settings Items, User Guide in English.

Names and Functions of the Operation Screen



1. **Operational Status or Messages**

   Displays the printer status and messages.

2. **[Option]**

   Press the selection keys on the left to display the following menu items.

   - Print from Memory Device
   - Form Feed
   - Error Log

3. **[Prt.Jobs]**

   Press the selection key in the center to display the [Print Jobs] menu. You can view or print a Sample Print, Locked Print, Hold Print, and Saved Print documents.

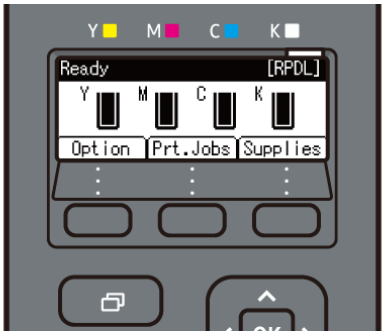
4. **[Supplies]**

   Press to display the information about printer supplies.

Note

- By default, the remaining amount of toner is displayed. To avoid displaying the remaining amount of toner, set [Display Supply Info] to [Off] in [General Settings] under [Maintenance].

How to Use the Selection Keys



To select an item on the bottom line of the display, press the corresponding selection key directly below the item. For example, if you want to select [Option], as shown in the illustration above, press the selection key on the left side.

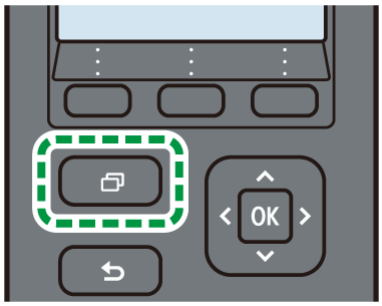
User Authentication

Logging In from the Control Panel

When the machine is configured by the administrator to restrict use by unauthorized users, you must authenticate your login information before starting the operation.

Enter the user name and password to log in.

1. **Press the [Menu] key.**



2. **Press the selection key beneath [Enter].**
3. **Press the [▲], [▼], [◀] or [▶] key to select the user name, and then press the [OK] key to enter it.**
4. **Press the selection key beneath [Accept].**
5. **Press the selection key beneath [Enter].**
6. **Press the [▲], [▼], [◀] or [▶] key to select a password, and then press the [OK] key to enter it.**
7. **Press the selection key beneath [Accept].**

Note

- If the item you want to select is not displayed on the screen, press the [▲] or [▼] key on the control panel to change the screen.
- To log out from the machine, press the [Menu] key, press the selection key beneath [Logout], and then press the selection key beneath [Yes].
- If an incorrect password is entered a specified number of times, login with the same name is disabled (Lockout Function). The default setting for unsuccessful attempts before a user is locked out is five. If the user is locked out, the administrator must release the lockout.

  page 106 "Specifying the Policy on Login/Logout"

Loading Paper

1

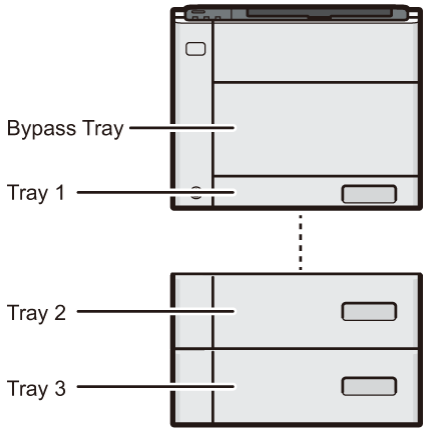
Loading Paper into the Paper Tray

The method of loading paper varies for each tray type.

⚠CAUTION

- When replacing paper or removing jammed paper, make sure not to trap or injure your fingers.

- If the lower paper tray is installed, do not pull out more than one tray at a time. Pressing down forcefully on the machine's upper surface might cause the machine topple over, possibly resulting in injury.



- Before loading paper into a tray, check the paper size and type that can be loaded in the tray.

  page 139 "Recommended Paper Sizes and Types"

- To load thin paper, thick paper, or other special paper, specify the paper type or thickness in [Paper Input].

  See Paper Input, User Guide in English.

  page 26 "Specifying Paper Type and Thickness Settings"

- Check the paper setting before printing. If the paper differs from the paper setting, a mismatch error will occur when you print.
- Straighten curled or warped paper before loading.
- Load a new stack of paper only after the paper in the tray runs out. Adding paper to the existing stack may cause double feeds or paper jams.
- If a paper tray is pushed vigorously when putting it back into place, the position of the tray's side fences may slip out of place.

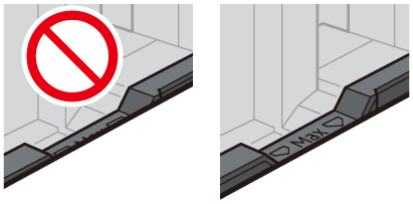
- When loading a low number of sheets, be sure not to squeeze the side fences in too tightly. If the side fences are squeezed too tightly against the paper, the edges may crease, thin paper may wrinkle, or the paper may misfeed.
- You may hear the sound of rubbing paper. This is not a malfunction.
- Do not stack paper over the limit mark.

Loading Paper into Tray 1 to 3

Adjust the side and end fences according to the paper size.

Important

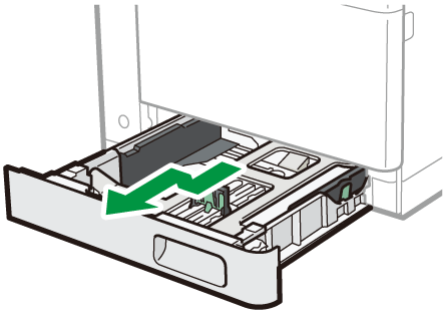
- **If loaded paper exceeds the upper limit mark of the side fence, images may be printed at an angle or paper jams may occur.**



Load paper into every tray in the same way. In the following example procedure, Tray 1 is used.

1. **Check that paper in the paper tray is not being used.**
2. **Pull out the paper tray carefully until it stops, and then pull the tray completely out of the machine while slightly raising the front end of the tray.**

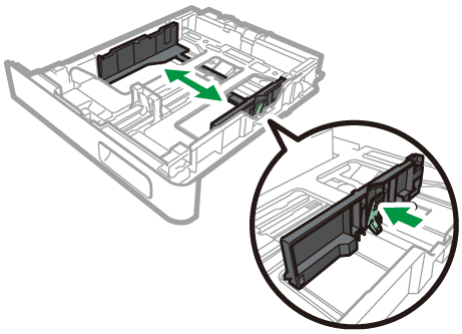
   Place the tray on a flat surface.



3. **Remove paper if loaded.**
4. **While pressing the release lever of the side fence, slide the side fences outward.**

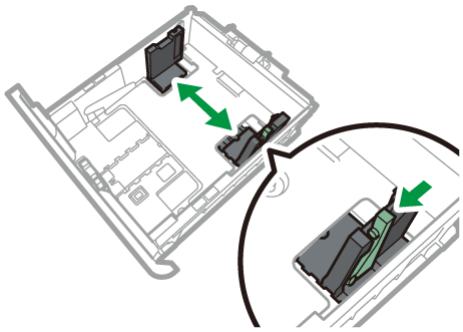
   Tray 1

   Expand them wider than the width of the paper you are loading.



Tray 2

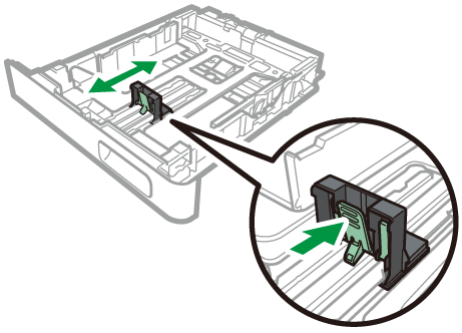
Fit to the size of the paper you are loading.



5. **While pressing the release lever of the end fence, slide the end fence outward.**

Tray 1

Expand them wider than the width of the paper you are loading.

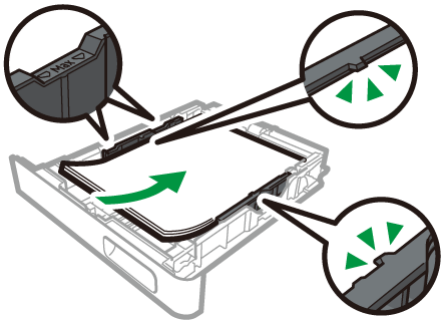


Tray 2

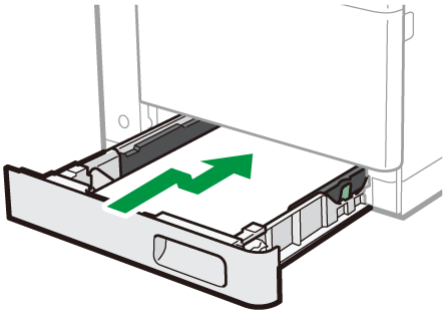
Fit to the size of the paper you are loading.

6. **Square the paper and load it with the print side facing up.**
   - Fan sheets before loading so that multiple sheets of paper do not stick to each other and are not fed at once.
   - When loading paper, align the leading edge of the paper with the back of the tray so that there is no gap between them.
   - Make sure the paper is not stacked higher than the upper limit marked inside the tray.

- Make sure the paper is not stacked higher than the projection on the side fences.



7. **For Tray 1, press and hold the release lever and fit the side fences and the end fence to the size of the paper.**
8. **Make sure that there is no gap between the paper and the side fences or the end fence.**
   - If there is a gap between the paper and the side fences or the end fence is pressing tightly against the paper, paper jams may occur. In this case, adjust the position of the fences.
   - Do not move the paper too much inside the paper tray. The paper may become caught in the gap between the bottom plate and the paper tray, and it may cause a paper jam or folding paper.
9. **While raising the front end of the tray slightly, carefully slide the tray back into the machine until it stops.**



Push the tray straight in. If the paper tray is damaged, it may cause a paper jam. Also, if you push the tray forcibly, the side fence of the tray may be moved.

To avoid paper jams, make sure the tray is securely inserted.

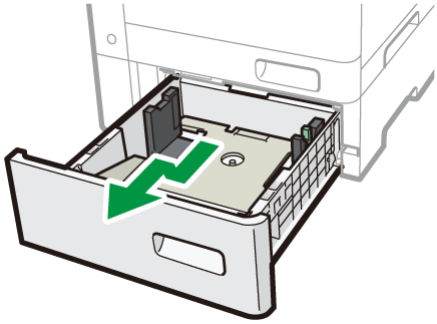
Extending tray to load paper (Tray 2, 3 only)

You can load paper that is longer than A4 (297 mm, 11.7 inches) when the optional extension unit is attached.

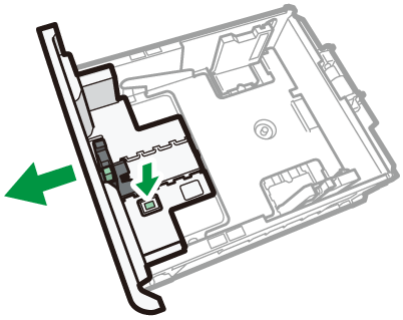
This section explains how to load paper longer than A4 into the machine.

1. **Pull out the paper tray carefully until it stops, and then pull the tray completely out of the machine while slightly raising the front end of the tray.**

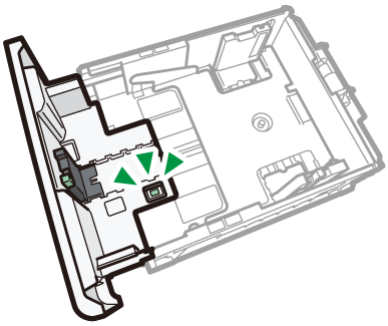
   Place the tray on a flat surface.



2. **While pushing on the green lock on the edge of the bottom plate, pull out the front part of the paper tray.**

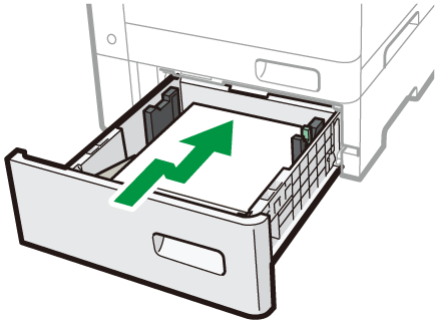


   Pull it out until it is locked in place, and you hear a click.

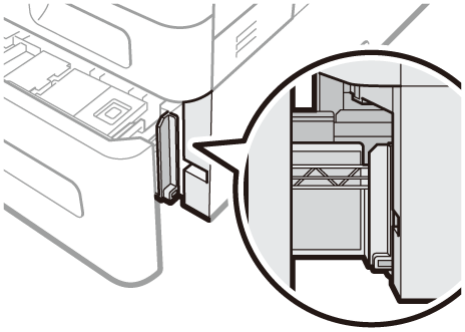


3. **Follow Steps 3 to 7 in page 19 "Loading Paper into Tray 1 to 3".**
4. **While raising the front end of the tray slightly, carefully slide the tray back into the machine until it stops.**

   Push the tray straight in. If the paper tray is damaged, it may cause a paper jam. Also, if you push the tray forcibly, the side fence of the tray may be moved.



The tray protrudes from the exterior of the machine when you extend it, so push in the part of the tray that is indicated in the illustration until it is aligned with the front of the expansion tray.



To avoid paper jams, make sure the tray is securely inserted.

Loading Paper into the Bypass Tray

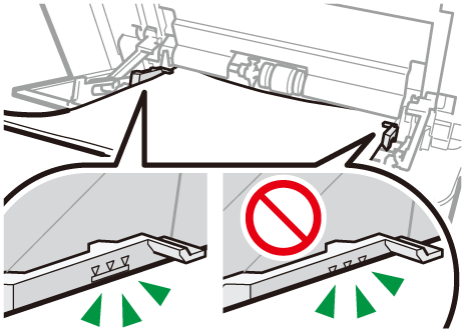
Use the bypass tray to load paper of a size that cannot be loaded into Tray 1 to 3, such as label paper (adhesive labels).

The maximum number of sheets you can load at the same time depends on paper type.

page 139 "Recommended Paper Sizes and Types"

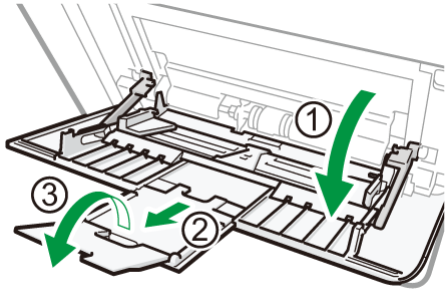
Important

- **Do not stack paper over the limit mark. If you load paper over the limit mark, the print image may be slanted or the paper may be jammed.**



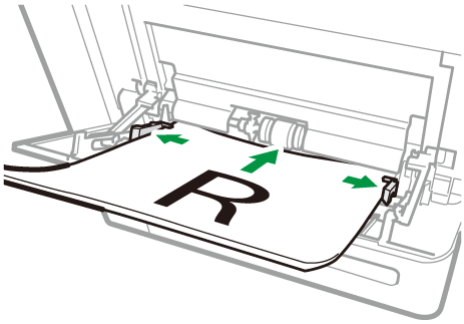
- **You can load up to five sheets of Thick Paper 2.**

1. **Open the bypass tray.**



Make sure that the bypass tray is fully opened.

2. **Spread out the paper guide, and insert paper with the print side facing up until it stops.**



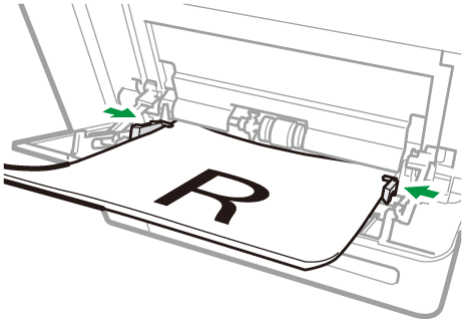
Fan sheets before loading so that multiple sheets of paper do not stick to each other and are not fed at once.

When loading envelopes or letterhead paper, confirm the orientation, face and back, or location of flaps.

page 144 "Envelope Orientation and Recommended Status"

page 145 "Loading Orientation-fixed Paper or Two-sided Paper"

3. **Align the paper guides to the paper size.**

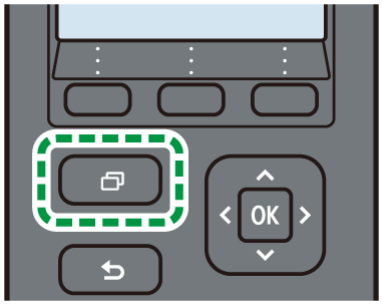


Note

- To load paper on the bypass tray, it is better to orient it in the direction of .

Specifying the Paper Size

1. **Press the [Menu] key.**



2. **Select [Paper Input], and then press the [OK] key.**
3. **Select [Paper Size: (tray name)], and then press the [OK] key.**
4. **Select the size of the paper set in the specified tray, and then press the [OK] key.**

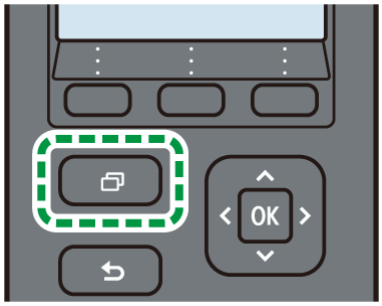
Note

- If the item you want to select is not displayed on the screen, press the [▲] or [▼] key on the control panel to change the screen.

  page 139 "Recommended Paper Sizes and Types"

Specifying a Custom Size Paper Using the Control Panel

1. **Press the [Menu] key.**



2. **Select [Paper Input], and then press the [OK] key.**
3. **Select [Paper Size: (tray name)], and then press the [OK] key.**
4. **Select [Custom Size], and then press the [OK] key.**
5. **Enter the horizontal value, and then press the [OK] key.**
6. **Enter the vertical value, and then press the [OK] key.**

Note

- If the item you want to select is not displayed on the screen, press the [▲] or [▼] key on the control panel to change the screen.

  page 139 "Recommended Paper Sizes and Types"

Specifying Paper Type and Thickness Settings

If the print settings and the loaded paper that are used for a print job do not match, a mismatch error occurs.

Check and specify the paper settings before you start printing.

Important

- **Before you change the settings, confirm the priority of the paper settings for printing (priority to the printer driver or to the control panel).**
- **[Print Settings] ▶ [Machine Modes] ▶ [Tray Setting Priority]**

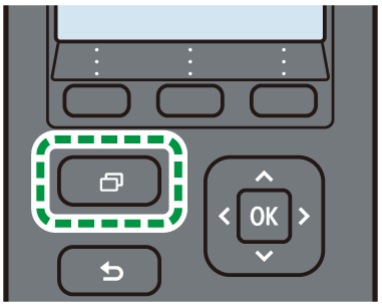
On the printer driver

Check the settings of paper tray and paper type on the printer driver and make sure the settings match the loaded paper.

On the control panel

Specify the types of paper you loaded on the machine. You can print your data with more appropriately.

1. **Press the [Menu] key.**



2. **Press [Paper Input], and press the [OK] key.**
3. **Select [Paper Type: (tray name)], and press the [OK] key.**
4. **Select the type of paper you loaded on the tray, and press the [OK] key.**

   When you specified any of the following paper type, the configuration procedure is now completed.

- Plain Paper 1 or 2, Thin Paper, Medium Paper, Thick Paper 1 or 2, Special Paper 1, 2, or 3

  When you specified any other paper type, proceed to the next step.

5. **Select [Recycled Paper Setting], [Color Paper Setting], [Letterhead Setting], [Label Paper Setting], [Envelope Setting], or [Coated Paper Setting], and press the [OK] key.**
6. **When you select [Recycled Paper Setting], [Color Paper Setting], [Letterhead Setting], or [Coated Paper Setting], specify the tray to configure, and press the [OK] key.**
7. **Select the paper thickness, and press the [OK] key.**

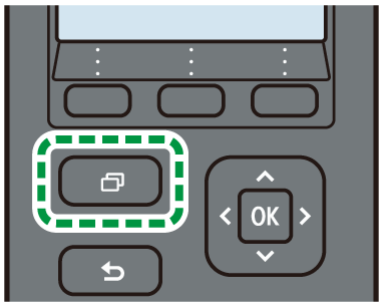
Note

- If the item you want to select is not displayed on the screen, press the [▲] or [▼] key on the control panel to change the screen.

  page 139 "Recommended Paper Sizes and Types"

Configuring Envelope Settings Using the Control Panel

1. **Press the [Menu] key.**



2. **Select [Paper Input] and press the [OK] key.**
3. **Select [Paper Size: Bypass Tray] or [Paper Size: Tray 1], and press the [OK] key.**
4. **Select the envelope size and press the [OK] key.**
5. **Select [Paper Type: Bypass Tray] or [Paper Type: Tray 1], and press the [OK] key.**
6. **Select [Envelope] and press the [OK] key.**
7. **Select [Envelope Setting] and press the [OK] key.**
8. **Select the paper thickness and press the [OK] key.**

Note

- If the item you want to select is not displayed on the screen, press the [▲] or [▼] key on the control panel to change the screen.

  page 139 "Recommended Paper Sizes and Types"
- For details about how to load envelopes, see page 144 "Envelope Orientation and Recommended Status".
- Before you print your document, specify the paper settings correctly on both the control panel and in the printer driver. For details about the settings to specify in the printer driver, see page 41 "Printing on Envelopes".

Operating or Configuring the Machine from Computer (Web Image Monitor)

Web Image Monitor is a tool that can check the machine status and configure machine settings from your computer.

If the machine and your computer are ready to connect to the network, you can access Web Image Monitor just by entering the IP address or host name of the machine in the address bar of your web browser.

The settings that can be set by using the control panel can also be set by using the Web Image Monitor, except for some functions.

For example, you can also view the list of stored documents from your computer. As mentioned above, it is recommended that you use Web Image Monitor if you want to operate the machine from your own desk.

Useful functions available by using Web Image Monitor

To check the help of Web Image Monitor, see to the procedure below.

page 32 "Specifying Web Image Monitor Help"

Function summary	Procedure and reference
Displaying list/history of print jobs, and canceling print jobs You can check the printing status and print history of the machine from your computer. Also, you can cancel stored print jobs in batches from your computer.	• Job list Displayed by going to [Status/Information] in Web Image Monitor ▶ [Job] ▶ [Job List] ▶ [Current/Waiting Jobs]. • Job history Displayed by going to [Status/Information] in Web Image Monitor ▶ [Job] ▶ [Job List] ▶ [Job History]. • Canceling job Displayed by going to [Status/Information] in Web Image Monitor ▶ [Job] ▶ [Job List] ▶ [Current/Waiting Jobs].
Managing output quantity You can check and reset the total counter and counters per user from your computer.	See [Status/Information] in Web Image Monitor help ▶ [Counter per User] for details.

Function summary	Procedure and reference
Synchronize with time server You can synchronize with a time server when you want to adjust the clock in the machine.	See [Device Management] in Web Image Monitor help ▶ [Configuration] ▶ [Device Settings] ▶ [Date/Time] ▶ [SNTP Server Name] for details.
Setting the time to enter sleep mode You can configure the time settings for the "Sleep mode" function that automatically turns the display of the control panel off if there is no operation within a specified period of time.	See [Device Management] in Web Image Monitor help ▶ [Configuration] ▶ [Device Settings] ▶ [Timer] ▶ [Sleep Mode Timer] for details.
Setting auto email notification You can configure the machine to send emails to notify you about the machine's status, such as when paper has run out or a paper jam has occurred. This is useful when managing multiple printers.	See Machine Status Notification by E-mail, User Guide in English.
Configuring/changing security/network settings You can configure/change the IP address that can access the machine and configure the settings of the DNS server, and so on.	• Security settings page 110 "Access Control" • Network settings See Configuring Network Settings from a Computer Using Web Image Monitor, User Guide in English.

Recommended Web Browser

Windows	macOS
Firefox 52 or later	Safari 3.0 or later
Google Chrome version 50 or later	Firefox 52 or later
Microsoft Edge 79 or later	Google Chrome version 50 or later

- You can use the screen reader software JAWS 2018.0 or later on Windows 10 and JAWS 2021 or later on Windows 11.

What You Can Do on the Web Image Monitor

Items displayed on the Web Image Monitor and settings depend whether the machine is logged in.

- When not logged in

The machine status, settings, and job status are displayed. You can browse the settings of the machine but cannot change them.

- When logged in (as a user)

  Log in as a user registered in the Address Book. The users can operate the jobs that they executed and change a part of settings of the machine.

- When logged in (as an Administrator)

  The administrator can change all settings of the machine.

What you can do

Function	Not logged in	User	Administrator
Machine status	✓	✓	✓
Machine settings	✓*1	✓*1	✓
Machine setting change	-	✓*1	✓
Job list	✓	✓	✓
Job history	✓	✓	✓
Access to Address Book	-	✓	✓
Network settings	-	✓*1	✓
Network settings change	-	✓*1	✓
Cancel printing	-	-	✓
Security settings	-	-	✓

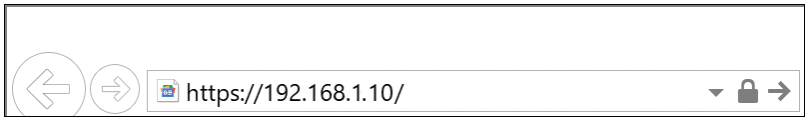
✓: Available -: Not available

*1 Depending on the Administrator settings

Accessing to Web Image Monitor

1. **Enter the IP address of the machine in the address bar of the Web browser.**

   You can check the IP address of the machine in by accessing [Details] in [Network Property].



   Example: when the IP address of the machine is "192.168.1.10"

   - If SSL is specified

     https://192.168.1.10/

- If SSL is not specified

  http://192.168.1.10/

When you do not know whether SSL is specified on the machine, enter the address starting with https. When you fail the connection, enter the address starting with http.

When entering the IPv4 address, do not enter "0" for each segment. If "192.168.001.010" is entered, you cannot access the machine.

2. **Confirming the machine status or settings on the top page of Web Image Monitor.**

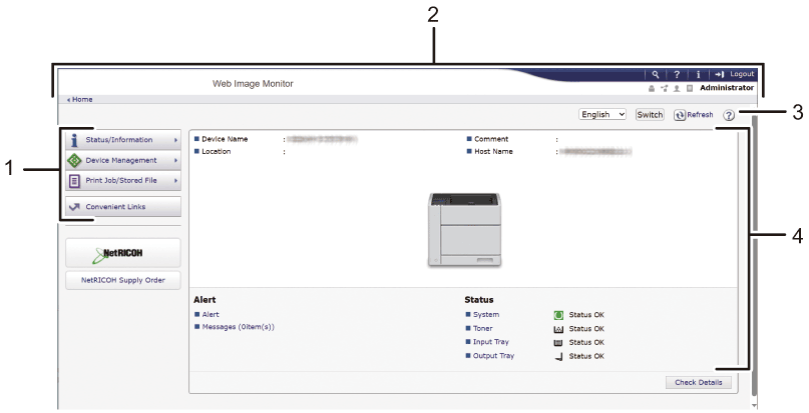


The machine status and remaining amount of consumables are displayed.

You can access Web Image Monitor more quickly by registering the machine's URL as a bookmark. Note that the URL you register must be the URL of the top page, which is the page that appears before login. If you register the URL of a page that appears after login, Web Image Monitor will not open properly from the bookmark.

To change the settings, click [Login] at the top right on the screen and enter the User Name and Password.

Web Image Monitor Screen



1. **Menu**

Menu items described below are displayed.

- Status/Information: Displays the machine status, option configuration, counter, and job status.

- Device Management: Manages the machine settings and Address Book.
- Print Job/Stored File: Operates the files stored in the printer driver.
- Convenient Links: Displays the link to the Favorite URL.

2. **Header**

   An icon to link to the Login screen is placed at the top right on the screen. The Help, Version Information, and Keyword Search buttons are also displayed.

3. **Refresh/Help**

   (Refresh): Update the information in the work area.

   (Help): View or download Help file contents.

4. **Main Area**

   The machine status and settings are displayed.

Specifying Web Image Monitor Help

Web Image Monitor has Help to describe the function of setting items. When you use Help for the first time, you can select to read online Help or to download Help File.

View Online Help Now

You can view the latest Web Image Monitor Help on the Internet.

Download Help File

You can download Web Image Monitor Help to the computer and view it. When you store the downloaded Help file in the Web server and assign to the Help button ( ), you can view the Help without connecting to the Internet.

To assign the downloaded Help file to the Help button ( ), specify the path to the Help file following the procedure below.

1. **Log in to Web Image Monitor as a network administrator.**
2. **Click [Configuration] on the [Device Management] menu on Web Image Monitor.**



3. **Click [Webpage] under the "Webpage" category.**
4. **In "Download Help File", select the operating system and displayed language, and then click [Download].**
5. **Unzip the downloaded zip file and store it in the Web server.**
6. **Enter the path to the Help file stored in the Web server in "URL" under "Set Help URL Target".**

   For example, when URL of the Help File is "http://a.b.c.d/HELP/JA/index.html", enter "http://a.b.c.d/HELP/".
7. **Click [OK].**
8. **After completing the procedure, log out and finish Web Image Monitor.**

2. Printer

Basic Printing

Basic Procedure for Printing Documents

Specify the printer driver and configure the Document Size, Paper Type, and other settings to print a document.

Important

- **Duplex printing is selected as the default setting. If you want to print on only one side, select [Off] for the two-sided printing setting.**
- **If you send a print job via USB 2.0 while the machine is in Sleep mode, an error message may appear after the print job is completed. In this case, check whether the document was printed.**
- **If you set [On] for [Prohibit Printing PS/PDF], you cannot print a data that is PS/PDF format.**

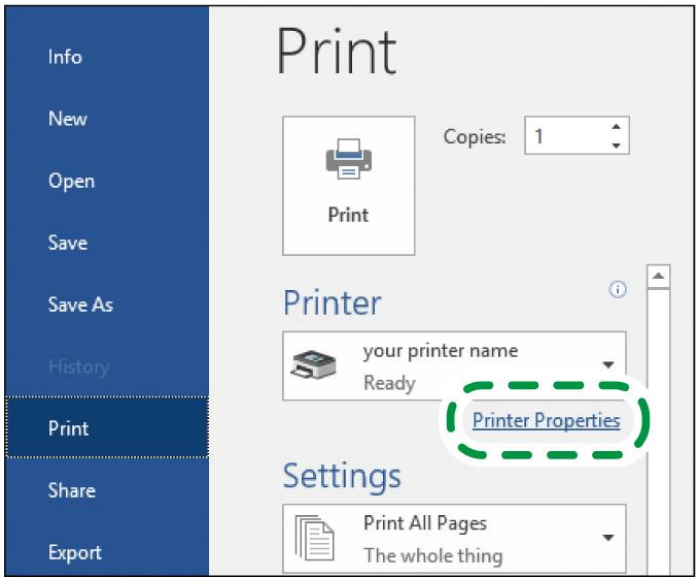
  See Maintenance, User Guide in English.

Printing a Document in Windows

1. **Open a document to print on the computer, and display the setting screen of the printer driver from the print menu in the application.**

   The procedure to display a document varies depending on the applications.

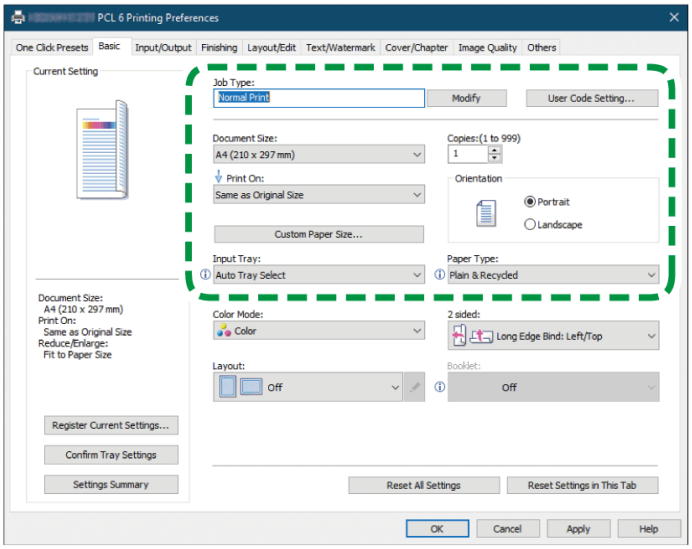
   For example in Microsoft Word/Excel, click [Print] on the [File] menu, select the device to use, and then click [Printer Properties].



DZC420

2. **Specify the Document Size, Paper Type, Input Tray, and other settings.**

   You can configure the basic settings just by using the [Basic] tab.



- Job Type: Select [Normal Print] to execute printing immediately.

  You can make a partial print as a test and proceed to print the rest of the document (Sample Print).

  See Making a Partial Print as a Test and Printing the Rest of the Document, User Guide in English.

  You can store documents in the machine (Locked Print, Hold Print, or Stored Print).

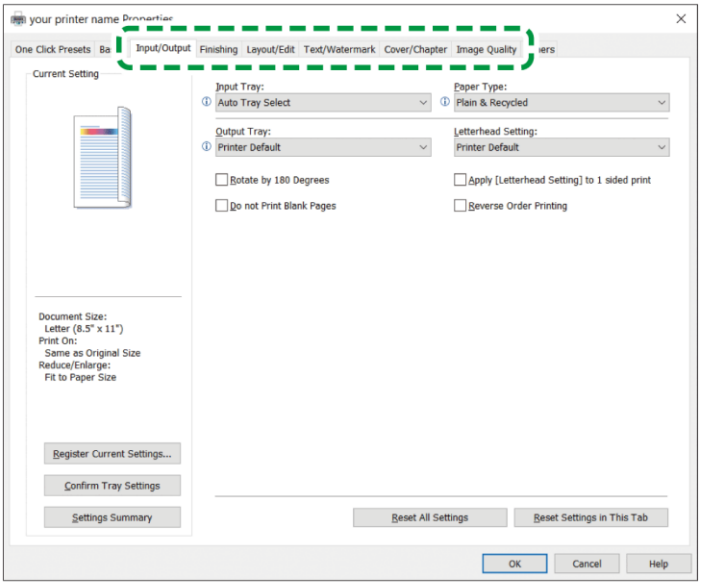
  See Storing Documents to Print in the Machine, User Guide in English.
- Document Size: Select the size of the document to print.
- Print On: Select the size of the paper to print on.
- Copies: Enter the print quantity.
- Orientation: Specify the orientation of the document. Select Portrait or Landscape.
- Input Tray: Select the tray loaded with the paper to use. When you select [Auto Tray Select], a suitable paper tray is selected automatically according to the specified [Print On] and [Paper Type].
  - If you do not want to use particular trays when [Auto Tray Select] is specified, set the machine so it does not automatically select those trays.
  - To prevent the machine from selecting other trays automatically, disable auto tray switching.

    See Paper Input, User Guide in English.
- Paper Type: Select the type of paper to use.
- Color Mode: Black and White: Select the print color.

  You can print in universal color by using the following settings:

- [Image Quality] tab ▶ [Barrier-free Color Management:] ▶ [On]

You can configure some advanced settings using the [Input/Output] to [Image Quality] tabs.



D0DXDA5608

The caution icon (ⓘ) indicates that there are disabled items. Click the icon to check the cause.

To set each function in details, click the detail settings button ( ).

3. **After completing the configuration, click [OK] to print.**

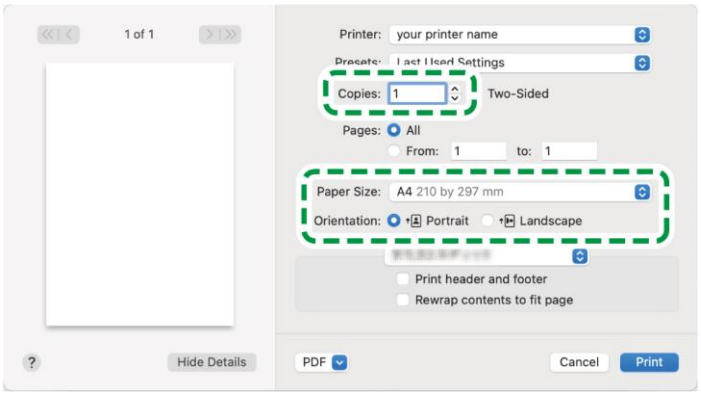
Note

- On the [Devices and Printers] screen, right-click the printer icon of the machine, and then click [Printing preferences] to change the default values of the printer settings.
- When you use the driver distributed from the print server, [Standard settings] specified in the print server are displayed as the default.

Printing a Document in macOS

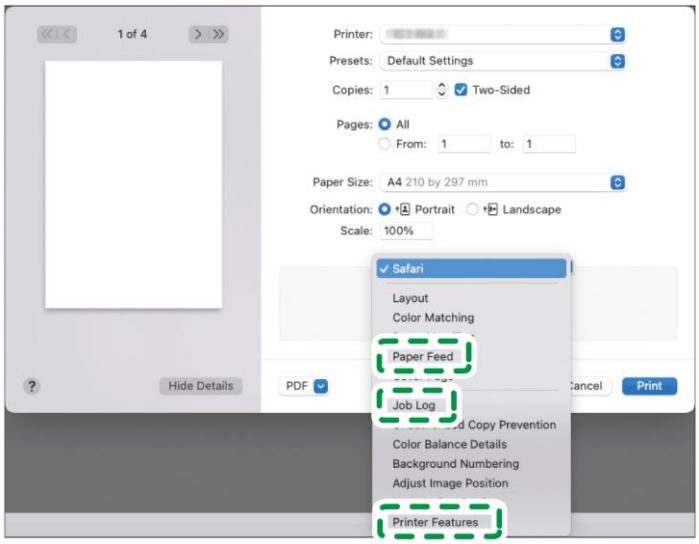
In the following example procedure, macOS 12 is used. The procedure may vary for different versions.

1. **Open a document to print on the computer, and click [Print] on the [File] menu.**
2. **Select the printer you use from [Printer:].**
3. **Specify Paper Size, Orientation, and other settings.**



- Copies: Enter the print quantity.
- Paper Size: Select the size of the document to print.
- Orientation: Specify the orientation of the document. Select [Portrait] or [Landscape].

4. **Select a category from the pop-up menu, and then specify the paper tray and paper type.**



Paper Feed

- All Pages From: Select the tray loaded with the paper to use. When you select [Auto Select], a suitable paper tray is selected automatically according to the specified paper size and paper type.

  When the paper of the specified size is not loaded on the machine, printing is performed following the settings of the machine.

Job Log

- Job Type: Select [Normal Print] to execute printing immediately.

You can make a partial print as a test and proceed to print the rest of the document (Sample Print).

See Making a Partial Print as a Test and Printing the Rest of the Document, User Guide in English.

You can store documents in the machine (Locked Print, Hold Print, or Stored Print).

See Storing Documents to Print in the Machine, User Guide in English.

Printer Features

Select a category in "Feature Sets", and then specify the setting items.

- Basic
  - Color Mode: Select the print color.
- Paper
  - Paper Type: Select the type of paper to use.

5. **After completing the configuration, click [Print] to print.**

Printing on Both Sides of Paper

Specify 2-sided Print in the printer driver.

Specifying 2-sided Print (Windows)

Specify 2-sided Print on the [Basic] tab.

1. **Open a document to print on the computer, and display the setting screen of the printer driver from the print menu in the application.**
2. **Specify document size, paper type, orientation and others.**

   page 35 "Basic Procedure for Printing Documents"
3. **In [2 sided:] on the [Basic] tab, specify the binding side of and way to open the paper.**

   Orientation of the original and opening type

Orientation	Open to left	Open to top
Portrait 		
Landscape 		

4. **After completing the configuration, click [OK] to print.**

Specifying 2-sided Print (macOS)

Specify 2-sided Print on the [Layout] menu.

1. **Open a document to print on the computer, and display the setting screen of the printer driver from the print menu in the application.**
2. **Specify Paper Size, Orientation, Paper Type, and other settings.**

   page 35 "Basic Procedure for Printing Documents"
3. **Select the [Two-Sided] check box, and then select [Layout] to specify the binding side and opening type of the paper.**

   Orientation of the original and opening type

Long edge	Short edge
	

4. **After completing the configuration, click [Print] to print.**

Combining and Printing Multiple Pages on a Single Sheet of Paper

You can print multiple pages on a single sheet at a reduced size (Combine 2 Originals).

For example, you can reduce an original of A4 size to A5 size and print two pages on an A4 sheet. You can use the 2 Sided Print and Combine 2 Originals functions at the same time to economize on paper.

You can print up to 16 pages on a single sheet and specify the order to arrange the pages on the sheet.



Specifying the Combine 2 Originals Function (Windows)

Specify the Combine 2 Originals function on the [Basic] tab.

1. **Open a document to print on the computer, and display the setting screen of the printer driver from the print menu in the application.**
2. **Specify document size, paper type, orientation, and other settings.**

   page 35 "Basic Procedure for Printing Documents"
3. **In [Layout:] on the [Basic] tab, specify the number of pages to combine.**

   Click the detail settings button of [Layout] to do the following settings:
   - Page Order: Select the order of the pages.
   - Draw Frame Border: Select the check box to draw a line between pages.
4. **After completing the configuration, click [OK] to print.**

When printing from an application that supports the same function as the machine, do not set the function in the application. If the setting in the application is enabled, the print result may not be as intended.

Specifying the Combine 2 Originals Function (macOS)

Specify the Combine 2 Originals function on the [Layout] menu.

1. **Open a document to print on the computer, and display the setting screen of the printer driver from the print menu in the application.**
2. **Specify paper size, orientation, paper type, and other settings.**

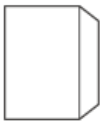
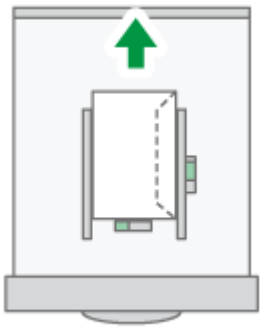
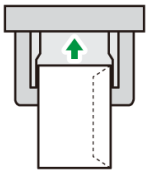
   page 35 "Basic Procedure for Printing Documents"
3. **Select [Layout], and then specify the number of pages to combine and the order of the pages.**

   Configure the following settings:
   - Pages per Sheet: Select the number of pages to combine.
   - Layout Direction: Select the order of the pages.
   - Border: Select a type of border line to draw between the pages.
4. **After completing the configuration, click [Print] to print.**

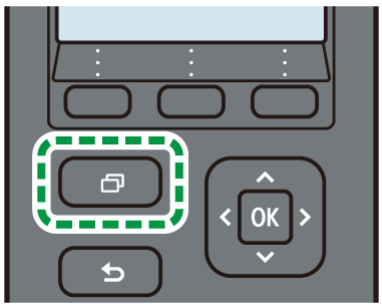
Printing on Envelopes

Load envelopes in the bypass tray or paper tray and change the tray paper settings on the control panel.

1. **Load an envelope in the bypass tray or the paper tray.**

Orientation of Envelopes	Tray 1	Bypass Tray
Side-opening envelopes 	 Flap: close Bottom side of the envelope: left Printing surface: upper side	 Flap: close Bottom side of the envelope: left Printing surface: upper side

2. **Press the [Menu] key.**



3. **Select [Paper Input], and then press the [OK] key.**
4. **Select [Paper Size: (tray name)], and then press the [OK] key.**

   Select the name of the tray in which the envelopes are loaded.
5. **Select the envelope size, and then press the [OK] key.**

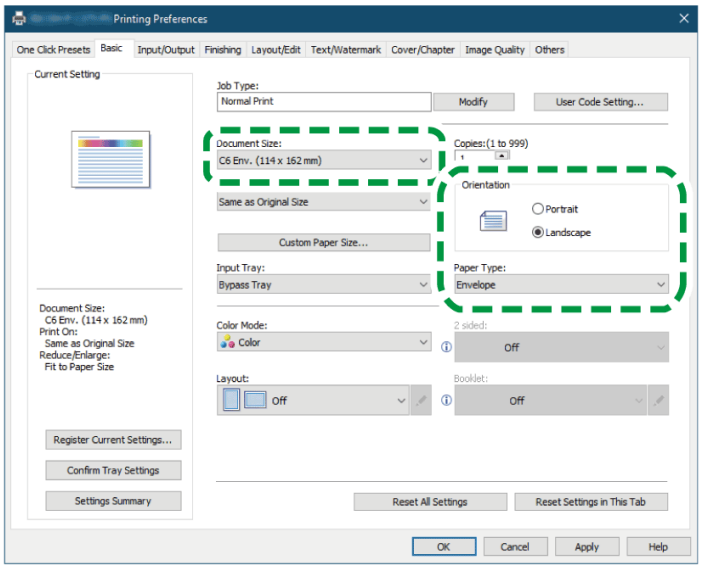
   If the size of the loaded envelope is not included in the list, select [Custom Size] and specify the size using the [▲] or [▼] key.
6. **Select [Paper Type: (tray name)], and then press the [OK] key.**

   Select the name of the tray in which the envelopes are loaded.
7. **Select [Envelope], and then press the [OK] key.**
8. **Select [Envelope Setting], and then press the [OK] key.**
9. **Select [Tray 1] or [Bypass Tray] , and then press the [OK] key.**

   Select the tray in which the envelopes are loaded.

10. **Select the envelope thickness from [Thick Paper 1] or [Thick Paper 2], and then press the [OK] key.**
11. **Open a document to print in the computer, and display the setting screen of the printer driver from the print menu application.**
12. **Specify the paper size, orientation, and paper type.**

Windows

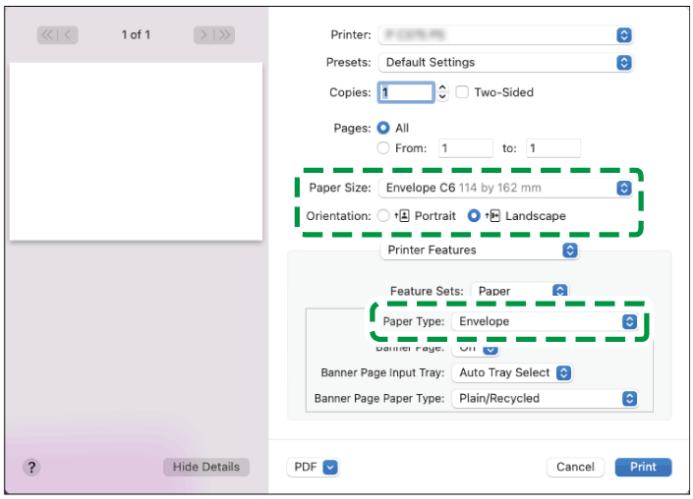


- Document Size: Select the envelope size. If the envelope size is not included among the options, enter the value in [Custom Paper Size...].
- Orientation: [Landscape]
- Paper Type: [Envelope]

You can specify a custom paper size, which is commonly used as the option of the Document Sizes.

See Printing on Custom-sized Paper Loaded on the Bypass Tray, User Guide in English.

macOS



- Paper Size: Select the envelope size. If the envelope size is not included among the options, select [Manage Custom Sizes] and enter the value.
- Orientation: [Landscape]
- Paper Type: [Envelope]

13. **Execute printing.**

Printing from a Storage Media

Printing from a USB Flash Memory Device Directly

You can connect a memory storage device to the media slot of the machine and print the files stored on it. Use this to print external data easily.

⚠CAUTION

- Keep USB flash memory devices out of reach of children. If a child accidentally swallows a USB flash memory device, consult a doctor immediately.

Note

- USB flash memory device is supported for direct printing. However, certain types of USB flash memory device cannot be used.
- The machine cannot print a document over 1 GB.
- You can select up to 999 files within 1 GB total.
- If the print job of PDF file is canceled, execute printing from a PDF viewer such as Acrobat Reader while using the printer driver.
- If the PDF file includes the fonts that are not supported by the machine, garbled characters may be printed. You can check the supported fonts by printing [PCL Config./Font Page], [PS Config./Font Page], or [PDF Config./Font Page] in [List/Test Print].

  See List/Test Print, User Guide in English.

Printable File Formats

File format	Details
JPEG files	Exif version 1.0 or later
TIFF files	Uncompressed TIFF files TIFF files compressed using the MH, MR, or MMR method
PDF files	PDF version 1.7 (Acrobat 8.0 compatible) or earlier*1

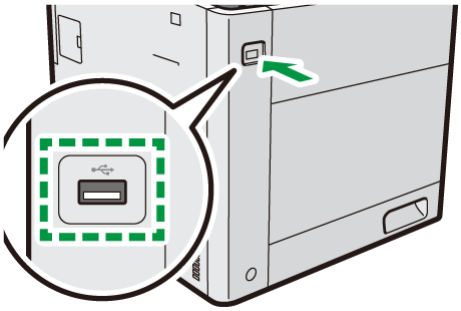
*1 The machine does not support the following functions: Crypt Filter, DeviceN Color Space (more than eight components), watermark note, optional contents (version 1.6), AcroForm

Note

- The PDF file of a custom size may not be printed.

Printing from a USB Flash Memory Device

1. **Insert a USB flash memory device in the media slot on the front side of the machine.**



2. **Press the selection key beneath [Option].**



3. **Select [Print from Memory Device], and then press the [OK] key.**
4. **Select the file to print, and then press the selection key beneath [Print].**

   Press the selection key beneath [Print Settings] to change the print settings such as the number of copies, paper tray, and color.

3. Maintenance

Replacement and Replenishment of Consumables

Replacing the Print Cartridge

When replacing the print cartridge, refer to the replacement procedure described on the box of the new print cartridge.

You can see the procedure in the video.

http://support.ricoh.com/services/device/video/M0FB/toner/ww/index.html?utm_source=Ricoh&utm_medium=manual&utm_campaign=M0FB

Important

- **If you continue to use the print cartridge set in the machine at the time of purchase after the message prompting you to replace it appears, the machine may stop working.**
- **When you replace the print cartridge, replace it with a replacement print cartridge.**
- **Once you remove the print cartridge set in the machine at the time of purchase and replace it with a replacement print cartridge, you will not be able to use it again.**
- **Replace the print cartridge after the message prompting replacement is displayed on the control panel.**
- **The machine may become damaged if you use print cartridge of a different type.**
- **Do not turn off the power of the machine when replacing the print cartridge. If you turn off the power when replenishing the print cartridge, the specified settings are canceled, and printing will not resume afterwards.**
- **After removing the print cartridge from the machine, do not shake it while its opening is facing downward. The remaining toner may spill out.**
- **After removing the print cartridge, do not touch the interior of the machine.**
- **Do not pull out and put back the print cartridge repeatedly. The remaining toner may leak.**

Note

- If is displayed even though there remains sufficient toner, pull out the print cartridge by following the toner replacement procedure displayed on the screen, and then re-insert the toner.

Precautions When Storing Toner

⚠WARNING

- Do not store toner (new or used) or toner containers while toner is inside in a place with an open flame. The toner can ignite and result in burns or fire.

⚠CAUTION

- Do not leave the following items in a place where children can reach them:
  - Toner (new or used)
  - Toner containers while toner is inside
  - Toner-attached parts

Important

- **Store the print cartridge in a dry environment away from direct sunlight and generally under the temperature below 35°C(95°F).**
- **Keep the print cartridge horizontal when storing it.**

Precautions When Replacing the Toner

⚠WARNING

- Do not dispose of the following items into a fire. Toner will ignite on contact with naked flame and burns can result.
  - Toner (new or used)
  - Toner containers while toner is inside
  - Toner-attached parts

- Do not absorb spilled toner (including used toner) using a vacuum cleaner. Absorbed toner may cause ignition or explosion due to electric contact sparks inside the vacuum cleaner. However, you can use a toner-compatible industrial vacuum cleaner. When toner is spilled, remove the spilled toner using a wet cloth so that the toner is not scattered.

⚠CAUTION

- When the following occurs while toner is handled, receive emergency measures first, and then consult a doctor if necessary.
  - When inhaling toner, gargle with a large amount of water and move into a fresh air environment.
  - When swallowing toner, dilute gastric contents with a large amount of water.
  - When getting toner into your eyes, flush them with a large amount of water.

- When removing jammed paper, replenishing or replacing toner (new or used), make sure not to inhale toner.

- When removing jammed paper, replenishing or replacing toner (new or used), be careful not to have toner dirt your skin or clothes.

- If toner (new or used) comes into contact with your skin or clothes and smears them, take the following actions:
  - If toner comes into contact with your skin, wash the affected area thoroughly with soap and water.
  - If toner comes into contact with your clothes, wash the stained area with cold water. Heating the stained area by applying hot water will set the toner into the fabric and removing the stain may become impossible.

- When replacing a container with toner (including used toner) or consumables with toner, be careful that the toner does not splatter. After removing used consumables and shutting the lid of the container if the lid is available, put them in a bag.

- Do not open toner containers forcibly while toner is inside, crush or squeeze them. Toner spillage can cause accidental ingestion or dirtying of clothes, hands, or floor.

Disposing Exhausted Toners

You cannot reuse exhausted toners.

When disposing a depleted print cartridge, place the cartridge in a box or plastic bag while paying attention not to spill any toner powder.

Region A (mainly Europe and Asia)/ Region B (Taiwan)

If you want to discard your used toner container, please contact your local sales office. If you discard it by yourself, treat it as general plastic waste material.

Region B (mainly North America)

Please see our local company website for information on the recycling of supply products, or you can recycle items according to the requirements of your local municipalities or private recyclers.

Replacing the Waste Toner Bottle

Read the replacement instruction provided with the new consumable thoroughly before you replace a consumable.

The current waste toner bottle is approaching the end of its service life when the following message appears on the machine's control panel. Prepare a new waste toner bottle for replacement.

"Waste Toner almost full"

Replace the waste toner bottle when the following message appears on the machine's control panel.

"Waste Toner Bottle full."

You can see the procedure in the video.

http://support.ricoh.com/services/device/video/M0FB/wtoner/ww/index.html?utm_source=Ricoh&utm_medium=manual&utm_campaign=M0FB

Important

- **For safe and correct use, please be sure to read Safety Information before replacing the machine's supplies.**
- **You cannot reuse the waste toner bottle.**
- **Before removing the waste toner bottle, place a sheet of paper such as the enclosed replacement instructions on the floor to the right of the machine to prevent your workplace from getting dirty with the removed waste toner bottle.**

Precautions When Replacing the Waste Toner Bottle

⚠WARNING

- Do not store toner (new or used) or toner containers while toner is inside in a place with an open flame. The toner can ignite and result in burns or fire.

- Do not dispose of the following items into a fire. Toner will ignite on contact with naked flame and burns can result.
  - Toner (new or used)
  - Toner containers while toner is inside
  - Toner-attached parts

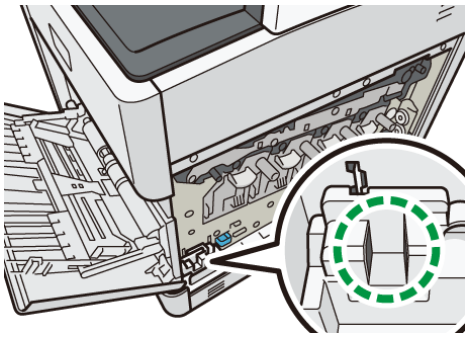
- Do not absorb spilled toner (including used toner) using a vacuum cleaner. Absorbed toner may cause ignition or explosion due to electric contact sparks inside the vacuum cleaner. However, you can use a toner-compatible industrial vacuum cleaner. When toner is spilled, remove the spilled toner using a wet cloth so that the toner is not scattered.

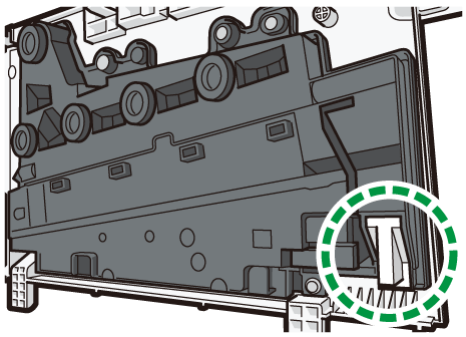
- The following explains the warning messages on the plastic bag used in this product's packaging:
  - Do not leave the polythene materials (bags, etc.) supplied with this machine close to babies and small children. Suffocation can result if polythene materials are brought into contact with the mouth or nose.

⚠CAUTION

- Do not leave the following items in a place where children can reach them:
  - Toner (new or used)
  - Toner containers while toner is inside
  - Toner-attached parts

- Some of the internal components of this machine are fragile. Do not touch the sensors shown below when removing the waste toner bottle. Doing so may cause malfunctions.





- When the following occurs while toner is handled, receive emergency measures first, and then consult a doctor if necessary.
  - When inhaling toner, gargle with a large amount of water and move into a fresh air environment.
  - When swallowing toner, dilute gastric contents with a large amount of water.
  - When getting toner into your eyes, flush them with a large amount of water.

- When removing jammed paper, replenishing or replacing toner (new or used), make sure not to inhale toner.

- When removing jammed paper, replenishing or replacing toner (new or used), be careful not to have toner dirt your skin or clothes.

- If toner (new or used) comes into contact with your skin or clothes and smears them, take the following actions:
  - If toner comes into contact with your skin, wash the affected area thoroughly with soap and water.
  - If toner comes into contact with your clothes, wash the stained area with cold water. Heating the stained area by applying hot water will set the toner into the fabric and removing the stain may become impossible.

- When replacing a container with toner (including used toner) or consumables with toner, be careful that the toner does not splatter. After removing used consumables and shutting the lid of the container if the lid is available, put them in a bag.

- Do not open toner containers forcibly while toner is inside, crush or squeeze them. Toner spillage can cause accidental ingestion or dirtying of clothes, hands, or floor.

Disposing the Used Waste Toner Bottle

When disposing the used waste toner bottle, place the bottle in a box or plastic bag while paying attention not to spill any toner powder.

Region A (mainly Europe and Asia)/ Region B (Taiwan)

If you want to discard your used waste toner bottle, please contact your local sales office. If you discard it by yourself, treat it as general plastic waste material.

Region B (mainly North America)

Please see our local company website for information on the recycling of supply products, or you can recycle items according to the requirements of your local municipalities or private recyclers.

Replacing the Drum Unit

Read the replacement instruction provided with the new consumable thoroughly before you replace a consumable.

The current drum unit is approaching the end of its service life when the following message appears on the machine's control panel. Prepare a new drum unit for replacement.

- "Rplct Rqrd Soon:K Drum Unit"
- "Rplct Rqrd Soon:C Drum Unit"
- "Rplct Rqrd Soon:M Drum Unit"
- "Rplct Rqrd Soon:Y Drum Unit"

Replace the drum unit when the following message appears on the machine's control panel.

- "Replace Black Drum Unit"
- "Replace Cyan Drum Unit"
- "Replace Magenta Drum Unit"
- "Replace Yellow Drum Unit"

You can see the procedure in the video.

http://support.ricoh.com/services/device/video/M0FB/pcdu/ww/index.html?utm_source=Ricoh&utm_medium=manual&utm_campaign=M0FB

Important

- **When you replace the drum unit, replace it with a replacement drum unit.**
- **Once you remove the drum unit set in the machine at the time of purchase and replace it with a replacement drum unit, you will not be able to use it again.**
- **The performance of the drum unit may deteriorate if you expose the unit to light for an extended period of time. Replace the unit quickly.**
- **The drum unit (green cylinder) is fragile and easily scratched. Handle the unit carefully.**
- **Do not leave the machine unattended with the drum unit removed.**
- **Before removing the waste toner bottle, place the included plastic sheet on the floor to the right of the machine to prevent your workplace from getting dirty with the removed waste toner bottle.**

Precautions When Replacing the Drum Unit

⚠WARNING

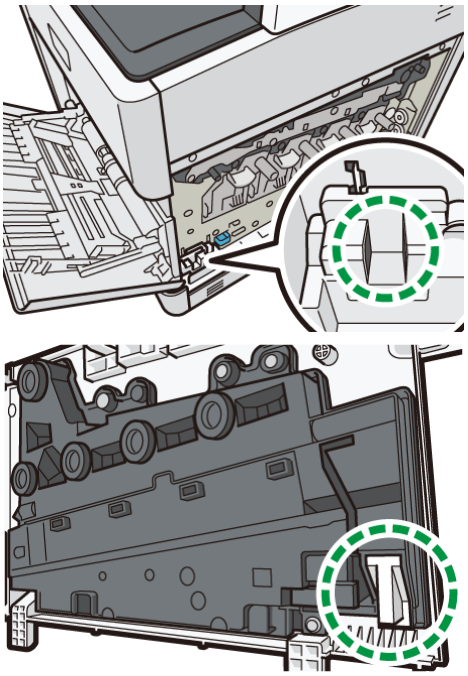
- Do not dispose of the following items into a fire. Toner will ignite on contact with naked flame and burns can result.
  - Toner (new or used)
  - Toner containers while toner is inside
  - Toner-attached parts

- Do not absorb spilled toner (including used toner) using a vacuum cleaner. Absorbed toner may cause ignition or explosion due to electric contact sparks inside the vacuum cleaner. However, you can use a toner-compatible industrial vacuum cleaner. When toner is spilled, remove the spilled toner using a wet cloth so that the toner is not scattered.

- The following explains the warning messages on the plastic bag used in this product's packaging:
  - Do not leave the polythene materials (bags, etc.) supplied with this machine close to babies and small children. Suffocation can result if polythene materials are brought into contact with the mouth or nose.

⚠CAUTION

- Some of the internal components of this machine are fragile. Do not touch the sensors shown below when removing the right cover (waste toner bottle). Doing so may cause malfunctions.



- When the following occurs while toner is handled, receive emergency measures first, and then consult a doctor if necessary.
  - When inhaling toner, gargle with a large amount of water and move into a fresh air environment.
  - When swallowing toner, dilute gastric contents with a large amount of water.
  - When getting toner into your eyes, flush them with a large amount of water.

- When removing jammed paper, replenishing or replacing toner (new or used), make sure not to inhale toner.

- When removing jammed paper, replenishing or replacing toner (new or used), be careful not to have toner dirt your skin or clothes.

- If toner (new or used) comes into contact with your skin or clothes and smears them, take the following actions:
  - If toner comes into contact with your skin, wash the affected area thoroughly with soap and water.
  - If toner comes into contact with your clothes, wash the stained area with cold water. Heating the stained area by applying hot water will set the toner into the fabric and removing the stain may become impossible.

- When replacing a container with toner (including used toner) or consumables with toner, be careful that the toner does not splatter. After removing used consumables and shutting the lid of the container if the lid is available, put them in a bag.

- Do not open toner containers forcibly while toner is inside, crush or squeeze them. Toner spillage can cause accidental ingestion or dirtying of clothes, hands, or floor.

Disposing the Used drum unit

When disposing the used drum unit, place the drum unit in a box or plastic bag while paying attention not to spill any toner powder.

Region A (mainly Europe and Asia)/Region B (Taiwan)

If you want to discard your used drum unit, please contact your local sales office. If you discard it by yourself, treat it as general plastic waste material.

Region B (mainly North America)

Please see our local company website for information on the recycling of supply products, or you can recycle items according to the requirements of your local municipalities or private recyclers.

Replacing the Transfer Unit

Read the replacement instruction provided with the new consumable thoroughly before you replace a consumable.

The current transfer unit is approaching the end of its service life when the following message appears on the machine's control panel. Prepare a new transfer unit for replacement.

"Replace Transfer Unit soon."

Replace the transfer unit when the following message appears on the machine's control panel.

"Replace Transfer Unit."

You can see the procedure in the video.

http://support.ricoh.com/services/device/video/M0FB/tu/ww/index.html?utm_source=Ricoh&utm_medium=manual&utm_campaign=M0FB

Important

- **The performance of the drum unit may deteriorate if you expose the unit to light for an extended period of time. Replace the unit quickly.**
- **The drum unit (green cylinder) is fragile and easily scratched. Handle the unit carefully.**
- **Do not leave the machine unattended with the drum unit removed.**
- **Before removing the waste toner bottle, place a sheet of paper on the floor to the right of the machine.**
- **When you finish replacing the transfer roller, reset the counter on the operation panel.**

  [Menu] ▶ [Maintenance] ▶ [Quality Maintenance] ▶ [Clear TransferUnit Counter]

Precautions When Replacing the Transfer Unit

⚠WARNING

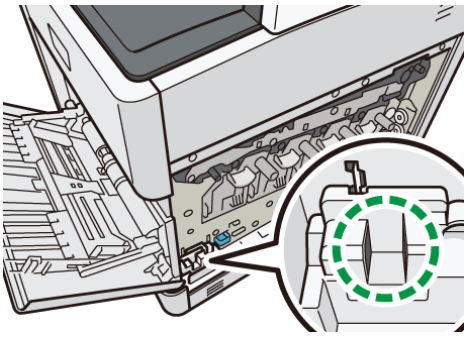
- Do not dispose of the following items into a fire. Toner will ignite on contact with naked flame and burns can result.
  - Toner (new or used)
  - Toner containers while toner is inside
  - Toner-attached parts

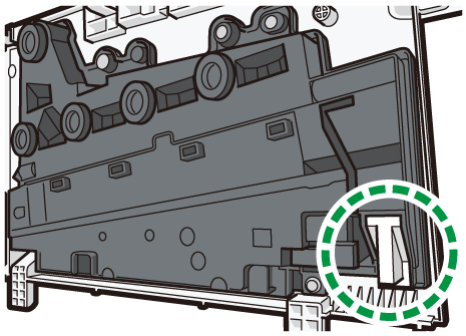
- Do not absorb spilled toner (including used toner) using a vacuum cleaner. Absorbed toner may cause ignition or explosion due to electric contact sparks inside the vacuum cleaner. However, you can use a toner-compatible industrial vacuum cleaner. When toner is spilled, remove the spilled toner using a wet cloth so that the toner is not scattered.

- The following explains the warning messages on the plastic bag used in this product's packaging:
  - Do not leave the polythene materials (bags, etc.) supplied with this machine close to babies and small children. Suffocation can result if polythene materials are brought into contact with the mouth or nose.

⚠CAUTION

- Some of the internal components of this machine are fragile. Do not touch the sensors shown below when removing the right cover (waste toner bottle). Doing so may cause malfunctions.





- When the following occurs while toner is handled, receive emergency measures first, and then consult a doctor if necessary.
  - When inhaling toner, gargle with a large amount of water and move into a fresh air environment.
  - When swallowing toner, dilute gastric contents with a large amount of water.
  - When getting toner into your eyes, flush them with a large amount of water.

- When removing jammed paper, replenishing or replacing toner (new or used), make sure not to inhale toner.

- When removing jammed paper, replenishing or replacing toner (new or used), be careful not to have toner dirt your skin or clothes.

- If toner (new or used) comes into contact with your skin or clothes and smears them, take the following actions:
  - If toner comes into contact with your skin, wash the affected area thoroughly with soap and water.
  - If toner comes into contact with your clothes, wash the stained area with cold water. Heating the stained area by applying hot water will set the toner into the fabric and removing the stain may become impossible.

- When replacing a container with toner (including used toner) or consumables with toner, be careful that the toner does not splatter. After removing used consumables and shutting the lid of the container if the lid is available, put them in a bag.

- Do not open toner containers forcibly while toner is inside, crush or squeeze them. Toner spillage can cause accidental ingestion or dirtying of clothes, hands, or floor.

Replacing the Fusing Unit

If the Alert indicator on the control panel lights up and the "Replacmnt Rqrd:Fusing Unit" message appears on the display, contact your sales or service representative.

4. Troubleshooting

Getting Started

Alert Sounds

The machine notifies you with an alert sound when a paper jam occurs or another problem occurs. Listen to the alert sound for one of the patterns described below, and perform the required procedure accordingly.

Beep pattern	Condition	Solution
A short beep	Touch/Notification	-
A short beep, followed by long beep	Invalid Operation	If you entered an incorrect password, enter the correct password.
Five short beeps (repeating five times)	Warning	Check the message displayed on the screen, and resolve the problem by removing the jammed paper or replacing the toner.

Note

- You cannot pause an alert sound that has started. The machine continues to emit the sound until the preset sound pattern is completed.
- Specify whether or not to emit the sound in [Maintenance] ▶ [General Settings] ▶ [Panel Key Sound].

Checking the Indicators, Icons, and Messages on the Control Panel

The machine notifies you of the machine condition with a message or the alert indicator. Check the status and resolve the problem accordingly.



- Message

  Displays error and status messages which indicate the status of the machine.

- Alert indicator

  If there is a problem such as a paper jam, the Alert indicator lights up or flashes along with a message displayed on the screen.

When you need to resolve a problem such as a paper jam, an icon is displayed at the beginning of a message. See the table below for the meaning of each icon.

Icon	Condition	Solution and reference
	Maintenance or repair is required.	Prepare for maintenance or consider repairing the machine.
	Paper is jammed.	See the animated illustration displayed on the control panel, and remove the jammed paper. See When Paper Is Jammed, User Guide in English.
	Toner is almost depleted, or has run out.	Prepare a replacement toner. Replace the toner when it runs out. page 47 "Replacing the Print Cartridge" **Note** • If appears when there is a lot of toner, pull out the print cartridge by following the toner replacement procedure that is displayed on the screen, and then set it back again.

Icon	Condition	Solution and reference
	The waste toner bottle is full, or almost full.	Prepare a replacement waste toner bottle. Replace the bottle when it becomes full. page 50 "Replacing the Waste Toner Bottle"

When Messages Appear

Status Messages

Message	Status
"Hex Dump Mode"	In Hex Dump mode, the machine receives data in a hexadecimal format. Turn off the machine after printing, and then turn it on again.
"Offline"	The machine is offline and cannot print.
"Please wait..."	This message may appear for a few seconds. It means the machine is initializing, replenishing toner, or performing maintenance operations. Wait a while.
"Printing..."	The machine is printing. Wait a while.
"Ready"	This is the default ready message. The machine is ready for use. No action is required.
"Resetting Job"	The machine is resetting the print job. Wait a while.
"Service Call"	The machine needs to be fixed. Report the message, SC number, and serial number to your service representative. When "SC491" is displayed, it is possible that dew condensation may have formed inside the machine due to temperature changes. Turn off the machine until condensation is eliminated and the machine has adapted to the environment.
"Setting change..."	The machine is applying the changes made to its settings. Wait a while.
"The internal cooling fan is active. Please wait. It will take about 4 minutes."	The fan in the ventilation slot is running to cool down the internal temperature of the machine after a large document has been printed. A rotation sound is heard while the fan is running. Printing may stop temporarily but it will resume in a while. Please wait.
"Waiting for print data..."	The machine is waiting for the next data to print. Wait a while.

Alert Messages that Appear on the Control Panel

Fusing Unit

Message	Cause	Solution and reference
"Replacmnt Rqrd:Fusing Unit" "Please call service."	You will need to replace the fusing unit soon.	Contact your service representative.
"Set the Fusing Unit correctly."	The fusing unit is not correctly set.	Contact your service representative.

Intermediate Transfer Unit

Message	Cause	Solution and reference
"Replacemnt Requird:IntTrans" "Please call service."	The replacement time for the transfer unit is approaching.	Replace the transfer unit.
"Set the Intermediate Transfer Unit correctly."	The Intermediate Transfer Unit is not installed or not installed properly.	Contact your service representative.

Paper Tray

Message	Cause	Solution and reference
"Change (tray name) to the following settings:"	The size of the paper in the tray does not match the paper size specified in the printer driver.	Select a tray containing paper that is the same size as the specified paper size.
"Duplex mode is in off position for (tray name)"	The duplex mode for the indicated tray is not available.	You can use one-sided printing only. Press [Change] to change the tray's settings, press [JobReset] to reset the job, or press [Form Feed] to force printing.
"Load paper in (tray name)"	There is no paper in the specified tray.	Load the specified paper in the tray, press [JobReset] to reset the job.
"Reset Paper Tray correctly."	The specified tray is not correctly set.	Check that the specified tray is set correctly.

Drum Unit

Message	Cause	Solution and reference
"Replc K Drum Unit:PrtSuspnd" "Replc C Drum Unit:PrtSuspnd" "Replc M Drum Unit:PrtSuspnd" "Replc Y Drum Unit:PrtSuspnd"	It is time to replace the drum unit.	Replace the drum unit of the indicated color.
"Rplct Rqrd Soon:K Drum Unit" "Rplct Rqrd Soon:C Drum Unit" "Rplct Rqrd Soon:M Drum Unit" "Rplct Rqrd Soon:Y Drum Unit"	It is almost time to replace the drum unit.	Prepare the drum unit of the indicated color.

Waste toner bottle

Message	Cause	Solution and reference
"Waste Toner almost full"	The waste toner in the print cartridge is almost full.	Prepare a new print cartridge.
"Waste Toner Full"	The waste toner in the print cartridge is full.	Replace the print cartridge. page 47 "Replacing the Print Cartridge"

Toner

Message	Cause	Solution and reference
"Add toner. Replace Print Cartridge."	The toner has run out.	Replace the print cartridge. page 47 "Replacing the Print Cartridge"
"Independent-supply toner"	Independent-supply toner is set.	Use the toner recommended for this machine.
"Set the Print Cartridge correctly."	The print cartridge may have not been installed correctly.	Turn the machine off, and install the print cartridge again.

Message	Cause	Solution and reference
"Toner is almost empty."	The toner is almost empty.	Prepare a new print cartridge.

Covers

Message	Cause	Solution and reference
"Cover Open. Please close the indicated cover."	A cover of the machine is open.	Close the cover as indicated on the control panel.

System/Others

Message	Cause	Solution and reference
"Cannot connect=>Comm.Serv. Check proxy user/password."	The proxy user name or password is incorrect.	Check the proxy server settings, and then change the user name and/or password if they are incorrect.
"Cannot print."	The machine cannot print the sent data.	Check that the file you want to print is a supported file type. Check the misfeeds and ask your network administrator for help.
"Classification Code Error"	A classification code is not specified for the print job.	Enter a classification code using the printer properties and print the document again.
"Ethernet Board Error"	An error on the Ethernet is detected.	Turn the machine off, and then turn it on again. If the problem persists, consult your sales or service representative.
"Exceeded max. No. of files."	While printing a Sample Print, Locked Print, Hold Print, or Stored Print file, the maximum file capacity was exceeded.	Delete unneeded files stored in the machine.

Message	Cause	Solution and reference
"Exceeded max. No. of pages."	While printing a Sample Print, Locked Print, Hold Print, or Stored Print file, the maximum page capacity was exceeded.	• Delete unneeded files stored in the machine. • Reduce the number of pages to print.
"Exceeded max. print size. Press [FormFeed] or [JobReset]."	The specified paper size exceeds the maximum size supported by this machine.	Press [Form Feed] to force printing or [JobReset] to cancel printing.
"No privileges to use funct."	The logged in user does not have the privileges to register programs or change the paper tray settings.	For details about authentication, contact your user administrator.
"Printer Font Error."	There are problems with the machine's font file.	Turn the machine off, and then turn it on again. If the problem persists, consult your sales or service representative.
"Problem:Wireless card"	The machine cannot detect a wireless LAN interface board.	Check that the wireless LAN interface board installed correctly. If the problem persists, consult your sales or service representative.
"Supply order has failed."	The automatic supply order failed.	The message indicates the machine tried to order the supplies.
"USB has a problem."	The machine has detected a USB board failure.	Turn the machine off, and then turn it on again. If the problem persists, consult your sales or service representative.

Alert Messages that Are Printed on Error Logs and Reports

This section describes likely causes of and possible solutions for the error messages that are printed on the error logs or reports.

Message	Cause	Solution and reference
"84: Error"	There is no work area available for image processing.	This data cannot be printed.
"85: Error"	The specified graphics library is unavailable.	Check that the data is valid.
"86: Error"	Parameters of the control code are invalid.	Check the print settings.
"91: Error"	Printing was canceled by the auto job cancel function due to a command error.	Check that the data is valid.
"92: Error"	Printing was canceled because the [Job Reset] key.	Perform the print operation again as necessary.
"Address book is in use."	The machine currently cannot perform authentication because the Address Book is being used by another function.	Wait a while, and then retry the operation.
"Authen. error, job canceled"	The authentication setting has been changed during printing, and the machine stopped printing due to auto job cancel.	Check the authentication setting.

Message	Cause	Solution and reference
"Auto-user prog. failed."	Automatic registration of information for LDAP Authentication or Windows Authentication failed because the Address Book is full.	Check the address book. page 94 "Specifying User Code Authentication"
"Background Numbering Error"	The background numbering function was specified for an unavailable paper size or for printing on slip sheets.	Check the settings for the background numbering functions on the printer driver. For details about these settings, see the printer driver Help. You cannot print background numbers on slip sheets.
"Banned PS/PDF job canceled."	PostScript or PDF printing is prohibited by the setting.	Set [Prohibit Printing PS/PDF] to [No] in [General Settings] in [Maintenance].
"Classification Code Error"	The classification code is not specified with the printer driver.	Select [Optional] for the classification code. Preventing Printing of a Job Without a Classification Code
"Collate cancelled."	Collate was canceled.	Turn the machine off, and then turn it on again. If the message appears again, consult your service representative.
"Collate: Page max."	The amount of free memory is insufficient to perform collating.	Reduce the number of pages to be printed.
"Comm. error with CM server."	The job is canceled due to a communication error with the Central Management server.	Check the status of the Central Management machine.

Message	Cause	Solution and reference
"Command Error."	Communications with the computer is temporarily unstable.	Consult your network administrator.
"Command of other maker rcvd"	Printing has been performed using a third-party printer driver.	Check the type of the printer driver you are using.
"Compressed Data Error"	The machine detected corrupt compressed data.	Check that the program you used to compress the data is functioning correctly.
"Compulsory Sec. Stamp Error"	An error has occurred during compulsory security printing and printing has stopped.	Lower the resolution of the data you are sending.
"Duplex cancelled."	Duplex printing was canceled.	Change the setting for "Duplex Tray" in [Paper Input] to enable duplex printing for the paper tray.
"Error occured. Prntd/Cncld."	An error occurred during printing, but it was ignored.	Check the print settings.
"Excd Prt Vol Use max count."	Printing was canceled because the print maximum number was reached.	page 94 "Specifying User Code Authentication"
	Maximum number of user codes that can be registered has been reached.	Delete unnecessary user codes.
"File System Error."	PDF direct printing could not be performed because the file system could not be obtained.	Turn the machine off, and then turn it on again. If the message appears again, consult your service representative.

Message	Cause	Solution and reference
"File System Full."	The PDF file cannot be printed because the capacity of the file system is full.	Delete all unnecessary files from the hard disk, or decrease the file size sent to the machine.
"Format or Syntax Error."	A syntax error, etc., occurred.	Check that the PDF file is valid.
"Function use denied."	The print job was cancelled because of one of the following: • The user does not have privileges to print. • No privileges to print are assigned to the entered user name or user code, or a wrong password was specified for the user name.	Enter the user name or user code with privileges to print, or enter the correct password for the user name.
"HDD not installed."	Documents are stored using Sample Print/Locked Print/Hold Print/Stored Print, but the internal storage is not working.	Restart the machine. If the same message continues to be displayed, contact your service representative.

Message	Cause	Solution and reference
"Insufficient Memory."	A memory allocation error occurred.	**PCL 6** Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help. On the printer driver's [Special Settings] tab, click [Image Quality] in "Menu:", and then select [Raster] in the "Vector/Raster:" list. In some cases, it will take a long time to complete a print job. **PCL 5c, PostScript 3** Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help.
"Internal Storage is full."	Overflow has occurred in the internal storage when performing Sample Print, Locked Print, Hold Print, Stored Print, or Registration of overlay data.	• Reduce the size of the document to be printed. • Delete unnecessary data. For the procedure to delete a document, see Deleting Documents Stored in the Machine, User Guide in English.
"Internal Storage is full."	Overflow has occurred in the internal storage area assigned for PostScript forms and fonts.	Delete unnecessary forms and fonts.
"Internal Storage is full."	Overflow has occurred in the internal storage while registering overlay data.	Delete the registered overlay data or reduce the size of the overlay data to be registered.

Message	Cause	Solution and reference
"Internal Storage is n/a."	Background Numbering is specified but the internal storage is not working.	Restart the machine. If the same message continues to be displayed, contact your service representative.
"No response from server."	A timeout occurred while the machine was connecting to the server for LDAP Authentication or Windows Authentication.	Check the status of the server.
"Others using print volume."	The count unit is occupied by the other machines.	Check the status of the client machine.
"Paper Size Error"	Printing was canceled because the specified paper size cannot be fed from the tray.	Check the available paper size.
"Paper Type Error"	The machine does not recognize the paper type specified using the printer driver.	Check that the machine is connected to the network correctly and bidirectional communication is enabled. If the problem persists, check the user paper type settings of the machine.
"Password err., job canceled"	The entered password was incorrect, and the machine stopped printing due to auto job cancel.	Check and enter the correct password set for the document.
"Password mismatch."	A wrong password was entered when an encrypted PDF file was printed.	Check the password. See PDF Menu, User Guide in English.

Message	Cause	Solution and reference
"PCL5e/XL error, job canceld"	An error occurred during PCL printing and the machine stopped printing due to auto job cancel.	Check that the machine is communicating properly with the computer.
"Print overrun."	Printing images was aborted.	Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help.
"PS3/machine settg unmatched"	During PostScript or PDF printing, a mismatch was detected between the print data and the machine configuration, and the machine stopped printing due to auto job cancel.	Make sure that the print settings specified in the print data match the settings in [PS Menu] in [Print Settings].
"PS3/PDF error, job canceled"	During PostScript or PDF printing, a language error occurred and the machine stopped printing due to auto job cancel.	Check the print data.
"PS3/PDF font err, job cncld"	During PostScript or PDF printing, a font error occurred and the machine stopped printing due to auto job cancel.	Register necessary fonts.

Message	Cause	Solution and reference
"PS3/PDF mem err, job cancld"	During PostScript or PDF printing, an error due to insufficient memory occurred and the machine stopped printing due to auto job cancel.	Specify a smaller size.
"PS3/PDF timeout, job cancld"	During PostScript or PDF printing, a timeout error occurred and the machine stopped printing due to auto job cancel.	• Check that the machine is communicating properly with the computer. • PostScript 3 Check the [Job Timeout] setting in [PS Menu] in [Print Settings]. Specify a longer timeout period when the machine settings have priority. When [Driver/Command] is specified, specify a longer timeout period using the command.
"Receiving data failed."	Data reception was aborted.	Resend the data.
"Sending data failed."	The machine received a command to stop a transmission from the printer driver.	Check that the computer is working correctly.
"User auth. already exists."	The same account name is already used in the newly selected domain or server in an environment using LDAP Authentication.	Consult your user administrator.
"Usr ID invalid, job canceld"	The entered user ID was incorrect, and the machine stopped printing due to auto job cancel.	Enter the correct login user name. Contact your user administrator for the login user name.

5. Security

Introduction

Taking Measures to Prevent Security Threats

Appropriate security measures are required to reduce the risk of information leaks and use by unauthorized persons.

The personal information stored in the Address Book and highly confidential files handled by the machine are important information assets. They should be protected from being stolen or abused.

To ensure secure use of the machine, specify the settings of the machine properly according to the specified environments, user level, administrator load, and the company's information security policy.

Administrators refer to special users who have the authority to manage various information and settings of the machine. To use the machine safely, important settings, such as user registration and security settings, must be configured only by administrators. Especially, security settings should be configured before the machine is placed in operation.

The security measures and their settings are described below. Take appropriate measures according to the operation environment of the machine.

: Basic security measures

: Strong security measures taken by the functions of the machine

: Stronger security measures using the options of this machine or external security functions

Defining the administrator of the machine

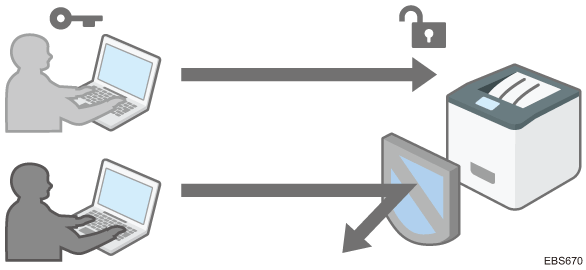


EBS669

Select an administrator who performs the maintenance and management of the machine. The administrator performs the important security settings.

Registering Administrators

Preventing unauthorized access by managing the users who can use the machine or the connected network



1 / 2 / 3 The administrator restricts the users who can use the machine to prevent the unauthorized access by unauthorized persons.

page 92 "Verifying Users to Operate the Machine (User Authentication)"

2 Prevent a brute-force attack on the password or unauthorized operation of the machine caused by user inattentiveness.

- When login is continuously fails due to an incorrect login password, login will be blocked.
- If the machine is not used for a specified period after logging in, the user is forcibly logged out.

  page 106 "Specifying the Policy on Login/Logout"

2 Restrict the range of the IP addresses that are allowed to access the machine to block access to the machine from unauthorized computers. Also, specify the unused protocols to reduce the risk of intrusion.

page 110 "Access Control"

2 / 3 Prevent the leak or falsification of information by encrypting communication.

page 120 "Encrypting Network Communication"

Preventing the leak of information by handling files



2 / 3 Prevent unauthorized copying or printed paper stolen by embedding a pattern on the printed surface or restricting normal printing.

page 130 "Preventing Data Leaks from Printed Sheets"

Prevent the leak of information when the machine is stolen or disposed by encrypting data.

page 132 "Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine"

Restrict the operation in Service Mode used for maintenance and repair by a customer engineer to prevent the leak of information.

page 136 "Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator"

Important

- **To prevent this machine from being stolen or willfully damaged, install it in a secure location.**
- **If the security settings are not configured, the data in the machine may be vulnerable to attack.**
- **To avoid disrupting the work of users, select as administrators who can use the machine proficiently, and then have them supervise the operation of the machine.**
- **Before setting this machine's security features, the administrators must read the descriptions on security completely and thoroughly. Pay particular attention to the section entitled page 78 "Registering Administrators".**
- **The administrators must inform users regarding proper usage of the security functions.**
- **If this machine is connected to a network, its environment must be protected by a firewall or similar security measure.**
- **For protection of data during communication, apply the machine's communication security functions and connect it to devices that support security functions such as encrypted communication.**
- **Administrators should regularly examine the machine's logs to check for irregular and unusual events.**

Checking Firmware Validity

When the machine starts up, this function is used to check that the firmware is valid.

If an error occurs while a verification process is performed, a verification error is displayed on the control panel.

Note that this can also be checked on Web Image Monitor after the machine starts. If an error occurs in a verification process of Web Image Monitor, Web Image Monitor cannot be used. If this is the case, check the control panel.

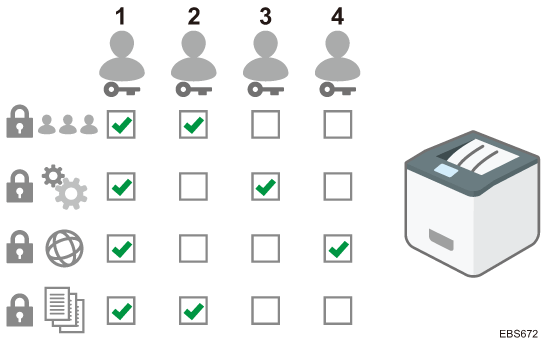
When an error occurs in a verification process, contact your service representative.

Registering Administrators

There are four types of administrator privileges in accordance with the functional categories and they are assigned to Administrator 1 through Administrator 4 (built-in administrators). You can assign all four privileges to one person, or assign a specific privilege to a specific person. When Windows authentication is activated, you can assign administrator privileges to external authentication server accounts as well (external administrators).

Sharing the administrator tasks facilitates each administrator's tasks and at the same time prevents unauthorized operations by administrators.

Types of administrator privileges



- User Management: Manages information registered in the Address Book. You can add users to the Address Book and change the registered information.
- Machine Management: Mainly manages the settings of the devices. You can configure the settings so that the settings for each function can be changed only by the administrator.
- Network Management: Manages the settings for connecting to the network.
- File Management: Manages the permission to access the stored files. You can specify the settings so that only the registered users or permitted users can view or edit the files stored in the machine.

Workflow to register built-in administrators

1. Activate Administrator Authentication.

   Activate the Administrator Authentication function of the machine.

   page 79 "Activating Administrator Authentication"

2. Log in to the machine as an administrator.

   Enter the login user name and login password of a built-in administrator to log in to the machine.

   page 80 "Logging in to the Machine as an Administrator"

3. Add built-in administrators or change the privileges.

   Assign the privileges to each administrator. You can register up to four built-in administrators.

   page 82 "Adding Built-in Administrators or Changing the Privileges"

Workflow to register external administrators

1. Activate Administrator Authentication.

   Activate the Administrator Authentication function of the machine.

   page 79 "Activating Administrator Authentication"

2. Log in to the machine as an administrator.

   Enter the login user name and login password of a built-in administrator to log in to the machine.

   page 80 "Logging in to the Machine as an Administrator"

3. Register external administrator groups and assign the privileges.

   Register external administrator groups and assign administrator privileges.

   page 84 "Registering External Administrator Groups and Assigning the Administrator Privileges"

Note

- The built-in administrators are distinguished from the users registered in the Address Book. The login user name registered in the Address Book cannot be used as the login user name of a built-in administrator.

Activating Administrator Authentication

An administrator can manage the machine by activating the management function.

Important

- **If you have activated Administrator Authentication, make sure not to forget the login user names and login passwords of the built-in administrators. If you forget an administrator login user name or password, you must specify a new password using the supervisor's privilege.**

  page 87 "Changing the Password of a Built-in Administrator"

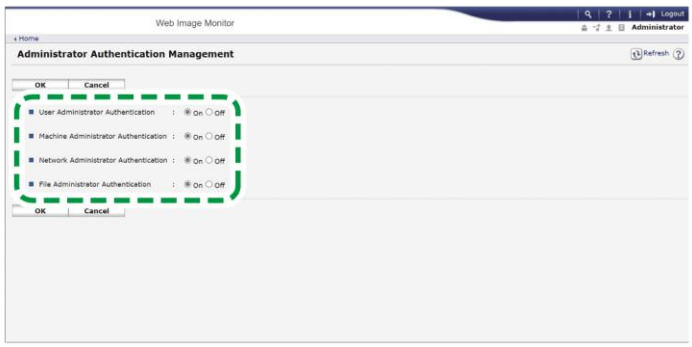
1. **Launch the Web browser.**
2. **Enter "http://(IP address of the machine) or (host name)/" in the address bar of the Web browser, and then press Enter.**
3. **Log in to the machine as an administrator.**

   page 80 "Logging in to the Machine as an Administrator"

4. **Click [Configuration] from the [Device Management] menu.**



5. **Click [Administrator Authentication Management] in the "Device Settings" category.**
6. **Select [On] on the administrator privilege to activate administrator authentication.**



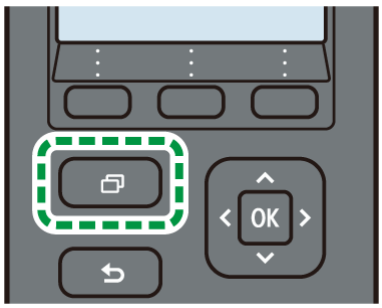
7. **Click [OK] and exit the Web browser.**

Logging in to the Machine as an Administrator

To log in to the machine for the first time, log in as Administrator 1 of the built-in administrators. To log in to the machine for the first time, login as Administrator 1. Refer to the provided guide for the Login User Name and Login Password.

Logging in to the machine using the control panel

1. **Press the [Menu] key.**



2. **Press the selection key beneath [Login].**



3. **Press the selection key beneath [Enter].**
4. **Press the [◀] or [▶] key to select a character for your login user name, and then press the [OK] key to enter the character. Repeat this to complete your login user name, and then press the selection key beneath [Accept].**



   - To enter upper-case letters, numerals, or symbols, press the selection key beneath [ABC/123].
   - To delete a character that has been entered, press the selection key beneath [Delete].
5. **Press the selection key beneath [Enter].**
6. **Follow the instructions in Step 4 to enter the login user password, and then press the selection key beneath [Accept].**

   To register or change an administrator other than yourself, follow the procedures described in page 82 "Adding Built-in Administrators or Changing the Privileges".
7. **After completing the procedure, press the selection key beneath [Logout].**

Note

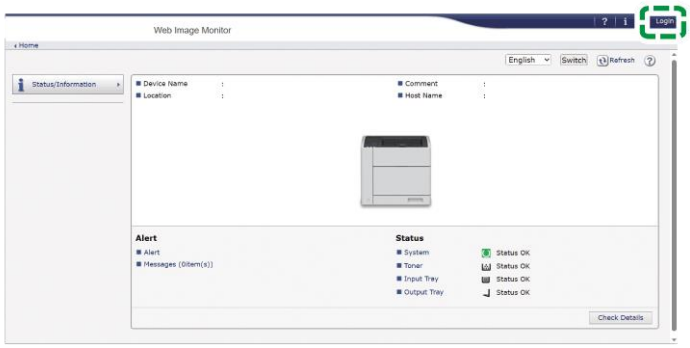
- If you log in to the machine using one of the administrator privileges, the name of the built-in administrator logging in appears. When you log in with a user name that has multiple administrator privileges, one of the administrator privileges associated with that name is displayed.
- For the characters that can be used for login user names and passwords, see page 89 "Usable Characters for User Names and Passwords".

Logging in to the machine using Web Image Monitor

1. **Launch the Web browser.**
2. **Enter "http://(IP address of the machine or host name)/" on the address bar of the Web browser, and then press the Enter key.**

   page 30 "Accessing to Web Image Monitor"

3. **Click [Login].**



4. **Enter the login user name and login password of the administrator, and then click [Login].**
5. **After completing machine operations, click [Logout].**

   Delete the cache memory of a web browser after logging out.

5

Note

- The Web browser might be configured to auto complete login dialog boxes by keeping login user names and passwords. This function reduces security. To prevent the browser from keeping login user names and passwords, disable the browser's auto complete function.

Adding Built-in Administrators or Changing the Privileges

You can register up to four administrators. All four registered personnel can have all the administrator privileges. To reduce the administrator's load, each of the four registered personnel can have a specific one of the administrator privileges.

Discuss the number of users to add and privileges to give in advance, decide the login user name and login password for Administrator 2 to Administrator 4, and configure the settings.

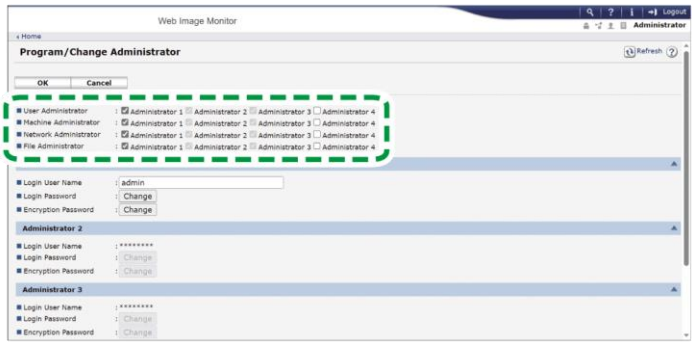
Important

- **Do not forget the login user names and login passwords of the added built-in administrators.**
- **A built-in administrator cannot change the login user names and passwords for other built-in administrators.**

1. **Log in to the machine as an administrator with all the administrator privileges from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**



3. **Click [Program/Change Administrator] in the "Device Settings" category.**
4. **Select an administrator to assign for each of the administrator privileges.**



   - Assign the privileges of User Administrator, Machine Administrator, Network Administrator, or File Administrator to [Administrator 1] to [Administrator 4].
   - By default, all administrator privileges are assigned to the logged-in built-in administrator (Administrator 1).
   - Administrator privileges assigned to a person can be assigned to another person.
5. **Enter the Login User Name of Administrator 1 to Administrator 4.**
6. **Click [Change] next to "Login Password" on each of the administrators.**
7. **Enter the login password in "New Password".**
8. **Re-enter the login password in "Confirm Password", and then click [OK].**

   When you manage the machine with software supporting SNMPv3 such as Device Manager NX, you have to specify the password to encrypt communication.
9. **Click [OK] and exit the Web browser.**

   Take note of the login user names and login passwords specified for other administrators and inform them of the specified ones.

Note

- For the characters that can be used for login user names and passwords, see page 89 "Usable Characters for User Names and Passwords".

- An administrator with any one of the administrator privileges can add built-in administrators or change the privileges as well by logging in to the machine. The privilege(s) that the administrator can assign to other built-in administrators, however, is limited to the same privilege as the one that is assigned to the administrator himself.

Registering External Administrator Groups and Assigning the Administrator Privileges

When Windows authentication is activated as the user authentication method, you can register external authentication server accounts as external administrators. Register external administrator groups and assign the same four types of administrator privileges as the ones that are assigned to the built-in administrators.

To register a Windows server account as an external administrator, register an external administrator group with the same name as the global account to which the target account belongs and for which it has administrative privileges. You first need to confirm the name of the global group to which the target account belongs.

page 95 "Specifying Windows Authentication"

Important

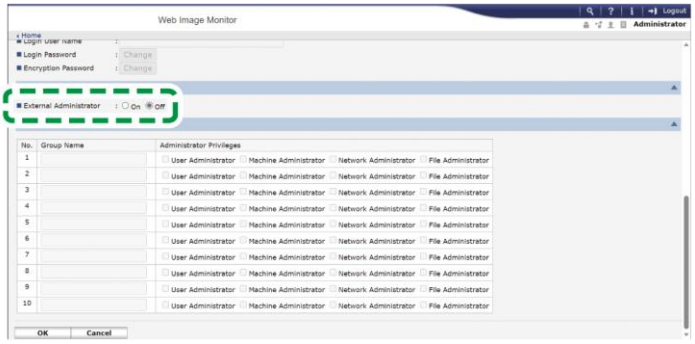
- **You cannot configure any Windows server account as an account for SNMPv3 access.**
- **When the central address book management is enabled, no external administrators can be registered.**

  For details about the central address book management, see Web Image Monitor Help.

1. **Log in to the machine as an administrator with all the administrator privileges from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**



3. **Click [Program/Change Administrator] in the "Device Settings" category.**
4. **Select [On] for [External Administrator].**



5. **Enter the name of an external administrator group in [Group Name].**

   To register Windows server accounts as external administrators, enter the same group name as the name of the global group to which the target account belongs.

6. **Select the administrator privileges to be assigned to the external administrator in "Administrator Privileges".**

Note

- You can register up to 10 external administrator groups.
- You can change the name or administrator privilege of the registered external administrator group in step 5.
- To delete the registered external administrator group, delete the group name in step 5, and then remove the check for administrator privileges.
- An administrator with any one of the administrator privileges can add external administrator groups or change the privileges as well by logging in to the machine. The privilege(s) that the administrator can assign to other external administrator groups, however, is limited to the same privilege as the one that is assigned to the administrator himself.
- In the event that a user account on the Windows server belongs both to a group with the administrator privileges and to an ordinary user group, the user is recognized as an ordinary user, not as an external administrator, when logging in to the machine. To let the user log in to the machine as an external administrator, make sure that the user is not a member of an ordinary user group on the Windows server.
- When a user registered in the Address Book of the machine logs in to the machine, user recognition by the machine varies depending on the group to which the user is registered on the Windows server.
  - When registered in a group with the administrator privileges: Recognized as an external administrator.
  - When registered in an ordinary user group: Recognized as the same user as the one registered in the address book of the machine.

Using the Supervisor Privilege

The supervisor has the privilege to manage the built-in administrators. When the built-in administrator is changed, the supervisor can reset the login password. There is only one supervisor.

Changing the Supervisor Settings

This section describes how to change the supervisor's login user name and password.

Refer to the provided guide for the default login user name and login password of the supervisor.

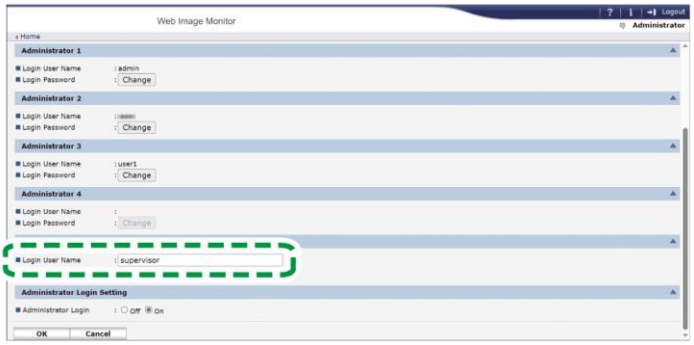
Important

- **Do not forget the login user name and login password of the supervisor. If you forget these, you have to restore the factory default settings, which will result in loss of data.**

1. **Log in to the machine as the supervisor from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**



3. **Click [Program/Change Administrator] in the "Device Settings" category.**
4. **Enter the Login User Name of Supervisor.**



5. **Click [Change] next to "Login Password".**
6. **Enter the login password in "New Password".**
7. **Re-enter the login password in "Confirm Password", and then click [OK].**
8. **Click [OK] and exit the Web browser.**

   When settings are complete, the machine is automatically logged out.

Note

- For the characters that can be used for login user names and passwords, see page 89 "Usable Characters for User Names and Passwords".

Changing the Password of a Built-in Administrator

Only the supervisor has the privilege to change the password of the built-in administrators. If a built-in administrator forgets the password or wants to change the password, the supervisor must reset the password.

Refer to the provided guide for the default login user name and login password of the supervisor.

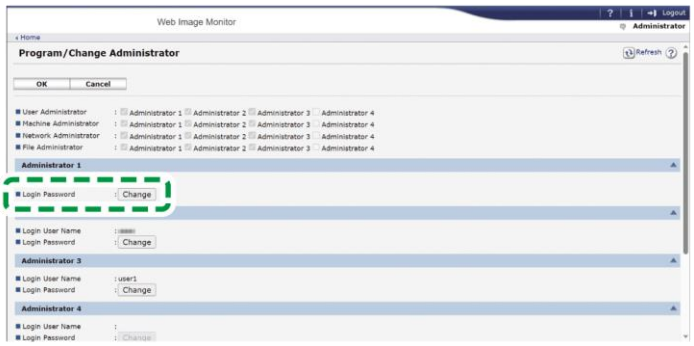
Important

- **Do not forget the login user name and login password of the supervisor. If you forget these, you have to restore the factory default settings, which will result in loss of data.**

1. **Log in to the machine as the supervisor from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**



3. **Click [Program/Change Administrator] in the "Device Settings" category.**
4. **Click [Change] next to "Login Password" on the administrator whose password is to be reset.**



5. **Enter the login password in "New Password".**
6. **Re-enter the login password in "Confirm Password", and then click [OK].**
7. **Click [OK] and exit the Web browser.**

Note

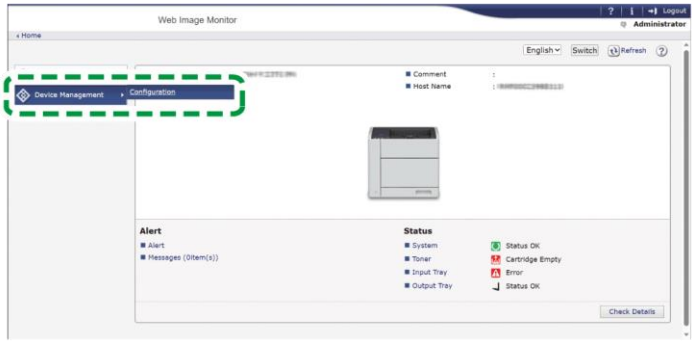
- For the characters that can be used for login user names and passwords, see Usable Characters for User Names and Passwords.
- You cannot specify the same login user name for the supervisor and the administrators.

Changing the Administrator Login Setting

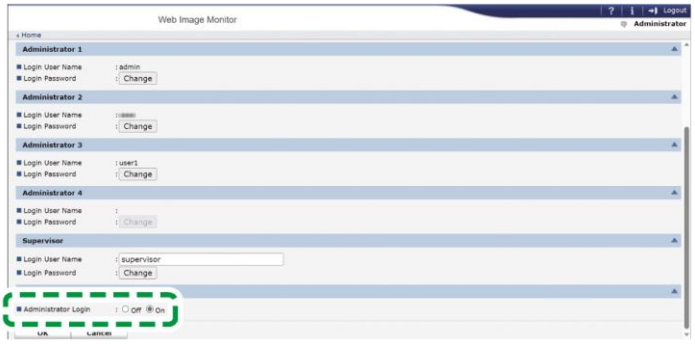
Only the supervisor has the privilege to allow/prohibit login to the machine by the built-in administrators.

In the event of a failure in communicating with an external authentication server while login by the built-in administrators is prohibited and only the external administrators are allowed to log in to the machine, no administrators can log in to the machine. In such a case, the supervisor must change the administrator login setting to allow the built-in administrators to log in to the machine.

1. **Log in to the machine as the supervisor from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**



3. **Click [Program/Change Administrator] in the "Device Settings" category.**
4. **Set [Administrator Login] to [On].**



5. **Click [OK] and exit the Web browser.**

Usable Characters for User Names and Passwords

The following characters can be used for login user names and passwords. Names and passwords are case-sensitive.

- Upper case letters: A to Z (26 characters)
- Lower case letters: a to z (26 characters)
- Numbers: 0 to 9 (10 characters)
- Symbols: (space) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 characters)

Login user name/Password	Supervisor/Built-in Administrators/Users	External Administrators
Login user name	• Can be up to 32 characters long. • Cannot contain spaces, colons or quotation marks. • Cannot be left blank. • The login user name of the supervisor and administrators must contain characters other than numerical characters (numbers) if it is up to 8 characters. If it consists of only numbers, 9 or more must be used.	
Login password	• The maximum password length for the administrators and supervisor is 32 characters. • The maximum password length for users is 128 characters.	• The maximum password length is 128 characters. *1

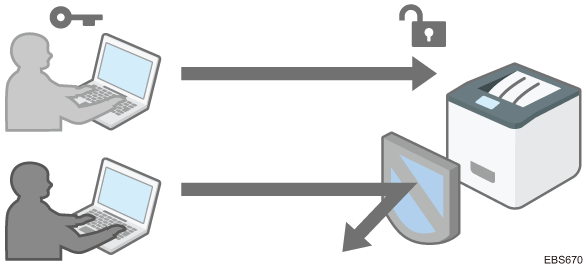
Login user name/Password	Supervisor/Built-in Administrators/Users	External Administrators
	• There are no restrictions on the types of characters that can be used for a password. For security, it is recommended to create passwords consisting of uppercase or lowercase characters, numbers, and symbols. A password consisting of a large number of characters is less easily guessed by others. • In [Password Policy] in [Extended Security], you can specify a password consisting of uppercase or lowercase characters, numbers, and symbols, as well as the minimum number of characters to be used for the password. See Specifying the Extended Security Functions, User Guide in English.	• For the other conditions, the password policy of the external authentication server is applied.

*1 Attempts to log in as an external administrator may fail from an application where a limitation is imposed on the password length.

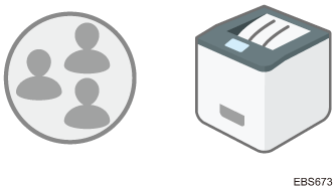
Preventing Unauthorized Accesses

Taking Measures to Prevent Unauthorized Access

Specify the machine to prevent access by anyone from any location so as to protect the information asset. You can prevent unauthorized access by restricting the users who can use the machine and encrypting or restricting the network.



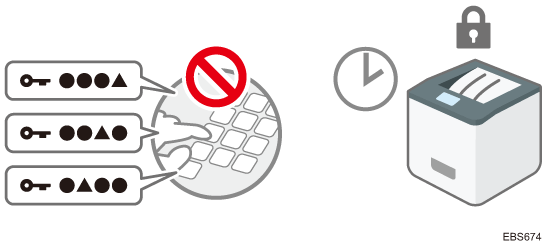
Specifying user authentication



The administrator registers the users on the machine and only the registered users can use the machine.

page 92 "Verifying Users to Operate the Machine (User Authentication)"

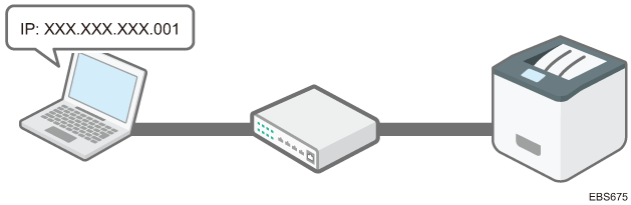
Specifying the authentication policy



Specify how many times entering an incorrect password is allowed and the auto-logout time when you do not operate the machine for a specified period of time to protect the machine from unauthorized use.

page 106 "Specifying the Policy on Login/Logout"

Restricting the network connection



To block access from an unauthorized computer for TCP/IP communication, restrict the range of IP addresses allowed to access the machine. Also, specify the unused protocols to reduce the risk of intrusion.

page 110 "Access Control"

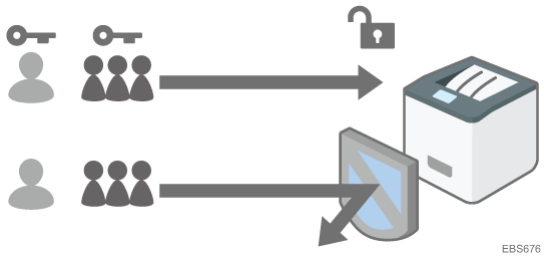
Encrypting the network communication

Reduce the risk of information leaks by encrypting communication between this machine and the computers or external devices. For encryption, installation of the Device Certificate is required.

page 120 "Encrypting Network Communication"

Verifying Users to Operate the Machine (User Authentication)

"User authentication" is a system to authenticate users and grant them privileges to use the machine. The machine requires entering an arbitrary text, the login user name, or the login password to authenticate a user.



User authentication prevents unauthorized users from operating the machine and is useful for managing and analyzing usage of the machine regarding the user, operation time, and frequency.

See Confirming the Counter for Each User, User Guide in English.

User Authentication Method

There are four types of user authentication methods including Basic authentication that limits use of the machine and methods that use an authentication server in the network. Select a method depending on the usage condition or the number of users. You cannot use more than one authentication method at the same time.

User Authentication Method	Explanation
User Code authentication	Authentication is performed using an up to eight-digit user code registered in the Address Book of the machine. When specifying User Code authentication, the machine prompts you to enter the user code to use the machine. Multiple users can use the same user code. You can activate User Code authentication without activating Administrator Authentication.
Basic authentication	Authentication is performed using the login user name and login password registered in the Address Book on the machine. When specifying Basic authentication, the machine prompts you to enter the login information to use the machine.
Windows authentication	Authentication is performed using the account registered in the Active Directory of the Windows server. When specifying Windows authentication, the machine prompts you to enter the login information to use the machine.
LDAP authentication	Authentication is performed using the user information registered in the LDAP server. When specifying LDAP authentication, the machine prompts you to enter the login information to use the machine.

- In Windows or LDAP authentication, the machine can authenticate you without registering your user information in the machine's Address Book manually, as the user information in the server is registered in the machine automatically.
- In Windows or LDAP authentication, you can manage user information centrally in the server. You can also always use the address provided by the server as the sender (From) of e-mails sent from the machine. These features are useful to avoid data leakage by erroneous input of information or spoofing by an unauthorized user.
- When switching the authentication method from User Code authentication to another method, the user code will be used as the login user name. In this case, the login password is not specified. To avoid unauthorized use, delete unnecessary user information and set up a password for the continuing users.

Note

- If user authentication cannot be performed due to a problem with the machine or network, the machine administrator can disable user authentication temporarily in order to use the machine. Take this measure only during emergencies.

Specifying User Code Authentication

Specify the functions to restrict with User Code authentication.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [User Authentication Management] in the "Device Settings" category.**
4. **Select [User Code] in [User Authentication Management].**
5. **Specify the functions to restrict.**
   - Printer Job Authentication

     Select the security level for print jobs using the printer driver.

     page 104 "Executing a Print Job with Authentication Information Only"
   - Functions to Restrict

     Specify whether to perform User Code authentication.

     When registering the user code of the printer driver automatically, select [PC Control]. Specify the user code registered in the address book to the printer driver.

     When [PC Control] is selected, the user code specified in the printer driver is registered in the address book automatically and is excluded from the print volume use limitation. To limit the print volume use, select [Black & White].

     Specifying Maximum Print Volume Use of Each User, Settings
6. **Click [OK] and exit the Web browser.**

   If registration of the user information is not completed, register the user in the Address Book and specify the user code.

   page 97 "Registering/Changing/Deleting User Codes"

Specifying Basic Authentication

Register the default values of the functions available to each user with Basic authentication.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [User Authentication Management] in the "Device Settings" category.**
4. **Select [Basic Authentication] in [User Authentication Management].**
5. **Specify the security level and the usable functions.**
   - Printer Job Authentication

     Select the security level for print jobs using the printer driver.

     page 104 "Executing a Print Job with Authentication Information Only"
   - Available Functions

Specify the functions available to the user.

6. **Click [OK] and exit the Web browser.**

   If registration of the user information is not completed, register the user in the Address Book and specify the login information. For details, see Web Image Monitor Help.

Note

- The login user name and login password can be used to authenticate the user in the SMTP or LDAP server, or to authenticate shared folders. Use a login user name other than "other", "admin", "supervisor", or "HIDE***". (Enter an optional character string in "***".) You cannot use these user names for authentication because they are already in use in the machine.

Specifying Windows Authentication

Register the Windows server information required for authentication with the Windows server.

Important

- **In advance, check the use conditions in the Windows server, and install the Web server (IIS) and the Active Directory Certificate Service in the Windows server.**

  page 98 "Preparing the Server to Use for User Authentication"
- **To use Kerberos authentication in the server, register the realm in advance to determine the network area.**

  See Registering the Realm, User Guide in English.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [User Authentication Management] in the "Device Settings" category.**
4. **Select [Windows Authentication] in [User Authentication Management].**
5. **Register the server for authentication and specify the usable functions.**
   - Printer Job Authentication

     Select the security level for print jobs using the printer driver.

     page 104 "Executing a Print Job with Authentication Information Only"
   - SSL

     To encrypt communication signals, click [On].
   - Kerberos Authentication

     To enable Kerberos Authentication, click [On].
   - Domain Name

     To disable Kerberos authentication, enter the domain name to authenticate.
   - Realm Name

To enable Kerberos authentication, select the realm name to authenticate.

- Group Settings for Windows Authentication

  If global groups have been registered, you can specify usable functions for each global group*. Enter the same name as the one registered in the server in "*Default Group" to specify the available functions.

  Users who are registered in multiple groups can use all functions available to those groups.

  A user who is not registered in any group can use the authority specified in "*Default Group". By default, all functions are available to the Default Group members.

6. **Click [OK] and exit the Web browser.**

Note

- For the characters that can be used for login user names and passwords, see page 89 "Usable Characters for User Names and Passwords".
- When accessing the machine subsequently, you can use all the functions available to your group and to you as an individual user.
- Under Windows authentication, you do not need to create a server certificate unless you want to automatically register user information such as user names using SSL.

Specifying LDAP Authentication

Register the LDAP server information required for authentication with the LDAP server.

Important

- **In advance, check the use conditions in the LDAP server, and register the LDAP server in the machine.**

  page 98 "Preparing the Server to Use for User Authentication"

  See Registering the LDAP Server, User Guide in English.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [User Authentication Management] in the "Device Settings" category.**
4. **Select [LDAP Authentication] in [User Authentication Management].**
5. **Register the server for authentication and specify the usable functions.**

   - Printer Job Authentication

     Select the security level for print jobs using the printer driver.

     page 104 "Executing a Print Job with Authentication Information Only"

   - LDAP Authentication

     Select the LDAP server to authenticate.

   - Login Name Attribute

Use this as a search criterion to obtain user information. Create a search filter based on the login name attribute, select a user, and then retrieve the user information from the LDAP server to transfer to the machine's address book.

When separating multiple login attributes with a comma (,), the search will return hits by entering a login name for either or both attributes.

Also, by entering two login names separated by an equal sign (=) (for example: cn=abcde, uid=xyz), the search will return hits only for a match of the attributes of both login names. This search function can be applied when Cleartext authentication is specified.

- Unique Attribute

  Specify this to match the user information in the LDAP server with that in the machine. A user whose unique attribute registered in the LDAP server matches that of a user registered in the machine is treated as the same user in the machine. Specify the attribute that is used for unique information in the server as the Unique Attribute. You can enter "cn" or "employeeNumber" to use as "serialNumber" or "uid" as long as it is unique.

- Available Functions

  Specify the functions available to the user.

6. **Click [OK] and exit the Web browser.**

Note

- For the characters that can be used for login user names and passwords, see page 89 "Usable Characters for User Names and Passwords".
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To use blank passwords, contact your service representative.

Registering/Changing/Deleting User Codes

By registering user codes in the Address Book, you can confirm print volume on a personal basis.

1. **Disable user authentication or specify User Code authentication.**

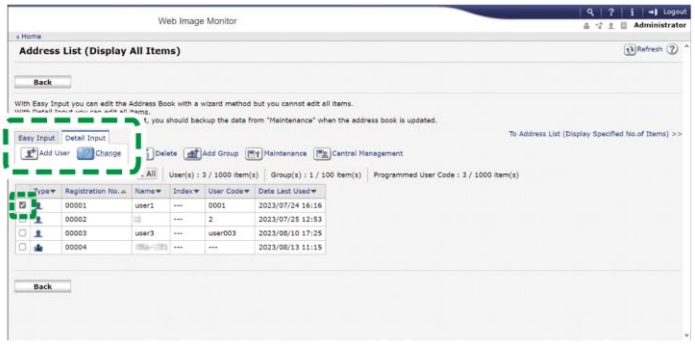
   page 92 "User Authentication Method"

   page 94 "Specifying User Code Authentication"

2. **Log in to the machine as the user administrator from Web Image Monitor.**
3. **Click [Address Book] from the [Device Management] menu.**



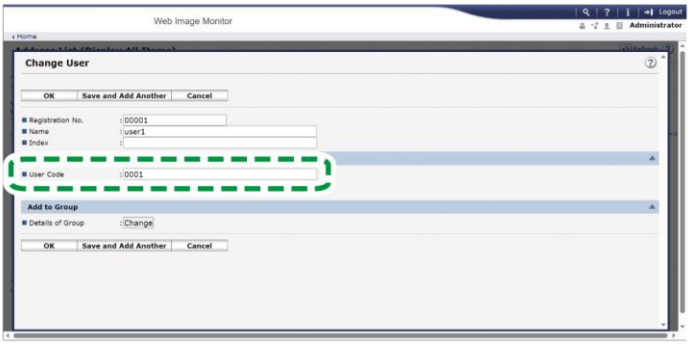
4. **Select a user, and then click [Change] on the [Detail Input] tab.**



5. **Enter a user code for "User Code".**

   To change a user code, delete the registered code and enter the new code.

   To delete a user code, delete the registered code.



6. **Click [OK] and exit the Web browser.**

Note

- Deleting a user code clears the respective print volume as well.

Preparing the Server to Use for User Authentication

When using Windows authentication or LDAP authentication as the user authentication method for the first time, check that your server environment meets the requirements for user authentication, and configure the required settings.

To use Windows authentication

Prepare the server as follows:

1. Check the requirements of Windows authentication.
2. Install the Web server (IIS) and the Active Directory Certificate Service in the server.
3. Create a server certificate.

   You do not need to create a server certificate to transmit user information that is not encrypted.

To use LDAP authentication

Check the requirements of LDAP authentication, and configure the settings according to the server environment as necessary.

Requirements of Server Authentication Used for User Authentication

Windows authentication

Items	Explanation
Usable OS	Windows Server 2012/2012 R2/2016/2019/2022
Authentication method	Supports the following authentication methods: • NTLM authentication (NTLMv1/NTLMv2) • Kerberos authentication
Requirements for authentication	• Set up a domain controller in the domain you specify. • To obtain user information when Active Directory is running, use LDAP. It is recommended that communication be encrypted between the machine and the LDAP server by using SSL/TLS. The server must support the TLS 1.0/1.1/1.2/1.3 or SSL 3.0 encryption method. Register the server certificate of the domain controller in advance. page 102 "Creating a Server Certificate" • TLS 1.0, TLS 1.1, and SSL 3.0 are disabled by default. To use TLS 1.0/1.1 or SSL 3.0, enable it on Web Image Monitor. • Data transmission between the machine and the KDC (Key Distribution Center) server must be encrypted if Kerberos authentication is enabled. page 120 "Encrypting Network Communication"

Note

- The server can authenticate users managed in other domains, but cannot obtain information such as an e-mail address.
- Even if you edit an authenticated user's information in the machine's Address Book, it may be overwritten by the information from the server when authentication is performed.
- If you created a new user in the domain controller and selected "User must change password at next logon" at password configuration, first log on the computer and change the password.
- If the Guest account on the Windows server is enabled, users not registered in the domain controller can be authenticated. When this account is enabled, users are registered in the Address Book and can use the functions available under "* Default Group".

LDAP authentication

Items	Explanations
Usable version	LDAP Version 2.0/3.0
Authentication method	Supports the following authentication methods: • Kerberos authentication • Digest authentication • Cleartext authentication When you select Cleartext authentication, LDAP simplified authentication is enabled. Simplified authentication can be performed with a user attribute (such as cn or uid) instead of the DN.
Requirements for authentication	• To use SSL/TLS, the server must support the TLS 1.0/1.1/1.2/1.3 or SSL 3.0 encryption method. • TLS 1.0, TLS 1.1, and SSL 3.0 are disabled by default. To use TLS 1.0/1.1 or SSL 3.0, enable it on Web Image Monitor. • To use Kerberos authentication, register the realm to distinguish the network area. See Registering the Realm, User Guide in English. • Data transmission between the machine and the KDC (Key Distribution Center) server must be encrypted if Kerberos authentication is enabled. page 120 "Encrypting Network Communication" • When you use LDAP, only version 3.0 can use Digest authentication.

Notes when the LDAP server is configured using Active Directory

- Anonymous authentication might be available. To improve security, set anonymous authentication to Disable.

Note

- Even if you edit an authenticated user's information in the machine's Address Book, it may be overwritten by the information from the server when authentication is performed.
- Under LDAP authentication, you cannot specify access limits for groups registered in the server.
- Do not use double-byte Japanese, Traditional Chinese, Simplified Chinese, or Hangul characters when entering the login user name or password. If you use double-byte characters, you cannot authenticate using Web Image Monitor.
- When using the machine for the first time, the user can use Available Functions specified in [User Authentication Management].
- To specify Available Functions for each user, register the user together with Available Functions in the Address Book, or specify Available Functions in the user registered automatically in the address book.

Installing the Web Server (IIS) and the "Active Directory Certificate Service"

Install the required service in the Windows server to obtain user information registered in Active Directory automatically.

1. **On the [Start] menu, click [Server Manager].**
2. **On the [Manage] menu, click [Add Roles and Features].**
3. **Click [Next].**
4. **Select [Role-based or feature-based installation], and then click [Next].**
5. **Select a server, and then click [Next].**
6. **Select the [Active Directory Certificate Service] and [Web Server (IIS)] check boxes, and then click [Next].**

   If a confirmation message appears, click [Add Features].
7. **Check the features to install, and then click [Next].**
8. **Read the content information, then click [Next].**
9. **Make sure that [Certification Authority] is selected in the Role Services area in Active Directory Certificate Services, and then click [Next].**
10. **Read the content information, then click [Next].**

    When using Windows Server 2016, proceed to Step 12 after reading the content information.

11. **Check the role services to install under Web server (IIS), and then click [Next].**
12. **Click [Install].**
13. **When using Windows Server 2019 or Windows Server 2022, click [Close].**
14. **After completing the installation, click the notification icon of the server manager, and then click [Configure Active Directory Certificate Service on the destination server].**
15. **Click [Next].**
16. **Check [Certification Authority] in the role service, and then click [Next].**
17. **Select [Enterprise CA], and then click [Next].**
18. **Select [Root CA], and then click [Next].**
19. **Select [Create a new private key], and then click [Next].**
20. **Select a cryptographic provider, key length, and hash algorithm to create a new private key, and then click [Next].**
21. **In [Common name for this CA:], enter the Certificate Authority name, and then click [Next].**
22. **Select the validity period, and then click [Next].**
23. **Leave [Certificate database location:] and [Certificate database log location:] without change, and then click [Next].**
24. **Click [Configure].**
25. **When the message "Configuration succeeded" appears, click [Close].**

Creating a Server Certificate

To encrypt user information, create a server certificate in the Windows server. Windows Server 2016 is used as an example.

1. **On the [Start] menu, point to [All Applications], and then click [Internet Information Service (IIS) Manager] of [Administrative Tools].**
2. **In the left column, click [Server Name], and then double-click [Server Certificate].**
3. **In the right column, click [Create Certificate Request...].**
4. **Enter all the information, and click [Next].**
5. **In [Cryptographic service provider:], select a provider, and then click [Next].**
6. **Click [...], and then specify a file name for the certificate request.**
7. **Specify a location in which to store the file, and then click [Open].**
8. **Click [Finish].**

Limiting Available Functions

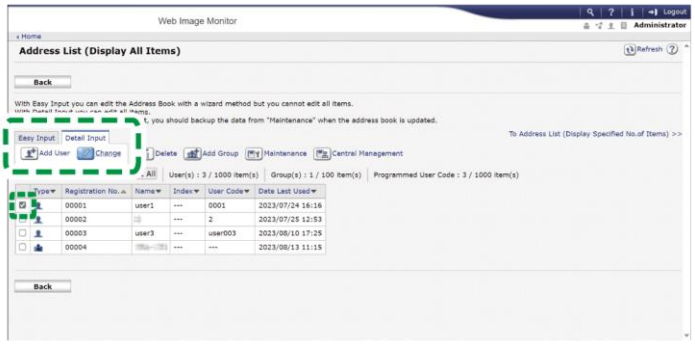
To prevent unauthorized operations, you can specify who is allowed to access each of the machine's functions.

Specify the functions available to registered users. By configuring this setting, you can limit the functions available to users.

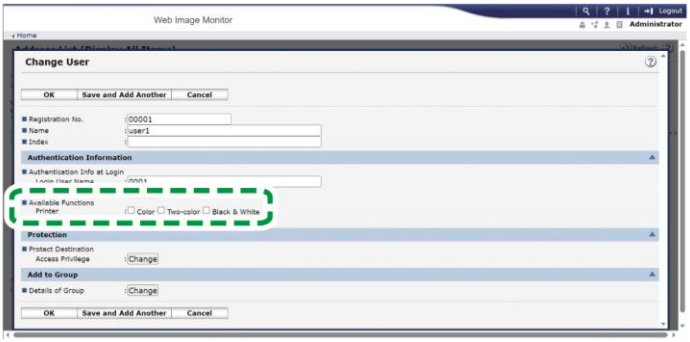
1. **Log in to the machine as the user administrator from Web Image Monitor.**
2. **Click [Address Book] from the [Device Management] menu.**



3. **Select a user, and then click [Change] on the [Detail Input] tab.**



4. **Select available functions.**



5. **Click [OK] and exit the Web browser.**

Executing a Print Job with Authentication Information Only

The machine authenticates print jobs specified on the control panel and also specified via the network.

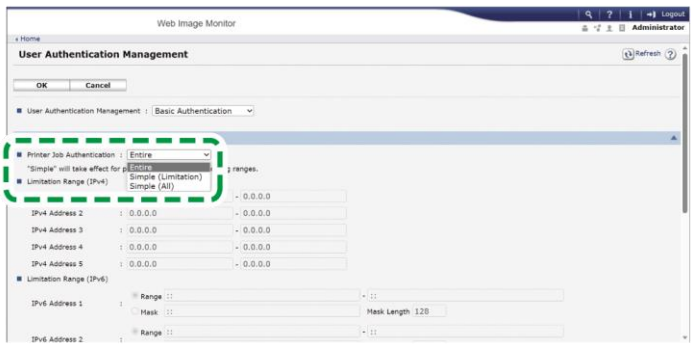
To print from the printer driver, specify user authentication in [Printer properties].

See Specifying Login Information in the Printer Driver, User Guide in English.

See Specifying a User Code in the Printer Driver, User Guide in English.

An unauthenticated print job may not be printed according to the security level specified in Printer Job Authentication. You can view the Printer Job Authentication setting in [User Authentication Management].

Security level of Printer Job Authentication



- Entire: Authenticates all print jobs. You cannot specify a print job from the printer driver or device that does not support user authentication. A print job that cannot be authenticated is displayed on the control panel and is canceled.
- Simple (Limitation): The print jobs from the specified range are exempt from authentication. Specify the range of IPv4 addresses not to authenticate. You can specify not to authenticate print jobs from the USB connection. The security level is the same as [Simple (All)].
- Simple (All): Authenticates only print jobs from the printer drivers that support user authentication. Print jobs without authentication information specified

from a printer driver that does not support user authentication or specified by a command are performed without being authenticated. Select this when printing with a printer driver or device that cannot be identified by the machine.

Printer drivers that support Printer Job Authentication

- PCL6: User code authentication, Basic authentication, Windows authentication, LDAP authentication
- PostScript 3: User Code authentication

Print job types and authentication settings

Depending on the combination of print job authentication level and print job type, the machine may not print properly as follows:

✓: Printing is possible when Printer Job Authentication is successful or regardless of user authentication.

-: Printing is not possible.

Types of printer driver/job	Authentication setting	Security level	
		All	Simple (All)
PCL 6	Login user name/Login password	✓	✓
	User code	✓	✓
	None	-	✓
PostScript 3	User code	✓	✓
	None	-	✓
LPR printing of a PDF file	None	-	✓
ftp printing of a PDF file	User ID and password logged in ftp	✓	✓
Generic driver	Login user name/Login password Driver encryption key	✓*1	✓*1
	Login user name/Login password	✓*2	✓*2
	User code	✓	✓

*1 Printing is not performed when the encryption method (encryption algorithm) is specified to AES (Advanced Encryption Standard).

*2 Printing is not performed when the encryption method (encryption algorithm) is specified to DES (Data Encryption Standard) or AES (Advanced Encryption Standard).

Note

- Specify the driver encryption key or encryption method in [Driver Encryption Key] or [] in [Extended Security] in [Security Options].
- You can specify the range of IPv4 addresses to use for [Simple Encryption] of [Driver Encryption Key: Encryption Strength] from Web Image Monitor or with the authfree command of telnet. For details about the telnet command, see "Device Monitoring (TELNET)" on our website.

Specifying the Policy on Login/Logout

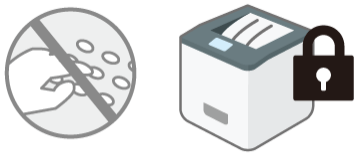
To protect the data in the machine, configure the machine so that login and logout are performed properly.

User authentication cannot prevent unauthorized use completely. For example, an unauthorized person can log in to the machine by guessing the password. If a user does not log out of the machine, another user can use the privileges of the previous user.

Specify the following functions to protect the machine against such risks.

User Lockout

If an incorrect login password is entered several times, the user lockout function prevents further login attempts under the same login user name (Lockout). The locked-out state can be automatically released in a specified period of time. It can be manually released by the administrator as well.



EBS692

- The number of times that the locked-out state is automatically released can be limited to a maximum of four times. For each of the 1st to 4th lockout actions, you can specify whether to activate/deactivate the user lockout function, the number of login attempts before lockout, and the period of time before the locked-out state is automatically released.
- You can also specify whether to release the locked-out state by restarting the machine.

  page 108 "Specifying User Lockout"
- By default, an incorrect login password entry is permitted up to five times and the locked-out state is not released automatically.

Note

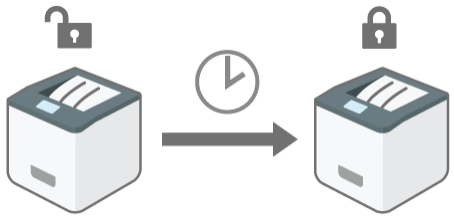
- The User lockout function is enabled on all users only when Basic authentication is specified. Under Windows authentication and LDAP authentication, only the supervisor and administrators are protected by User lockout. The policy of the certification server is applied to the other users.
- In the event that a user enters an incorrect login password, and the machine administrator changes the number of attempts before lockout afterwards, the state of the user concerning lockout may vary in accordance with the number of attempts before lockout that is changed by the administrator. Some examples are as follows:

Number of incorrect login password entries by user	Change to the number of attempts before lockout	State of user
3 entries	Twice -> 4 times	The locked-out state of the user is released.
3 entries	4 times -> Twice	The user is locked out.
3 entries	4 times -> 6 times	Remains unchanged (The user is not locked out.) *1

*1 After 3 entries of an incorrect login password, two more incorrect entries are permitted, and when an incorrect entry is performed for a third time, the user is locked out.

Auto Logout Timer

After you log in, the machine logs you out automatically if you do not use the control panel within a given time.



EBS677

- By default, the machine logs you out automatically if you do not use the control panel for one minute.

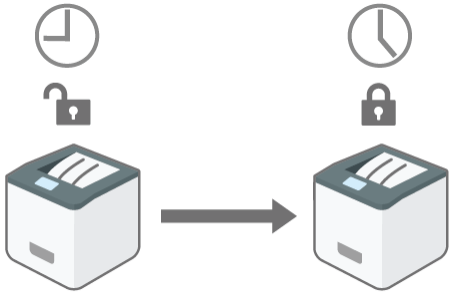
  See Timer Settings, User Guide in English.
- When the time period to allow users to log in to and use the machine is specified, the machine logs you out upon completion of the time period even though the auto logout timer has not expired.

  page 110 "Specifying the Time Period to Allow Users to Log In to and Use the Machine"

- For details about auto logout from Web Image Monitor, see Web Image Monitor Help.

Time Settings Allowing Operating Machine by Logging in

When the time period to allow users to log in to and use the machine is specified, the machine logs you out upon completion of the time period.



page 110 "Specifying the Time Period to Allow Users to Log In to and Use the Machine"

Specifying User Lockout

Specify the number of login password attempts to permit before locking out the user and the period of time until the lockout is released automatically.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**

   page 80 "Logging in to the Machine as an Administrator"

2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [User Lockout Policy] in the "Security" category.**
4. **Specify the number of login password attempts to permit before locking out the user and the period of time until the lockout is automatically released.**

   - Lockout (n^{th} Time)

     Select [Active], and then specify "Number of Attempts before Lockout" from 1 to 10.

   - Lockout Release Timer

     Select [Active] to release the locked-out state after a specified time elapses, and then enter the desired value in "Lock Out User for" up to 9999 minutes (about seven days).

   - Release Lockout When Restarting and Rebooting System

     Specify whether to activate the lockout release function by restarting the machine. The supervisor and administrators are subject to the lockout release function.

It takes about 60 seconds for the locked-out state to be actually released after the machine restarts.

5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Releasing the Locked-out State

When a general user is locked out, the user administrator must log in and release the locked-out state.

1. **Log in to the machine as the user administrator from Web Image Monitor.**

   page 80 "Logging in to the Machine as an Administrator"
2. **Click [Address Book] on the [Device Management] menu.**
3. **Select the locked-out user's account, and then click [Change] on the [Detail Input] tab.**
4. **Select [Inactive] on "Lockout" of "Authentication Information".**
5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Note

- When an administrator is locked out, the supervisor must log in to the machine and release the locked-out state. When the supervisor is locked out, the machine administrator must log in to the machine and release the locked-out state. Click [Device Management] ▶ [Configuration] ▶ [Program/Change Administrator] to display the Program/Change Administrator screen, and then release the locked-out state.
- For the supervisor and administrators, you can specify whether to activate the lockout release function by restarting the machine as well.

  page 108 "Specifying User Lockout"

Specifying the Period of Time Until the Machine Logs You Out Automatically

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [Timer] in the "Device Settings" category.**
4. **In "Auto Logout Timer", select [On] and enter the period of time until the machine logs you out automatically.**

   You can enter from 10 to 999 seconds.

5. **Click [OK] and exit the Web browser.**

Note

- When the time period to allow users to log in to and use the machine is specified, the machine logs you out upon completion of this time period even though the auto logout timer has not expired.

  page 110 "Specifying the Time Period to Allow Users to Log In to and Use the Machine"

Specifying the Time Period to Allow Users to Log In to and Use the Machine

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [Time Settings Allowing Operating Machine by Logging in] in the "Device Settings" category.**
4. **Select [Active] for "Time Settings Allowing Operating Machine by Logging in", and then enter the time in "Start Time" and "End Time".**
5. **Click [OK] and exit the Web browser.**

Access Control

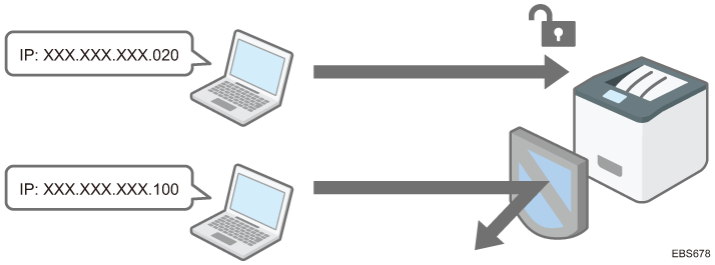
The administrator can limit devices or protocols that can be connected to the machine to avoid unintended access.

Also, the administrator can select a security level at which to enable or disable a protocol and to configure the port status.

Limiting machine access (access control)

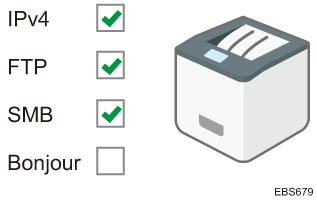
You can limit the IP addresses from which devices can access the machine or limit machine access with a firewall.

For example, when specifying the range of IP address from "192.168.15.1" to "192.168.15.99", the machine cannot be accessed from IP addresses in the range from 192.168.15.100 to 255.



Disabling unused protocols

The protocol setting can be changed on the control panel, in Web Image Monitor, or by using other setting methods. The protocols that can be configured vary depending on the method. Confirm the protocol to configure in page 113 "Protocol Setting Method List" and follow the instruction.



Specifying the security level

You can select from among four security levels combining different protocols, ports, and encryption algorithms. Confirm the description of each level in page 116 "Security Level Setting List".

You can customize the security setting based on the selected level setting to suit your condition.

Limiting Machine Access

Limiting the IP addresses from which devices can access the machine

Specify the range of the IP address that can access the machine.

Important

- **You can limit access from the following protocols.**

  LPR, RCP/RSH, FTP, Bonjour, SMB, WSD (Device), WSD (Printer), IPP, DIPRINT, SNMP, telnet, NBT
- **The machine also limits access from Web Image Monitor.**

1. **Log in to the machine as the network administrator from Web Image Monitor.**

   page 80 "Logging in to the Machine as an Administrator"
2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [Access Control] in the "Security" category.**
4. **In "Access Control Range", click [Active] and specify the range of IP addresses that have access to the machine.**
   - To specify an IPv4 address, enter a range that has access to the machine in [Access Control Range].
   - To specify an IPv6 address, select [Range] or [Mask] in "Access Control Range", and then enter a range that has access to the machine.

- To allow guest users to print directly via Wi-Fi using smart devices, select [Active] for "Access Control for Direct Connection (Group Owner Mode Only)".

5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Limiting machine access with a firewall

You can block machine access and then allow access only from/to the IP addresses specified in reception/transmission filters. Specify sets of an IP address, a port number, and a protocol as filters. You can configure up to five filters each for reception and transmission.

1. **Log in to the machine as the network administrator from Web Image Monitor.**

   page 80 "Logging in to the Machine as an Administrator"
2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [Access Control] in the "Security" category.**
4. **In Access Control Range, click [Active (Firewall)] and specify reception and transmission filters.**

   Specify the following for each reception/transmission filter.

   - IPv4/IPv6 reception filter
     - Remote IP Address: Enter source IP addresses from which to allow incoming communications. To allow incoming communications from all IP addresses, select [All].
     - Local Port Number: Enter a port number on the machine through which to allow incoming communications. To allow incoming communications to all ports, select [All].
     - Protocol: Select a protocol in which to allow communications.
   - IPv4/IPv6 transmission filter
     - Remote IP Address: Enter destination IP addresses to which to allow outgoing communications. To allow outgoing access to all IP addresses, select [All].
     - Remote Port Number: Enter port numbers to which to allow outgoing communications. To allow outgoing communications to all ports, select [All].
     - Protocol: Select a protocol in which to allow communications.

5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Note

- When filters are not configured properly, access to the machine is not possible. In such a case, specify [Inactive] for [Host Interface] ▶ [Access Control Function] on the control panel.

Protocol Setting Method List

You can view the protocol setting methods in the following list:

- 1: Control Panel 2: Web Image Monitor 3: telnet 4: Device Manager NX 5: Remote Communication Gate S

Protocol/Port	Setting method	Function that cannot be used when Protocol/Port is disabled
IPv4 -	1, 2, 3	All applications that operate over IPv4 (IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.)
IPv6 -	1, 2, 3	All applications that operate over IPv6
IPsec -	1, 2, 3	Encrypted transmission using IPsec
FTP TCP:21	2, 3, 4, 5	Transmissions that require FTP
telnet TCP:23	2, 4	Transmissions that require telnet
SMTP TCP:25 (variable)	1, 2, 4, 5	E-mail notification function that requires SMTP reception
HTTP TCP:80	2, 3	Transmissions that require HTTP Print using IPP on port 80
HTTPS TCP:443	2, 3	Transmissions that require HTTP (You can make settings to require SSL transmission only and to reject non-SSL transmission using Web Image Monitor.)
SMB TCP:139	1, 3, 4, 5	Transmissions that require SMB

Protocol/Port	Setting method	Function that cannot be used when Protocol/Port is disabled
TCP:445		
NBT UDP:137/UDP:138	3	SMB print via TCP/IP NetBIOS designated functions on the WINS server
SNMPv1-v2 UDP:161	2, 3, 4, 5	Transmissions that require SNMPv1/v2 (Using Web Image Monitor or telnet, you can specify SNMPv1/v2 to prohibit configuration and make it read-only.)
SNMPv3 UDP:161	2, 3, 4, 5	Transmissions that require SNMPv3 (You can make settings to require SNMPv3 encrypted transmission only and to reject non-SNMPv3 encrypted transmission using Web Image Monitor or telnet.)
RSH/RCP TCP:514	2, 3, 4, 5	Transmissions that require RSH
LPR TCP:515	2, 3, 4, 5	Transmissions that require LPR
IPP TCP:631	2, 3, 4, 5	Transmissions that require IPP
Bonjour UDP:5353	2, 3	Transmissions that require Bonjour
@Remote TCP:7443 TCP:7444	1, 2, 3	RICOH @Remote
DIPRINT TCP:9100	2, 3, 4, 5	Transmissions that require DIPRINT
RFU TCP:10021	1, 2, 3	Remote updating of firmware
WSD (Device) TCP:53000 (variable)	1, 2, 3	Transmissions that require WSD (Device) Note • WS-Discovery (TCP:3702, UDP:3702) also works.
WSD (Printer)	1, 2, 3	Transmissions that require WSD (Printer)

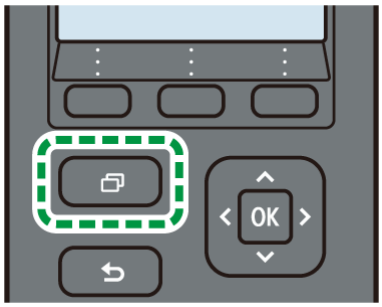
Protocol/Port	Setting method	Function that cannot be used when Protocol/Port is disabled
TCP:53001 (variable)		
LLMNR UDP:5355	2, 3	Name resolution requests using LLMNR

Note

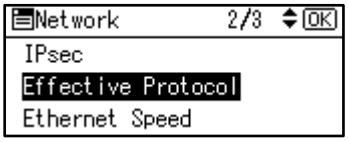
- For details about the telnet command, see "Device Monitoring (TELNET)" on our website.
- For details about the settings in Device Manager NX or Remote Communication Gate S, see the user's manual of each tool.

Disabling Unused Protocols Using the Control Panel

1. **Press the [Menu] key.**



2. **Log in to the machine as the network administrator on the control panel.**
3. **Select [Host Interface], and then press the [OK] key.**
4. **Select [Network], and then press the [OK] key.**
5. **Select [Effective Protocol], and then press the [OK] key.**



6. **Select an unused protocol, and then press the [OK] key.**
7. **Select [Inactive], and then press the [OK] key.**
8. **Repeat Steps 6 and 7 to disable other unused protocols.**
9. **After completing the procedure, press the selection key beneath [Logout].**

Disabling Unused Protocols Using Web Image Monitor

1. **Log in to the machine as the network administrator from Web Image Monitor.**

   page 80 "Logging in to the Machine as an Administrator"
2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [Network Security] in the "Security" category.**
4. **Specify protocols to disable or port numbers to close.**

   Select the security level from the "Security Level" list. You can change the security level of multiple items at the same time. For details about the items changed by the setting of the security level, see page 116 "Security Level Setting List".
5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Security Level Setting List

You can configure security level settings using the control panel. You can select the following security levels:

Important

- **With some utilities, communication or login may fail depending on the network security level.**
- Level 0

  Users can use all features without restriction. Select this when you have no information that needs to be protected from external threats.
- Level 1

  Level 1 is suitable for a connection in an office.
- FIPS 140

  FIPS 140 provides a security strength intermediate between "Level 1" and "Level 2".

  You can only use codes recommended by the U.S. government as its coding/authentication algorithm. Settings other than the algorithm are the same as "Level 2".
- Level 2

  Level 2 is the maximum security that is available in the machine. Select it to protect extremely important information.

For details about the security level settings, see the following list: You can change the setting for a particular function according to the use condition of the machine.

TCP/IP[*1] (✓: Enabled. -: Function is disabled.)

Function	Level 0	Level 1	FIPS 140	Level 2
TCP/IP[*2]	✓	✓	✓	✓
HTTP > Port 80	Open	Open	Open	Open
IPP > Port 80	Open	Open	Open	Open
IPP > Port 631	Close	Close	Close	Close
SSL/TLS > Port 443	Open	Open[*3]	Open[*3]	Open[*3]
SSL/TLS > Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only	Ciphertext Only
SSL/TLS Version > TLS1.3	✓	✓	✓	✓
SSL/TLS Version > TLS1.2	✓	✓	✓	✓
SSL/TLS Version > TLS1.1	✓	-	-	-
SSL/TLS Version > TLS1.0	✓	-	-	-
SSL/TLS Version > SSL3.0	✓	-	-	-
Encryption Strength Setting > AES	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit
Encryption Strength Setting > CHACHA20	256bit	256bit	256bit	256bit
Encryption Strength Setting > 3DES	168bit	-	-	-
Encryption Strength Setting > RC4	-	-	-	-
KEY EXCHANGE	RSA	RSA	RSA	RSA
DIGEST	SHA1	SHA1	SHA1	SHA1
DIPRINT	✓	✓	-	-
LPR	✓	✓	-	-
FTP	✓	✓	✓	✓
RSH/RCP	✓	✓	-	-
TELNET	✓	-	-	-

Function	Level 0	Level 1	FIPS 140	Level 2
Bonjour	✓	✓	-	-
NetBIOS over TCP/IPv4	✓	✓	-	-
WSD (Device)	-	-	-	-
WSD (Printer)	✓	✓	✓	✓
WSD (Encrypted Communication of Device)	-	-	✓*4	✓*4

*1 The same settings are applied to IPv4 and IPv6.

*2 TCP/IP setting is not controlled by the security level. Specify manually whether to enable or disable this setting.

*3 IPP-SSL Communication is enabled under Windows 10 or later.

*4 This is enabled under Windows 10 or later.

SNMP (✓: Enabled -: Disabled)

Function	Level 0	Level 1	FIPS 140	Level 2
SNMP	✓	✓	✓	✓
Permit Settings by SNMPv1 and v2	✓	-	-	-
SNMPv1, v2 Function	✓	✓	-	-
SNMPv3 FUNCTION	✓	✓	✓	✓
Permit SNMPv3 Communication	Encryption/Cleartext	Encryption /Cleartext	Encryption Only	Encryption Only

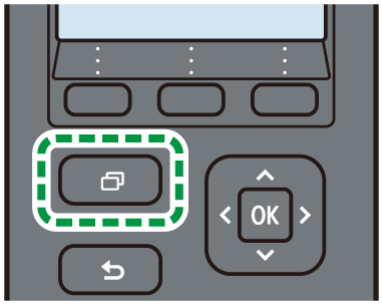
TCP/IP Encryption Strength Setting

Function	Level 0	Level 1	FIPS 140	Level 2
IPsec	-	-	-	-
IEEE 802.1X (Wired)	-	-	-	-
IEEE 802.1X (Wired)>Authentication Method	-	-	-	-
SNMPv3 > Authentication Algorithm	MD5	SHA1	SHA1	SHA1
SNMPv3 > Encryption Algorithm	DES	DES	AES-128	AES-128

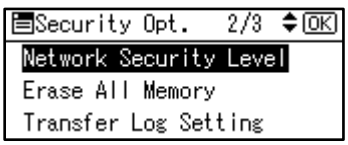
Function	Level 0	Level 1	FIPS 140	Level 2
Kerberos Authentication > Encryption Algorithm	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1/RC4-HMAC/DES-CBC-MD5	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1/RC4-HMAC	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96
Driver Encryption Key > Encryption Strength Setting	Simple Encryption	DES	AES	AES

Specifying the Security Level

1. **Press the [Menu] key.**



2. **Log in to the machine as the network administrator on the control panel.**
3. **Select [Security Options], and then press the [OK] key.**
4. **Select [Network Security Level], and then press the [OK] key.**



If the confirmation screen appears, press the selection key beneath [Exit].

5. **Select the security level, and then press the [OK] key.**

Select a security level from among Level 0, Level 1, Level 2, and FIPS140.

For the security levels, see page 116 "Security Level Setting List".

6. **Press the selection key beneath [Logout].**

Encrypting Network Communication

To protect communicated information, it is necessary to encrypt communication between computers and external equipment.

Data sent from and received by the machine can be intercepted, cracked, or tampered with during transmission. For example, the following data can be transmitted between the machine and external devices or the computer:

- Documents printed in the company using the printer driver
- Login user name and login password

See the table below for the methods of encrypting data.

Data to encrypt	Encryption method	Process/Reference
Web Image Monitor IPP print Windows authentication LDAP authentication	SSL/TLS	Install a device certificate. 1. Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority 2. Encrypting Transmission Using SSL/TLS
Machine management data	SNMPv3	Specify an encryption password. • Encrypting Data Communicated with Machine Management Software Via SNMPv3
Authentication information of print jobs	Driver encryption key IPP authentication	Specifying a Driver Encryption Key Specify IPP authentication. • Encrypting the Login Password of Print Jobs
Kerberos authentication data	Varies depending on the KDC server	Select an encryption method. • Encrypting Communication Between KDC and the Machine

Important

- **The administrator is required to manage the expiration of certificates and renew the certificates before they expire.**
- **The administrator is required to check that the issuer of the certificate is valid.**

Installing a Self-signed Certificate/Certificate Issued by a Certificate Authority

To encrypt communication with the machine, install a device certificate.

Two types of device certificates can be used: a self-signed certificate created by the machine and a certificate issued by a certificate authority. When you need higher reliability, use a certificate issued by a certificate authority.



EBS680

1. **Log in to the machine as the network administrator from Web Image Monitor.**

   page 80 "Logging in to the Machine as an Administrator"

2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [Device Certificate] in the "Security" category.**
4. **On the "Device Certificate" screen, install a self-signed certificate or certificate issued by a certificate authority by following the instructions below:**

   To install a self-signed certificate

   Create and install a self-signed certificate.

   1. Select the number from the list to create a self-signed certificate.
   2. Click [Create] to specify the necessary settings.

      Common Name: Enter the name of the device certificate to create. You must enter a name.

      Specify "Organization", "Organizational Unit", and other items as necessary.
   3. Click [OK].

      A message appears while settings are being done. You may need to wait a short time before proceeding to the next step.
   4. Click [OK].

      "Installed" is displayed in [Certificate Status].

   To install a certificate issued by a certificate authority

   Request a device certificate from a certificate authority and install it. Follow the same steps to install an intermediate certificate.

   1. Select the number from the list to create a device certificate.
   2. Click [Request] to specify the necessary settings.
   3. Click [OK].

      A message appears while settings are being done. You may need to wait a short time before proceeding to the next step.

4. Click [OK].

   "Requesting" is displayed in "Certificate Status".

5. Apply to the certificate authority for the device certificate.

   You cannot apply to the certificate authority from Web Image Monitor. The application procedure varies depending on the certificate authority. For details, contact the certificate authority.

   For the application, click the Details icon and use the information that appears on the "Certificate Details" screen.

   The issuing location may not be displayed if you request multiple certificates at the same time. When you install a certificate, be sure to check the certificate destination and installation procedure.

6. After the device certificate has been issued by the certificate authority, select the number of the issued certificate from the list on the "Device Certificate" screen, and then click [Install].

7. Enter the contents of the device certificate in the entry fields.

   To install the intermediate certificate at the same time, enter also the contents of the intermediate certificate.

   If an intermediate certificate issued by a certificate authority is not installed, an alert message is displayed during network communication. When an intermediate certificate has been issued by a certificate authority, you must install the intermediate certificate.

8. Click [OK].

   "Installed" is displayed in "Certificate Status".

5. **After completing the installation, select the certificate for each application on "Certification".**
6. **Click [OK].**

   A message appears while settings are being done. You may need to wait a short time before proceeding to the next step.

7. **Click [OK].**
8. **Log out of the machine, and then exit the Web browser.**

Note

- To print data in the machine using IPP-SSL, the user must install a certificate in the computer. Select [Trusted Root Certification Authorities] for the certificate store location when accessing the machine by IPP.
- To change [Common Name] of the device certificate when using the Windows standard IPP port, delete any previously configured PC printer beforehand and install the printer driver again. Also, to change the user authentication settings (login user name and password), delete any previously configured PC printer beforehand, change the user authentication settings, and then install the printer driver again.

- On Web Image Monitor, you can upload created device certificates as well. Device certificates in the following file formats are supported. For details about uploading, see Web Image Monitor Help.
  - PKCS#12
  - PEM

Encrypting Transmission Using SSL/TLS

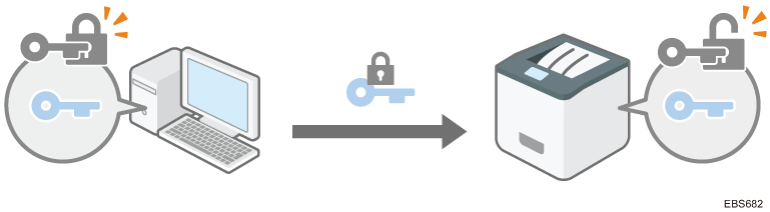
SSL (Secure Sockets Layer) /TLS (Transport Layer Security) is a method to encrypt network communications. SSL/TLS prevents data from being intercepted, cracked, or tampered.

Flow of SSL/TLS encrypted communications

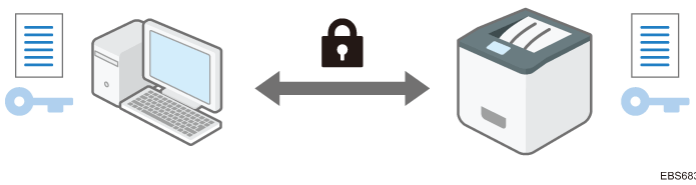
1. The user's computer requests the SSL/TLS device certificate and public key when accessing the machine.
2. The device certificate and public key are sent from the machine to the user's computer.



3. The shared key created on the computer is encrypted using the public key, sent to the machine, and then decrypted using the private key in the machine.



4. The shared key is used for data encryption and decryption, thus achieving secure transmission.



- To enable encrypted communication, install a device certificate in the machine in advance.
- To encrypt communication using SSL/TLS, enable SSL/TLS as follows:

Note

- To check whether SSL/TLS configuration is enabled, enter "https://(the machine's IP address or host name)/" in your Web browser's address bar to access this machine. If the "The page cannot be displayed" message appears, check the configuration because the current SSL/TLS configuration is invalid.
- If you enable SSL/TLS for IPP (printer functions), sent data is encrypted, preventing it from being intercepted, analyzed, or tampered with.

Enabling SSL/TLS

1. **Log in to the machine as the network administrator from Web Image Monitor.**
   page 80 "Logging in to the Machine as an Administrator"
2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [SSL/TLS] in the "Security" category.**
4. **Select the protocol to enable encrypted communication on "SSL/TLS" to specify the details about the communication method.**
   - Permit SSL/TLS Communication: Select one of the encryption communication modes below, and then specify whether to activate HSTS. To activate HSTS, specify the max-age attribute in the range of 0 to 31,536,000 seconds as well. While HSTS is activated, HTTPS communication is automatically used for connections from the Web browser to the machine. The max-age attribute is renewed every time Web Image Monitor and HSTS remains active for the same period.
     - Ciphertext Priority: Performs encrypted communication when a device certificate has been created. If encryption is not possible, the machine communicates data in clear text.
     - Ciphertext/Cleartext: Performs encrypted communication when connecting to the machine using an "https" address from a Web browser. Communicates in clear text when connecting to the machine using an "http" address.
     - Ciphertext Only: Allows encrypted communication only. If encryption is not possible for some reason, the machine cannot communicate. If this is the case, change the communication mode to [Ciphertext/Cleartext] in [Host Interface] ▶ [Network] ▶ [Permit SSL/TLS Comm.] temporarily, and then check the settings.
   - SSL/TLS Version: Specify TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0 to enable or disable. At least one of these protocols must be enabled.
   - Encryption Strength Setting: Specify the encryption algorithm to apply to AES, CHACHA20, 3DES, and RC4. You must select at least one check box.
   - KEY EXCHANGE: Specify whether to enable or disable exchanging of the RSA key.
   - DIGEST: Specify whether to enable or disable SHA1 DIGEST.

5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**
7. **To encrypt communications with the SMTP server, use the following procedure to change [Use Secure Connection (SSL)] to [SMTP over SSL] or [STARTTLS].**

Note

- To use HSTS, a certificate issued by a certificate authority must be installed.
- While HSTS is active, selecting "Close" for "Port 443" of "SSL/TLS" on the "Network Security" screen makes Web Image Monitor inaccessible.
- Depending on the states you specify for TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0, the machine might not be able to connect to an external LDAP server.

Enabling SSL for SMTP connection

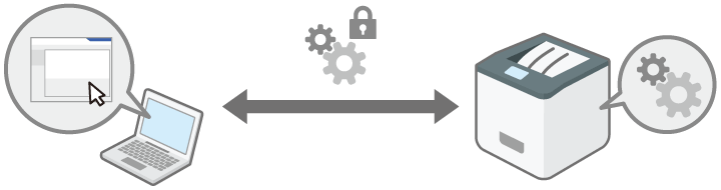
1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [Email] in the "Device Settings" category.**
4. **In "SSL" under "SMTP", select [SMTP over SSL] or [STARTTLS].**
   - Selecting [SMTP over SSL] changes the port number to 465, and selecting [STARTTLS] changes it to 578.
   - When [Auto Select] is specified, the encryption method is determined based on the port number.
   - When a number other than 465 or 578 is specified for the port number, encryption using STARTTLS is attempted, but if it fails, the communication is encrypted using SMTP over SSL.
5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Note

- When SSL is enabled in the SMTP server, e-mails are always sent via the SMTP server.

Encrypting Data Communicated with Machine Management Software via SNMPv3

When monitoring devices using Device Manager NX via a network, you can encrypt the transmitted data by using the SNMPv3 protocol.



EBS684

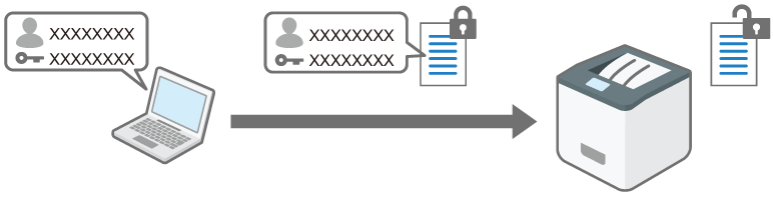
1. **Log in to the machine as the network administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [Network Security] in the "Security" category.**
4. **In "Permit SNMPv3 Communication" of "SNMP", click [Encryption Only].**
5. **Click [OK] and exit the Web browser.**

Note

- To change the settings specified in the machine from Device Manager NX, specify an encryption password to the network administrator in [Program/Change Administrator], and then register the encryption password in the SNMP account of Device Manager NX.
- If network administrator's [Encryption Password] setting is not specified, the data for transmission may not be encrypted or sent. For details about specifying the network administrator's Encryption Password setting, see page 82 "Adding Built-in Administrators or Changing the Privileges".

Encrypting the Login Password of Print Jobs

You can encrypt the login password for the printer driver and the password for IPP printing to increase security against password cracking.



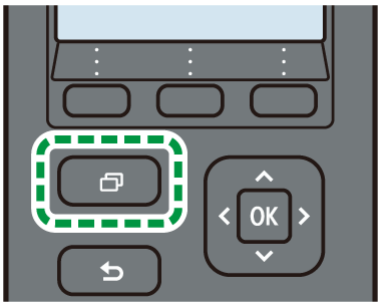
EBS685

- To perform printing from a LAN inside the office, specify the driver encryption key.
- To perform IPP printing from an external network, encrypt the password of IPP printing.

Specifying a Driver Encryption Key to Encrypt Passwords

Specify the driver encryption key specified in the machine also to the printer driver to encrypt and decrypt passwords.

1. **Press the [Menu] key.**



2. **Log in to the machine as the network administrator on the control panel.**
3. **Select [Security Options], and then press the [OK] key.**
4. **Select [Extended Security], and then press the [OK] key.**
5. **Select [Driver Encryption Key], and then press the [OK] key.**
6. **Press the selection key beneath [Enter].**
7. **Enter the driver encryption key, and then press the [OK] key.**

   Enter the driver encryption key using up to 32 alphanumeric characters.
8. **Repeat Steps 6 and 7 to re-enter the driver encryption key.**
9. **Press the selection key beneath [Logout].**
10. **The network administrator must give users the driver encryption key specified on the machine so they can register it on their computers.**
    - Make sure to enter the same driver encryption key as that specified on the machine.
    - When using a PCL 6 printer driver, you can enter the driver encryption key on [Printer Properties] ▶ the [Advanced Options] tab ▶ [User Authentication].

Note

- For details about specifying the encryption key on the printer, see the driver help.

Encrypting the password of IPP printing

When printing using the IPP protocol, specify the authentication method to [DIGEST] to encrypt the IPP authentication password. Register the user name and password for IPP authentication separately from the user information in the Address Book.

1. **Log in to the machine as the network administrator from Web Image Monitor.**

page 80 "Logging in to the Machine as an Administrator"

2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [IPP Authentication] in the "Security" category.**
4. **Select [DIGEST] in "Authentication".**
5. **Enter User Name and Password.**
   - Click [On] of "User Authentication Function of Main Unit" to use the user authentication information specified on the machine instead of the username and password for IPP authentication.
6. **Click [OK].**

   A message appears while settings are being done. You may need to wait a short time before proceeding to the next step.
7. **Click [OK].**
8. **Log out of the machine, and then, exit the Web browser.**

Encrypting Communication Between KDC and the Machine

You can encrypt communications between the machine and the Key Distribution Center (KDC) server when using Kerberos authentication with Windows or LDAP authentication to secure communication.

The supported encryption algorithm differs depending on the type of KDC server.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**

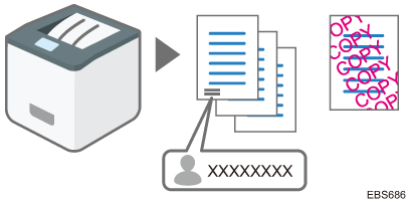
   page 80 "Logging in to the Machine as an Administrator"
2. **Click [Configuration] on the [Device Management] menu.**
3. **Click [Kerberos Authentication] in the "Device Settings" category.**
4. **Select the encryption algorithm to enable.**
   - Only Heimdal supports DES3-CBC-SHA1.
   - To use DES-CBC-MD5 in the Windows Server operating system, enable it in the operating system settings.
5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Preventing Information Leaks

Taking Measures to Prevent Information Leaks

Information leaks may be caused by loss of documents or data, or by human error. The information asset in the machine will be safer by decreasing these problems and promoting user awareness of file management.

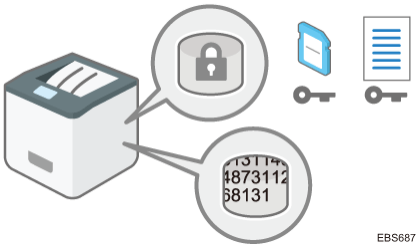
Specifying the function to avoid leaving documents or unauthenticated copies



- To avoid leaving printed documents in the machine, specifies to print the name of the user who performed printing on the output sheet or to use the control panel to perform printing.
- Specifies also to print embedded text to warn of unauthorized copying.

page 130 "Preventing Data Leaks from Printed Sheets"

Encrypting data in the internal storage or deleting data by overwriting



The internal storage of the machine stores all data about documents and users in the Address Book. The data in the internal storage can be encrypted or temporary data can be deleted by overwriting to avoid restoring the data.

page 132 "Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine"

Note

- See also the sections below on how to prevent information leaks:

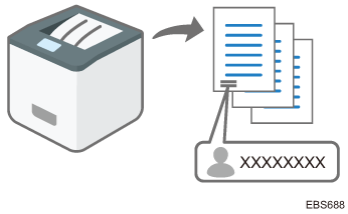
page 136 "Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator"

Preventing Data Leaks from Printed Sheets

Confidential or private information printed on paper may be copied improperly or stolen, leading to data leaks.

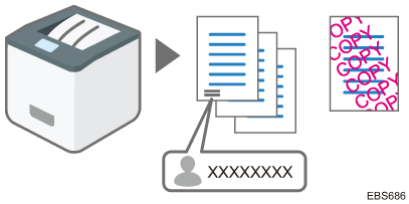
The following functions in the machine can promote user awareness of file management and discourage unauthorized copying or leaving of printed sheets.

Adding the name of the user printing the job on printed sheets (Compulsory Security Stamp)



Always adding a printed name can promote user awareness of file management.

Warning unauthorized copying (Unauthorized Copy Prevention/Data Security for Copying)



You can embed special text to the documents printed using the machine to prevent unauthorized copying. You can configure to use this function without user operation.

Specifying the Compulsory Security Stamp Function

Specify the location to stamp user information such as a login user name.

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [Compulsory Security Stamp] in the "Device Settings" category.**
4. **Select [On] in "Compulsory Security Stamp", and then specify the stamp information and position.**
    - [Date/Time]: Prints the job output time.
    - [Printout User Name]:
        - [Stamp User Name]: Prints the name in the address book.
        - [Stamp Login User Name]: Prints the user code or login user name in the authentication information in the address book.

- [Machine ID]: Prints the serial number of the machine. You can check the serial number in [Status/Information] ▶ [Device Info] ▶ [System] ▶ [Machine ID].
- [IP Address]: Prints the IP address of the machine.
- Stamp Position: Select the stamp position.
- Adjust Stamp Position: Enter a value or adjust the position by pressing the arrow button.

5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Specifying the Unauthorized Copy Prevention Function

1. **Log in to the machine as the machine administrator from Web Image Monitor.**
2. **Click [Configuration] from the [Device Management] menu.**
3. **Click [Unauthorized Copy Prevention: Printer] in the "Device Settings" category.**
4. **Specify the unauthorized copy prevention function.**
    - Unauthorized Copy Prevention Setting: Specify whether to enable unauthorized copy prevention.
        - On:

          Enables the unauthorized copy prevention function specified in the machine regardless of the settings on the printer driver.
        - Off:

          Disables the unauthorized copy prevention function specified in the machine. If the unauthorized copy prevention function is specified in the printer driver, the machine performs print jobs according to the specified settings.
    - Compulsory Unauthorized Copy Prevention: Select the contents of unauthorized copy prevention and their priority.
        - Driver/Command:

          The added pattern is not printed. Specify the unauthorized copy prevention function on the control panel or in the printer driver as necessary.
        - Driver/Command (Most Settings):

          The settings specified in the machine are applied to the mask type for pattern, color, and density, and the settings specified on the control panel or in the printer driver are applied to the other items.
        - Machine Setting(s):

          The settings specified in the machine are applied to printing.

- Unauthorized Copy Prevention Type: Select the type of unauthorized copy prevention.
  - Data Security for Copying:

    Protects documents by printing a gray pattern when making unauthorized copies.
  - Unauthorized Copy Prevention for Pattern:

    Adds text or a pattern to unauthorized copies of documents. When you select an unauthorized copy prevention pattern, you need to specify the effect, mask pattern, density, and so on.
- Mask Type for Pattern: Select from among 11 types.
- Pattern Color: Select a color from among Black, Cyan, and Magenta.
- Pattern Density: Select one of 5 levels of gradation.
- Data Security for Copying Effect: Specify a combination of text and a pattern.
- Unauthorized Copy Prevention of Patterns Effect: Specify a combination of text and a pattern.
- Text Selection: Select a text string for Text Selection from among the standard text strings such as User Name, Date & Time, custom text, or "Do not copy". You can specify the font, point size, text position, and angle for the selected text string, as well as whether to repeat the selected text string. When repeating the selected text string, you can also specify the carriage return space.

5. **Click [OK].**
6. **Log out of the machine, and then exit the Web browser.**

Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine

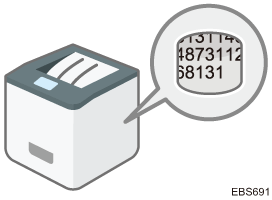
By encrypting data on the internal storage of the machine, you can prevent possible data leaks when you replace or dispose of the machine, or even if the machine were to be stolen.

Encrypting data on the internal storage



Encryption is an effective measure against data leaks. Be sure to keep the encryption key secure to use for decryption. Print it on a sheet or save it to a USB flash memory device.

Overwriting data to prevent restoration



You can delete data that you do not want to be restored. The Erase All Memory function deletes all data and initializes the internal storage of the machine.

Encrypting Data on the Internal Storage

You can encrypt data contained in the Address Book, authentication information, and stored documents to prevent data leaks in case the internal storage is removed from the machine.

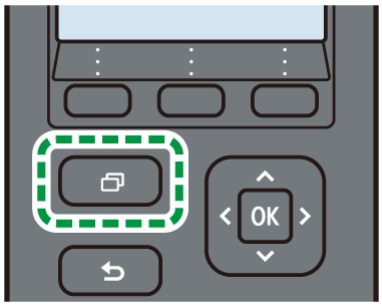
Once encryption is enabled, all data subsequently stored on the machine will be encrypted.

The encryption algorithm used in the machine is AES-256.

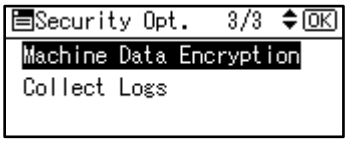
Important

- **The machine cannot be operated while encrypting data or canceling encryption.**
- **Do not turn off the power of the machine while encrypting data or canceling encryption. If you turn off the power, the internal storage may be damaged and all data may be unusable.**
- **After completing this procedure on the machine's control panel, turn off the main power and restart the machine to enable the new settings by turning it back on. Restarting can be slow when there is data to be carried over to the internal storage.**
- **The process for encrypting the internal storage takes several minutes.**
- **The encryption key is required for data recovery or migration to another machine. Be sure to keep the encryption key secure by printing it on a sheet.**
- **To transfer data from the machine to another machine, you must decrypt the encrypted data. Contact your service representative for data migration.**
- **If you specify both the Erase All Memory function and the encryption function, the Erase All Memory function is performed first. Encryption starts after the Erase All Memory function has been completed and the machine has been rebooted.**

1. **Press the [Menu] key.**



2. **Log in to the machine as the machine administrator on the control panel.**
3. **Select [Security Options], and then press the [OK] key.**
4. **Select [Machine Data Encryption], and then press the [OK] key.**



5. **Make sure that [Encrypt] is selected, and then press the [OK] key.**
6. **Press the selection key beneath [PrtOnPpr].**



7. **Press the selection key beneath [Print].**

   The encryption key is printed on paper.
8. **Press the selection key beneath [Continue].**
9. **Press the selection key beneath [Exit].**
10. **Press the selection key beneath [Logout].**
11. **Turn off the main power of the machine, and then turn it back on.**

    When the main power is turned on, the machine starts to convert the data on the memory. Wait until the message "Memory conversion complete. Turn the power switch off." appears. After that, turn off the main power again.

Initializing the Machine with the Erase All Memory Function

Overwrite and erase all data stored on the internal storage when you relocate or dispose of the machine. The device settings stored on the machine's memory are initialized.

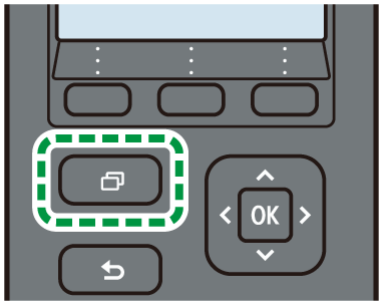
For details about using the machine after executing Erase All Memory, contact your service representative.

Important

- **If the main power switch is turned off before the Erase All Memory process is completed, overwriting will be stopped and data will be left on the internal storage. Do not stop the overwrite mid-process. Doing so will damage the internal storage.**
- **Before you start the Erase All Memory process, we recommend that you back up the user codes, the counters for each user code, and the Address Book. You can back up the user codes and the counters for each user code using Device Manager NX. For details, see Device Manager NX Help. You can back up the Address Book using Web Image Monitor.**

  See Making a Backup or Restoring the Address Book, User Guide in English.
- **If the method of Random Numbers is selected and overwrite three times is set, the Erase All Memory process takes up to 35 minutes. You cannot operate the machine during overwriting.**
- **The Erase All Memory function also clears the machine's security settings, so that neither machine nor user administration will be possible. Ensure that users do not save any data on the machine after the Erase All Memory process is completed.**

1. **Press the [Menu] key.**



2. **Log in to the machine as the machine administrator on the control panel.**
3. **Select [Security Options], and then press the [OK] key.**
4. **Select [Erase All Memory], and then press the [OK] key.**



5. **Select the method of erasing the data.**

   The default method for overwriting is "Random Numbers", and the default number of overwrites is 3.

   - NSA[*1]: Overwrites data twice with random numbers and once with zeros.
   - DoD (5220.22-M)[*2]: Overwrites data with a random number, then with its complement, then with another random number, and the data is verified.

- Random Numbers: Overwrites data multiple times with random numbers. Select the number of overwrites from one to nine.
- BSI/VSITR: Overwrites data seven times with the fixed value (for example: 0x00).
- Secure Erase (ATA): Overwrites data three times with random numbers.
- Format: Formats the internal storage. Data is not overwritten.

*1 National Security Agency (U.S.A)

*2 Department of Defense (U.S.A)

6. **Press the selection key beneath [Yes].**

   Depending on the method of erasing selected in Step 5, [Yes] may not appear.The machine restarts automatically, and then overwriting starts.

7. **When overwriting is completed, press the selection key beneath [Exit]**

Note

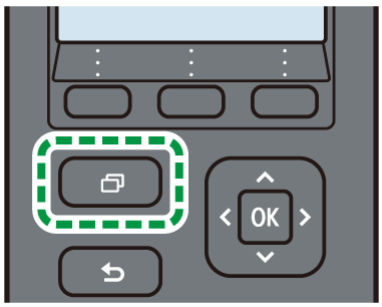
- If the main power of the machine is turned off before the [Erase All Memory] process is completed, overwriting will start over when the main power is turned back on.
- If an error occurs before overwriting is completed, turn off the main power of the machine. Turn it back on, and then repeat from Step 1.
- To print the erase result, select [Security Options] ▶ [Erase All Memory] ▶ [Print Erase All M. Report].

Restricting Operations of the Customer Engineer without the Supervision of the Machine Administrator

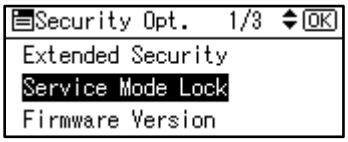
You can restrict the customer engineer's access to the service mode when performing inspection or repair.

A customer engineer needs permission from the machine administrator to use the service mode. This ensures that the machine cannot be operated without the supervision of the machine administrator.

1. **Press the [Menu] key.**



2. **Log in to the machine as the machine administrator on the control panel.**
3. **Select [Security Options], and then press the [OK] key.**
4. **Select [Service Mode Lock], and then press the [OK] key.**



5. **Select [On], and then press the [OK] key.**
6. **Press the selection key beneath [Yes].**
7. **Press the selection key beneath [Logout].**

6. Specifications

Paper Specifications

Recommended Paper Sizes and Types

The recommended paper sizes and types for each tray are as described below.

Note

- When performing multiple sheet feeding, fan sheets thoroughly or load sheets one by one from the bypass tray.
- The printing speed may be lower depending on the paper size or paper type.
- For details about specifying the paper size and custom paper size, see page 25 "Specifying the Paper Size" and page 25 "Specifying a Custom Size Paper Using the Control Panel".

Tray 1

Paper type and weight	Paper size	Paper capacity
Thin Paper to Thick Paper 2 60 to 200 g/m^2 (Approx. 16 to 53 lb.)	• Specify the paper size in [Paper Input]: A4□, A5□, A6□, B5 JIS□, B6 JIS□, 8^1/$_2$ × 11□, 7^1/$_4$ × 10^1/$_2$□, 5^1/$_2$ × 8^1/$_2$□, 16K□ • Custom size: 98.0 to 216.0 mm in width, 148.0 to 297.0 mm in length (3.86 to 8.50 inches in width, 5.83 to 11.69 inches in length)	250 sheets (80 g/m^2, 20 lb., Paper Thickness 100µm)
Envelope	Specify the paper size in [Paper Input]: 4^1/8 × 9^1/$_2$□, 3^7/8 × 7^1/$_2$□, C5 Env□, C6 Env□, DL Env□	The maximum number of sheets that can be loaded may vary depending on the thickness and condition of the paper. Make sure the paper stack does not exceed the upper limit mark.

Tray 2, 3 (optional trays)

Note

- For details about the names and the abbreviated names of the options described in this manual, see the following.

  page 5 "Abbreviated Names of Options"

Paper type and weight	Paper size	Paper capacity
Thin Paper to Thick Paper 2 60 to 200 g/m^2 (Approx. 16 to 53 lb.)	• Specify the paper size in [Paper Input]: A4□, A5□, B5 JIS□, 8^1/$_2$ × 14□, 8^1/$_2$ × 13□, 8^1/$_2$ × 11□, 8^1/$_4$ × 13□, 8 × 13□, 7^1/$_4$ × 10^1/$_2$□, 5^1/$_2$ × 8^1/$_2$□, 16K□, 8^1/$_2$ × 12□, 8^1/$_2$ × 13^3/$_5$□ • Custom size: 139.7 to 216.0 mm in width, 210.0 to 356.0 mm in length (5.50 to 8.50 inches in width, 8.27 to 14.01 inches in length)	500 sheets (80 g/m^2, 20 lb., Paper Thickness 100µm) 1 sheet (for label paper (adhesive labels))

Bypass Tray

Paper type and weight	Paper size	Paper capacity
60 to 200 g/m^2 (Approx. 16 to 53 lb.) Plain Paper 1	• Specify the paper size in [Paper Input]: A4□, A5, A6□, B5 JIS□, B6 JIS, 8^1/$_2$ × 14□, 8^1/$_2$ × 13□, 8^1/$_2$ × 11□, 8^1/$_4$ × 14□, 8^1/$_4$ × 13□, 8 × 13□, 7^1/$_4$ × 10^1/$_2$□, 5^1/$_2$ × 8^1/$_2$, 16K□, 8^1/$_2$ × 12□, 8^1/$_2$ × 13^2/$_5$□ • Custom size: 76.2 to 216.0 mm in width, 127.0 to 356.0 mm in length (3.00 to 8.50 inches in width, 5.00 to 14.01 inches in length)	50 sheets (80 g/m^2, 20 lb., Paper Thickness 100µm) 5 sheets (for Thick Paper 2)

Paper type and weight	Paper size	Paper capacity
Envelope	Specify the paper size in [Paper Input]: $4^1/8 \times 9^1/_2$□, $3^7/8 \times 7^1/_2$□, C5 Env□, C6 Env□, DL Env□	The maximum number of sheets that can be loaded may vary depending on the thickness and condition of the paper. Make sure the paper stack does not exceed the upper limit mark.

Notes on Special Paper

Paper Type	Note
Setting thick paper	page 144 "Thick Paper Recommended Status"
Setting envelopes	page 144 "Envelope Orientation and Recommended Status"
Setting letterhead paper	page 145 "Loading Orientation-fixed Paper or Two-sided Paper"
Setting label paper (adhesive labels)	• We recommend that you use specified label paper. If paper other than the specified one is used, normal operation and quality cannot be guaranteed. • When using the optional paper feed unit (Trays 2 and 3), load sheets of label paper (adhesive labels) one at a time.
Setting coated paper	• Specify [Coated Paper] in [Paper Input] ▶ [Paper Type: (tray name)], and specify the appropriate paper thickness. • If a paper jam occurs or if the machine makes a strange noise, feed the coated paper from the bypass tray one sheet at a time.

Paper Thickness for Each Paper Weight

Paper Thickness	Minimum paper thickness	Maximum paper thickness
Thin Paper	60 g/m^2 (Approx. 16 lb. Bond)	65 g/m^2 (Approx. 17 lb. Bond)

Paper Thickness	Minimum paper thickness	Maximum paper thickness
Plain Paper 1	66 g/m^2 (Approx. 18 lb. Bond)	74 g/m^2 (Approx. 20 lb. Bond)
Plain Paper 2	75 g/m^2 (Approx. 20 lb. Bond)	90 g/m^2 (Approx. 24 lb. Bond)
Middle Thick	91 g/m^2 (Approx. 24 lb. Bond)	128 g/m^2 (Approx. 34 lb. Bond)
Thick Paper 1	129 g/m^2 (Approx. 34 lb. Bond)	163 g/m^2 (Approx. 43 lb. Bond)
Thick Paper 2	164 g/m^2 (Approx. 44 lb. Bond)	200 g/m^2 (Approx. 53 lb. Bond)

Unusable Paper

⚠CAUTION

- Do not use stapled sheets of paper, aluminum foil, carbon paper, or any kind of conductive paper. Doing so can result in fire.

Paper causing faults

Do not use any of the following kinds of treated paper. Doing so may cause faults.

- Paper for inkjet printers
- Thermal paper
- Art paper
- Aluminum foil
- Carbon paper
- Conductive paper
- Paper with perforated lines
- Hemmed-edge paper
- Window envelopes
- Tab stock
- OHP transparencies
- Translucent paper

Do not print onto sides that are already printed.

Paper causing paper jam

Do not use the following kinds of paper. It may cause a paper jam.

- Bent, folded, or creased paper
- Perforated paper
- Slippery paper
- Torn paper
- Rough paper
- Thin paper with little stiffness
- Paper with a dusty surface

Do not load sheets that have already been printed onto by another machine. Doing so may interfere with loading of paper because the powder for preventing offset may attach to the paper roller.

If you use paper curled by humidity or drying, the paper may jam.

Note

- A paper jam may occur depending on the condition of the paper even when using the recommended paper.

Paper Storage

When storing paper, the following precautions should always be followed:

- Do not store paper where it will be exposed to direct sunlight.
- Store paper in a dry environment (humidity: 70% or less).
- Store on a flat surface.
- Do not store paper vertically.
- Once opened, store paper in a plastic bag.

Saving Printouts

- Prints will fade if exposed to strong light or dampness and humidity for extended periods of time. Preserve the quality of your copies by storing them in a binder in a dark, dry place.
- When folding prints, toner in the folds will come off.
- If the prints are stored in the conditions described below, toner may melt:
  - When a print and a half-dried print are put on top of each other
  - When solvent-type adhesive agents are used for pasting prints
  - When prints are placed on mats made of chlorinated plastic in locations of high temperature for long periods of time

- When prints are placed in locations of extremely high temperatures, such as near a heater

Thick Paper Recommended Status

When loading thick paper of 129-200 g/m^2 (Approx. 34-53 lb. Bond) in the paper trays, or in the bypass tray, follow the recommendations below to prevent misfeeds and loss of image quality.

Paper Storage

- Temperature: 20–25°C (68–77°F)
- Humidity: 30–65%.

Do not use together paper that has been stored in different environments.

Note

- When printing on thick, smooth paper, be sure to fan the paper thoroughly before loading. If you do not fan thick paper, jams and misfeeds can occur. If paper continues to become jammed or feed in together even after they are fanned, load them one by one from the bypass tray.
- Proper performance and quality may not be achieved under the recommended conditions depending on the paper.
- The printed sheet may curl. If the printed sheet curls, correct it.

Envelope Orientation and Recommended Status

The way to load envelopes varies depending on the shape and orientation of the envelopes.

Important

- **Do not print on the following envelopes:**
  - **Window envelopes**
  - **Envelopes with moisture**

Before setting envelopes

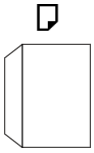
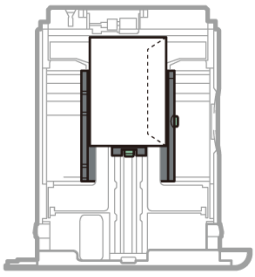
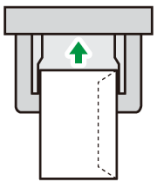
Before loading envelopes, press down on them to remove any air from inside and flatten out all four edges. If they are bent or curled, flatten their leading edges (the edge going into the machine) by running a pencil or ruler across them.

Note

- For information about recommended envelopes, contact your local dealer.
- The Duplex function cannot be used with envelopes.

- Set the margins on the top and bottom to be 15 mm or more, and set the left and right to be 10 mm or more, so as to print with adequate quality.
- An image may not be printed clearly on a sheet whose thickness is uneven. Print a few sheets and check the result.
- The printing result may not be adequate or the envelope may become wrinkled when the temperature or humidity is high.
- The printing result may not be adequate or output envelopes may become wrinkled depending on the printing environment even when using the recommended envelopes.
- When printing onto paper other than an envelope after printing onto several envelopes, you may have to wait about one minute until printing starts to allow the machine to make adjustments.

Procedure for Loading Envelopes

Orientation of Envelopes	Tray 1	Bypass Tray
Side-opening envelopes 	 Flaps: closed Side to be printed: face up Bottom side of envelopes: toward the left of the machine	 Flaps: closed Side to be printed: face up Bottom side of envelopes: toward the left of the machine

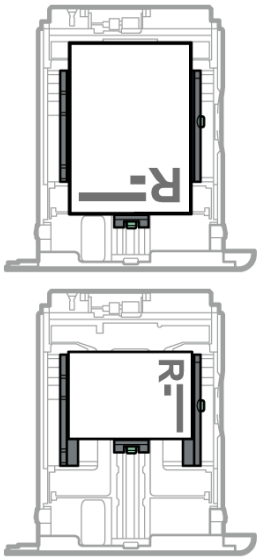
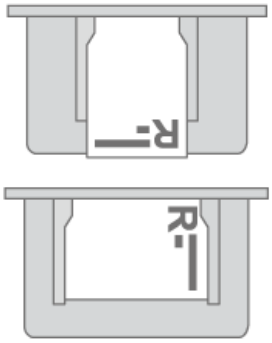
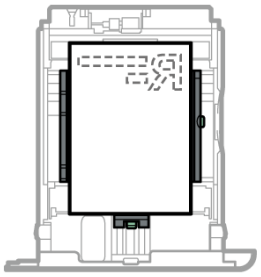
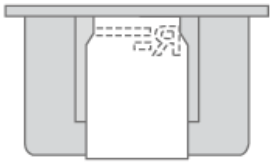
Loading Orientation-fixed Paper or Two-sided Paper

To print onto letterhead paper or business letter paper on which logos or patterns are printed, confirm how to set the paper or the settings of this machine so that the original is printed onto the orientation-fixed (top to bottom) or two-sided paper correctly.

Before you print on letterhead paper from the printer driver, specify the machine settings as follows.

[Print Settings] ▶ [Machine Modes] ▶ Letterhead Setting ▶ [Auto Detect]

Paper Orientation

Copy Side	Tray 1-3	Bypass Tray
One-sided originals		
Two-sided originals		

Note

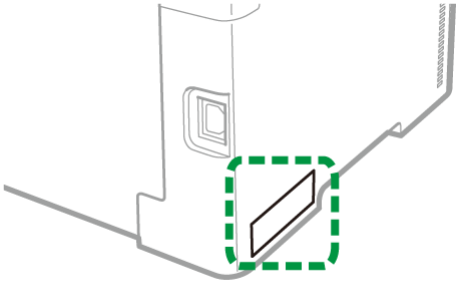
- When you set [Letterhead Setting] to [On (Always)], you can print onto letterhead paper when the paper type in the printer driver's settings is set to [Letterhead].
- If a print job is changed partway through printing from one-sided to two-sided printing, one-sided output after the first copy may be printed facing a different direction. To ensure all paper is output facing the same direction, specify different input trays for one-sided and two-sided printing. Note also that two-sided printing must be disabled for the tray specified for one-sided printing.

Machine and Options Specifications

Model-Specific Information

This section explains how you can identify the region your machine belongs to.

There is a label on the rear of the machine, located in the position shown below. The label contains details that identify the region your machine belongs to. Read the label.



The following information is region-specific. Read the information under the symbol that corresponds to the region of your machine.

Region A (mainly Europe and Asia)

If the label contains the following, your machine is a region A model:

- CODE XXXX -27, -25, -29, -21
- 220–240 V

Region B (mainly North America and Taiwan)

If the label contains the following, your machine is a region B model:

- CODE XXXX -17, -19
- 120-127 V (mainly North America)
- 110 V (Taiwan)

Note

- If your machine is a region A model and "CODE XXXX -27" is printed on the label, see "Region A (mainly Europe)" also.
- If your machine is a region A model and "CODE XXXX -25, -29" is printed on the label, see "Region A (mainly Asia)" also.
- If your machine is a region A model and "CODE XXXX -21" is printed on the label, see "Region A (China)" also.
- If your machine is a region B model and "CODE XXXX -17" is printed on the label, see "Region B (mainly North America)" also.
- If your machine is a region B model and "CODE XXXX -19" is printed on the label, see "Region B (Taiwan)" also.

- Dimensions in this manual are given in two units of measure: metric and inch. Refer to the units that are used in your country/region.

List of Specifications

Specifications for the Main Unit

Note

- For details about the names and the abbreviated names of the options described in this manual, see the following.

  page 5 "Abbreviated Names of Options"

Item	Specifications
Configuration	Desktop
CPU	Qbit QB66xx 1.2GHz
Memory	2 GB
Color	Full Color
Photosensitivity type	OPC drum
Copy process	Laser beam scanning and electro-photographic printing
Warm-up time	32 seconds or less (Temperature 23°C, rated voltage)
First print time	Full color: 5.3 seconds / B&W: 4.1 seconds (A4□/8$^{1}/_{2}$ × 11□, Tray 1)
Print speed (per minute)	32 sheets/minute (A4□)
Paper weight	• Trays 1 and the bypass tray: page 139 "Recommended Paper Sizes and Types" • Duplex: 60–163 g/m^2 (Approx. 16-43 lb. Bond) *1 *1 Paper types that cannot be used for two-sided: envelopes, label paper, and coated paper
Paper output capacity	200 sheets (80 g/m^2)
Resolution (copying)	600 × 600dpi 1/2/4 bit

Item	Specifications
Paper capacity (80 g/m^2, Approx. 20 lb. Bond)	page 139 "Recommended Paper Sizes and Types"
Duplex	Standard
Power requirements	Region A (mainly Europe and Asia) 220-240 V, 6 A, 50/60 Hz Region B (mainly North America) 120–127 V, 12 A, 60 Hz Region B (Taiwan) 110V, 12 A, 60 Hz
Power consumption	Region A (mainly Europe and Asia) • Ready: 18.7 W • During printing Color: 441.7 W B&W: 426.5 W • Maximum: 1,420 W or less Region B (mainly North America and Taiwan) • Ready: 18.1 W • During printing Color: 448.6 W B&W: 444.9 W • Maximum: 1,500 W or less
Dimensions	410 × 429 × 360 mm (16.2 × 16.9 × 14.2 inches)
Space for main unit (W × D)	410 × 640 mm (16.2 × 25.2 inches) or less (When the bypass tray is open.)
Noise emission (Sound power level)	Stand-by: 42.6 dB Copying: 67.6 dB
Noise emission (Sound pressure level)	Note • Sound power levels and sound pressure levels are actual values measured in accordance with ISO 7779. • Sound pressure levels are measured from the position of the bystander.

Item	Specifications
Weight	Approx. 26.2 kg (57.8 lb.)

Specifications for Printer

Note

- To connect the machine to the network, use a LAN cable supporting 1000BASE-T, 100BASE-TX, and 10BASE-T. The length of the usable cable is up to 100 m.

Item	Specifications
Print speed (per minute)	32 sheets/minute (A4□)
Resolution	600 dpi
Printer language	• Standard: PCL5c/6(XL), PostScript 3 Emulation, PDF Emulation, MediaPrint (JPEG, TIFF) • Option: Genuine Adobe PostScript 3, PDF Direct from Adobe
Interface	• Standard: Ethernet (10BASE-T/100BASE-TX/1000BASE-T)*1 USB2.0 (Type B) port • Option: IEEE 802.11a/b/g/n/ac wireless LAN interface*1 Device Server option *1 You can use only one option at one time.
Network protocol	TCP/IP (IPv4, IPv6), LPR, DIPRINT(Port9100), FTP, IPP, Bonjour, IPP-SSL, WSD(Printer)
USB interface	• Transmission spec: USB 2.0 Standard • Connectable device: Devices corresponding to USB 2.0 Standard
Operating system	• Windows 10/11 • Windows Server 2012/2012 R2/2016/2019/2022 • macOS 11 or later

Item	Specifications
Fonts	• PCL 5c/6(XL): 80 fonts, 13 International fonts • Genuine Adobe PDF: 136 fonts • Genuine Adobe PostScript 3: 136 fonts
Store function	Total number of documents that can be stored: Up to 50 documents Number of pages for each document that can be stored: Up to 1,000 pages Total number of pages of all documents that can be stored: Up to 9,000 pages
Sort function	Number of pages that can be sorted: Up to 100 pages Number of copies that can be sorted: Up to 999 copies

Note

- The maximum length for the cable connecting the machine to an Ethernet network is 100 meters.

Specifications for Paper Feed Unit

Item	Specifications
Page size	page 139 "Recommended Paper Sizes and Types"
Paper capacity (80 g/m^2, Approx. 20 lb. Bond)	page 139 "Recommended Paper Sizes and Types"
Paper weight	page 139 "Recommended Paper Sizes and Types"
Power requirements	Power is supplied from the main unit.
Maximum power consumption	14 W or less
Dimensions (W × D × H)	Retracted: Less than 410 × 429 × 127 mm (except protruding parts) Extended: Less than 410 × 487 × 127 mm (except protruding parts)
Weight	Approx. 6 kg (13.3 lb.)

Specifications for Caster Table

Item	Specifications
Dimensions (W × D × H)	410 × 429 × 89 mm (16.2 × 16.9 × 3.6 inches) (Upright pins not included)
Weight	Approx. 5 kg (11.1 lb.)

Specifications for Wireless LAN Board

Important

- **Note that the available channels (frequency ranges) and locations to use the wireless LAN are subject to the regulations of the country or region where the printer is used. Be sure to use the wireless LAN according to the applicable regulations.**

Item	Specifications
Transmission spec	Based on IEEE 802.11a/b/g/n/ac (wireless LAN)
Transmission rate	• 2.4 GHz band: 130 Mbps (maximum) • 5 GHz band: 300 Mbps (maximum)

Frequency range (Center Frequency)	IEEE 802.11a
	• 5180–5240 MHz (36, 40, 44, and 48 channels)
	• 5260–5320 MHz (52, 56, 60, and 64 channels)
	• 5500–5700 MHz (100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140 channels)
	• 5745–5825 MHz (149, 153, 157, 161, and 165 channels)
	IEEE 802.11b/g
	• 2412–2472 MHz (1–13 channels)
	IEEE 802.11n
	• HT20
	  • 2412–2472 MHz (1–13 channels)
	  • 5180–5240 MHz (36, 40, 44, and 48 channels)
	  • 5260–5320 MHz (52, 56, 60, and 64 channels)
	  • 5500–5700 MHz (100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140 channels)
	  • 5745–5825 MHz (149, 153, 157, 161, and 165 channels)
	• HT40

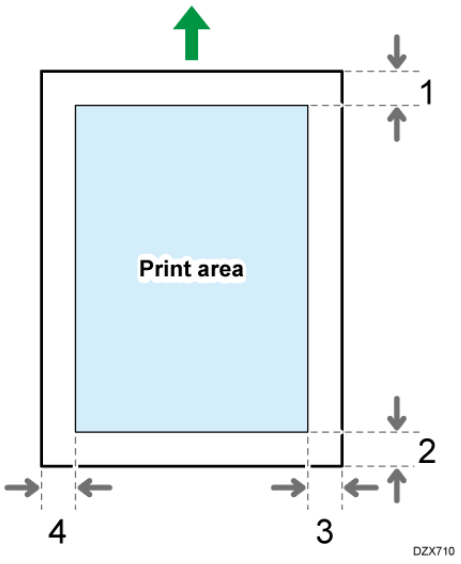
Item	Specifications
	• 5190–5310 MHz (38, 46, 54, and 62 channels) • 5510–5670 MHz (102, 110, 118, 126, and 134 channels) • 5755–5795 MHz (151 and 159 channels) IEEE 802.11ac (VHT80) • 5210–5290 MHz (42 and 58 channels) • 5530–5610 MHz (106 and 122 channels) • 5775 MHz (155 channel) Transmission mode
Transmission mode	• Infrastructure mode • Direct Connection Mode • Direct Connection: Group Owner Mode

Note

- Web Image Monitor is supported.
- The transmission rates of 130 Mbps in the 2.4 GHz band is the theoretical values of the wireless LAN specification. The actual transmission rate may be lower, depending on the operating environment.
- The channel in use might differ depending on the country.
- You may violate the local law or regulation if you specify the wireless LAN setting incorrectly.

  For details, see Connecting to a Wireless LAN, User Guide in English.

Printable Area and Margin



1. Leading edge: 4.2 ±1.5 mm (0.2 ±0.1 inches)

   Leading edge (thin paper): 3.8 mm (0.2 inches) or more
2. Trailing edge: 4.0 ±2.5 mm (0.2 ±0.1 inches)

   Trailing edge (duplex): 3.2 to 6.0 mm (0.2 to 0.3 inches) or more
3. Right edge: 3.0 ±2.0 mm (0.2 ±0.1 inches)
4. Left edge: 3.0 ±2.0 mm (0.2 ±0.1 inches)

Note

- The machine does not support edge-to-edge printing. To minimize the margins, specify the maximum printable area with the settings on the printer driver.

  See Maximizing the Printable Area When Printing, User Guide in English.
- The printable area may vary due to the paper size or settings of the printer driver.
- The outside of the printable area can be printed due to the settings of the printer driver or printing condition; however, the print result may be different from the intended one or the paper may not be fed correctly.

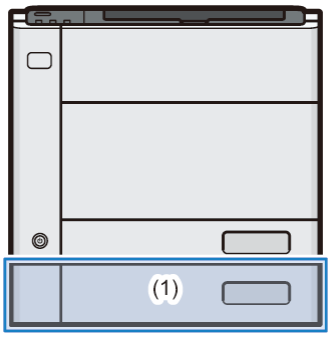
Machine Options

Note

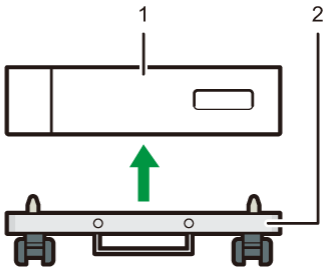
- For details about the names and the abbreviated names of the options described in this manual, see the following.

  page 5 "Abbreviated Names of Options"

Guide to Functions of the Machine's External Options



(1) Options Mounted on the Machine's Bottom



No.	Option	Description
1	Trays 2 and 3 (optional trays)	Paper is loaded here. You can load up to 500 sheets of paper. You can stack two trays.
2	Caster Table	You can attach it to the main unit or tray 2–3 (optional trays). Allows you to move the machine easily.

Note

- To use the machine with two trays combined with the caster table, contact your sales or service representative. The customer engineer must install the units.

Guide to Functions of the Machine's Internal Options

- PostScript 3 unit

  Allows you to output using Genuine Adobe PostScript 3.
- Device server option

  Allows you to add an Ethernet port to the printer. Allows you to print using the printer function via a network other than that connected to the machine.
- Wireless LAN board

  Allows you to communicate over wireless LAN.

Functions Requiring Optional Configurations

When options are installed, the functions and interface of this machine can be expanded.

Note

- For details about the names and the abbreviated names of the options described in this manual, see the following.

  page 5 "Abbreviated Names of Options"

Printer Function

Functions	Option
Genuine Adobe PostScript 3*1	PostScript 3 unit

*1 If an optional Genuine Adobe PostScript 3 is installed, the built-in standard PostScript 3 cannot be used.

Interface

Functions	Option
Wireless LAN communication See Connecting to a Wireless LAN, User Guide in English.	Wireless LAN board
Extra Ethernet Interface (for Printer) See Configuring the IP Address and Other Settings of the Device Server Option, User Guide in English.	Device server option

Legal and Contact Information

Environmental Regulations

ENERGY STAR Program(mainly North America)

ENERGY STAR® Program Requirements for Imaging Equipment

	This company is a participant in the ENERGY STAR® Program. This machine is compliant with the regulations specified by the ENERGY STAR® Program.

The ENERGY STAR® Program Requirements for Imaging Equipment encourage energy conservation by promoting energy efficient computers and other office equipment.

The program backs the development and dissemination of products that feature energy saving functions.

It is an open program in which manufacturers participate voluntarily.

Energy Star standards and logos are internationally uniform.

Energy Saving Functions

To reduce its power consumption, this machine has the following functions:

Sleep Mode

- If this machine remains idle for a specified period, it automatically reduces its electrical consumption.
- The default period the machine waits before entering Sleep Mode is 1 minute. This default time can be changed.

Specifications

Reduced Electrical Consumption by Sleep Mode	Region A (mainly Europe and Asia) 0.38 W Region B (mainly North America and Taiwan)

	0.36 W
Time of Switch into Sleep Mode (Default)	1 minute
Time of Switch out from Sleep Mode	10 seconds or less

The time it takes to switch out from energy saving functions and electrical consumption may differ depending on the conditions and environment of the machine.

Note

- For details about changing the time the machine waits before entering the Sleep mode, see Changing the Duration to Wait Before Entering Sleep Mode, User Guide in English.

User Information on Electrical and Electronic Equipment (mainly Europe)

Users in the countries where this symbol shown in this section has been specified in national law on collection and treatment of E-waste

Our Products contain high quality components and are designed to facilitate recycling.

Our products or product packaging are marked with the symbol below.



The symbol indicates that the product must not be treated as municipal waste. It must be disposed of separately via the appropriate return and collection systems available. By following these instructions you ensure that this product is treated correctly and help to reduce potential impacts on the environment and human health, which could otherwise result from inappropriate handling. Recycling of products helps to conserve natural resources and protect the environment.

For more detailed information on collection and recycling systems for this product, please contact the shop where you purchased it, your local dealer or sales/service representatives.

All Other Users

If you wish to discard this product, please contact your local authorities, the shop where you bought this product, your local dealer or sales/service representatives.

For Users in India

This product including components, consumables, parts and spares complies with the "India E-waste Rule" and prohibits use of lead, mercury, hexavalent chromium, polybrominated biphenyls or polybrominated diphenyl ethers in concentrations

exceeding 0.1 weight % and 0.01 weight % for cadmium, except for the exemptions set in the Rule.

For Turkey only

AEEE Yönetmeliğine Uygundur. Bu sistem sarf malzemeleri ve yedek parçaları da dahil olmak üzere AEEE Yönetmeliğine Uygundur.

Üretici:

Ricoh Company, Ltd.

3-6, Nakamagome 1-chome,

Ohta-ku, Tokyo 143-8555 Japan

+81-3-3777-811(English only/Sadece İngilizce)

Note for the Battery and/or Accumulator Symbol (For EU countries only) (mainly Europe)



In accordance with the Battery Directive 2006/66/EC Article 20 Information for end-users Annex II, the above symbol is printed on batteries and accumulators.

This symbol means that in the European Union, used batteries and accumulators should be disposed of separately from your household waste.

In the EU, there are separate collection systems for not only used electrical and electronic products but also batteries and accumulators.

Please dispose of them correctly at your local community waste collection/recycling centre.

Environmental Advice for Users (mainly Europe)

Users in the EU, Switzerland and Norway

Consumables yield

Please refer to either the User's Manual for this information or the packaging of the consumable.

Recycled paper

The machine can use recycled paper which is produced in accordance with European standard EN 12281:2002 or DIN 19309. For products using EP printing

technology, the machine can print on 64 g/m^2 paper, which contains less raw materials and represents a significant resource reduction.

Duplex printing (if applicable)

Duplex printing enables both sides of a sheet of paper to be used. This saves paper and reduces the size of printed documents so that fewer sheets are used. We recommend that this feature is enabled whenever you print.

Toner and ink cartridge return program

Toner and ink cartridge for recycling will be accepted free of charge from users in accordance with local regulations.

For details about the return program, please refer to the Web page below or consult your service person.

https://www.ricoh-return.com/

Energy efficiency

The amount of electricity a machine consumes depends as much on its specifications as it does on the way you use it. The machine is designed to allow you to reduce electricity costs by switching to Ready mode after it prints the last page. If required, it can immediately print again from this mode. If no additional prints are required and a specified period of time passes, the device switches to an energy saving mode.

In these modes, the machine consumes less power (watts). If the machine is to print again, it needs a little longer to return from an energy saving mode than from Ready mode.

For maximum energy savings, we recommend that the default setting for power management is used.

Notes to users in the state of California (Notes to Users in USA) (mainly North America)

Perchlorate Material - special handling may apply. See:
www.dtsc.ca.gov/hazardouswaste/perchlorate

Information for China energy efficiency label (China)

Specification model	P C375
Manufacturer name	Ricoh Company, Ltd.
Energy efficiency index	1
Typical energy consumption (kW/h)	1.11

According to the national standards	GB21521-2014

Notes for wireless LAN

This product is equipped with wireless LAN.

Depending on the machine type, wireless LAN is optional.

The product uses the 2.4/5 GHz frequency range for wireless LAN communication. Communications using radio waves may be interrupted by noise or interference. If you want to use this product for external communication, please be aware that communication failures may occur.

It is prohibited by law to disassemble or modify this product. The company takes no responsibility for illegal modifications that are made to the wireless module of this product.

No measures to prevent or block data tampering are available for devices that use radio waves for communication. The company takes no responsibility for security problems arising due to wireless LAN specifications or other conditions.

The frequency range used by this product may also be used by other products (industrial, scientific, or medical devices) manufactured by other companies. The outdoor use of wireless devices may be restricted. Pay attention to where you use this function.

Some applications of this product use the wireless function. Depending on the environment where you use the wireless function, communication may be interrupted due to radio wave interference.

In infrastructure mode, the wireless LAN function's usable frequencies vary depending on the access point you use.

Notas sobre IFETEL, México

La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Trademarks (User Guide)

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

Acrobat is either a registered trademark or a trademark of Adobe in the United States and/or other countries.

PostScript is either a registered trademark or a trademark of Adobe in the United States and/or other countries.

Reader is either a registered trademark or a trademark of Adobe in the United States and/or other countries.

Apple is a trademark of Apple Inc., registered in the United States and other countries.

Bonjour is a trademark of Apple Inc., registered in the United States and other countries.

macOS is a trademark of Apple Inc., registered in the United States and other countries.

Safari is a trademark of Apple Inc., registered in the United States and other countries.

Citrix XenApp is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries.

Dropbox is a registered trademark or trademark of Dropbox, Inc.

Firefox is registered trademark of the Mozilla Foundation.

Google is a trademark or a registered trademark of Google LLC.

Google Chrome is a trademark or a registered trademark of Google LLC.

Google Drive is a trademark or a registered trademark of Google LLC.

Java is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

JAWS® is a registered trademark of Freedom Scientific, Inc., St. Petersburg, Florida and/or other countries.

Kerberos is a trademark of the Massachusetts Institute of Technology (MIT).

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

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

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

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

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

- The proper name of Edge is Microsoft® Edge™.
- The proper name of Internet Explorer 11 is Internet Explorer® 11.

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

- The product names of Windows 10 are as follows:

  Microsoft® Windows® 10 Home

  Microsoft® Windows® 10 Pro

Microsoft® Windows® 10 Enterprise

Microsoft® Windows® 10 Education

- The product names of Windows 11 are as follows:

  Microsoft® Windows® 11 Home

  Microsoft® Windows® 11 Pro

  Microsoft® Windows® 11 Pro Education

  Microsoft® Windows® 11 Pro for Workstations

  Microsoft® Windows® 11 Education

- The product names of Windows Server 2012 are as follows:

  Microsoft® Windows Server® 2012 Foundation

  Microsoft® Windows Server® 2012 Essentials

  Microsoft® Windows Server® 2012 Standard

- The product names of Windows Server 2012 R2 are as follows:

  Microsoft® Windows Server® 2012 R2 Foundation

  Microsoft® Windows Server® 2012 R2 Essentials

  Microsoft® Windows Server® 2012 R2 Standard

- The product names of Windows Server 2016 are as follows:

  Microsoft® Windows Server® 2016 Essentials

  Microsoft® Windows Server® 2016 Standard

  Microsoft® Windows Server® 2016 MultiPoint® Premium Server

- The product names of Windows Server 2019 are as follows:

  Microsoft® Windows Server® 2019 Standard

  Microsoft® Windows Server® 2019 Essentials

- The product names of Windows Server 2022 are as follows:

  Microsoft® Windows Server™ 2022 Standard

PCL is a trademark of the Hewlett-Packard Company.

QBit and the QBit logo are trademarks of QBit Semiconductor LTD.

The SD is a trademark of SD-3C, LLC.

The SD logo is a trademark of SD-3C, LLC.



This product includes RSA BSAFE® Cryptographic software of EMC Corporation. RSA is a registered trademark or a trademark of EMC Corporation in the United States and other countries.

This product includes RSA BSAFE® Cryptographic software of EMC Corporation. BSAFE is a registered trademark or a trademark of EMC Corporation in the United States and other countries.

Wi-Fi® is a registered trademark of Wi-Fi Alliance.

Wi-Fi Direct® is a registered trademark of Wi-Fi Alliance.

Wi-Fi Protected Setup™ is a trademark of Wi-Fi Alliance.

WPA2™ is a trademark of Wi-Fi Alliance.

WPA3™ is a trademark of Wi-Fi Alliance.

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

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

7. Setup

Setting Up the Printer

Installing Options

Order of Option Installation

When installing multiple options, the following order is recommended:

1. **Attach the paper feed unit.**
   - Attach the paper feed unit to the bottom of the machine.

     You can attach up to two paper feed units. Up to 1,000 sheets of paper can be loaded.
   - When installing the caster table, place the optional paper feed unit on the caster table. For details, see the installation guides provided with the options.
2. **Install the optional wireless LAN interface board.**

   Install in the slot of the machine.
3. **Insert SD card option.**

   Insert in the SD card slot of the machine.

Note

- Ask your service representative for information on installing and configuring the device server option.

Attaching the Paper Feed Unit

You can install a paper feed unit.

⚠WARNING

- Do not handle the power cord plug with wet hands. Doing so can result in electric shock.

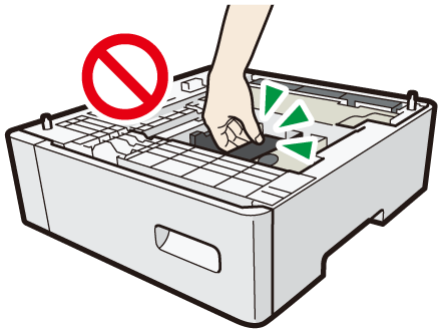
⚠CAUTION

- The machine weighs approximately 26.2 kg (57.8 lb.).
- When moving the machine, use the inset grips on both sides, and lift slowly in pairs. The machine will break or cause injury if dropped.
- Lifting the paper feed unit carelessly or dropping may cause injury.

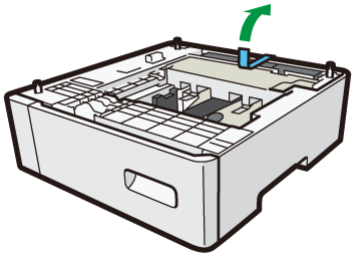
- When moving the machine, make sure to unplug the power cord from the wall outlet and confirm that line cords and other connecting cables have been removed. Otherwise, the power cord is damaged, possibly resulting in fire or electric shock.

Important

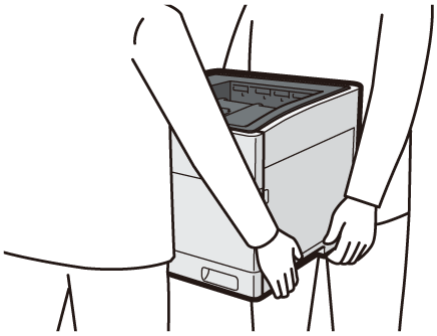
- **To attach two paper feed units at the same time, first stack them one upon the other, and then attach them as a single unit.**
- **When moving the machine, do not touch the following parts:**
  - **Places indicated on the labels attached to the machine**
  - **The bottom of the optional paper tray**
- **Do not hold the part indicated below when you lift the paper feed unit.**



1. **Remove the adhesive tape from the paper feed unit.**



2. **Turn the machine off and unplug the power cord.**
3. **Hold the carrying handles on both sides of the machine from the front and back as shown, carefully lift the machine using two people, and then move it horizontally over the optional paper feed unit.**

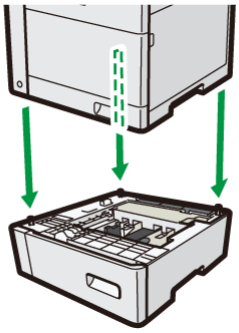


Lifting the machine requires two people.

When moving the machine, do not touch the following parts:

- Places indicated on the labels attached to the machine
- The bottom of the optional paper tray

4. **Align the three upright pins of the optional paper feed unit with the holes on the underside of the machine, and then lower the machine carefully.**



5. **Plug in the power cord, and then turn on the machine.**
6. **Print the configuration page to confirm that the unit was attached correctly.**

   To check whether the optional paper feed unit was correctly attached, print the configuration page, and check "Attached Equipment" on the configuration page. If the unit was attached correctly, "Tray 2" and "Tray 3" will appear.

   See Printing the Configuration Page, User Guide in English.

Note

- If the optional paper feed unit was not installed properly, repeat the procedure from the beginning. If it cannot be installed correctly even after trying the installation a second time, contact your sales or service representative.
- To use the paper feed unit, configure the machine options in "Accessories" in the printer driver.

  See Specifying the Option Configuration or Paper Settings Manually, User Guide in English.

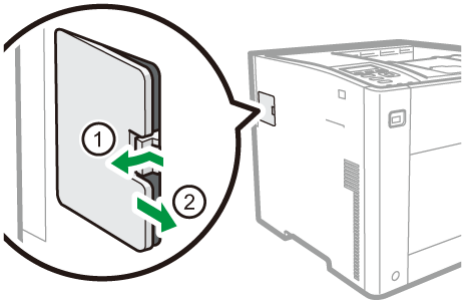
Installing the Wireless LAN Interface Board

Important

- **Before beginning work, ground yourself by touching something metal to discharge any static electricity. Static electricity can damage the interface units.**
- **Do not subject the wireless LAN interface board to physical shocks.**

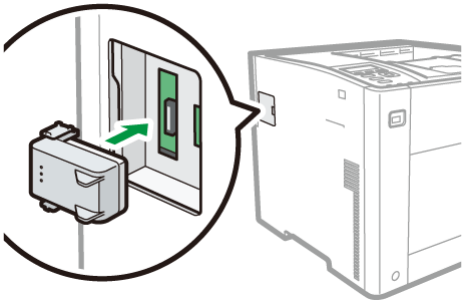
1. **Check the contents of the package.**
2. **Turn the machine off and unplug the power cord.**
3. **Remove the slot cover on the left side of the machine.**

   Pull up the tab of the slot cover while pushing it in (1), and remove the slot cover at an angle (2).



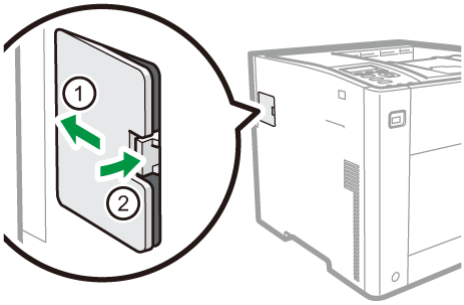
4. **Fully insert the wireless LAN interface board.**

   Align the connector in the direction shown in the illustration, and then fully insert it.



5. **Attach the slot cover.**

   Insert the two protrusions of the slot cover into the machine, and then push in the tab until it clicks.



6. **Plug in the power cord, and then turn on the machine.**
7. **Print the configuration page to confirm that the board was attached correctly.**

   Check that the board was correctly installed by printing the configuration page. If it is correctly installed, "Wireless LAN" will appear for "Device Connection" on the configuration page.

   See Printing the Configuration Page, User Guide in English.

Note

- If the board was not installed properly, repeat the procedure from the beginning. If it cannot be installed correctly even after trying the installation a second time, contact your sales or service representative.
- Before using the board, you must configure settings from the control panel.

  For details, see Connecting to a Wireless LAN.

Installing SD Card Option

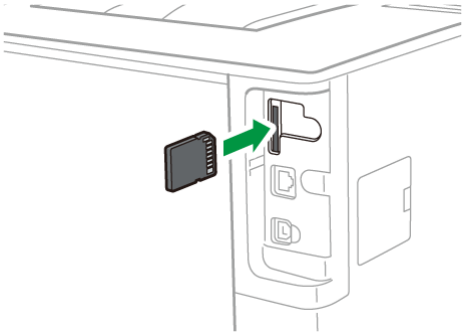
CAUTION

- Keep SD card out of reach of children. If a child accidentally swallows an SD card, consult a doctor immediately.

Important

- **Do not subject the card to physical shocks.**

1. **Check the contents of the package.**
2. **Turn the machine off and unplug the power cord.**
3. **Insert the SD card into the slot until it clicks.**



4. **Plug in the power cord, and then turn on the machine.**
5. **Check that the SD card was installed correctly.**

Note

- You can confirm that the SD card was installed correctly by checking the control panel menu or configuration page.
  - PostScript 3 unit: Printing the configuration page, if the card is installed properly, corresponding option's name will appear for "Printer Language" in "System Reference".

    See Printing the Configuration Page, User Guide in English.
- If the card is not installed properly, repeat the procedure from the beginning. If it cannot be installed correctly even after trying the installation a second time, contact your sales or service representative.
- Do not touch the card while the machine is in use. It may come loose, even if pushed only slightly.

8. Driver Installation Guide

Installing the Printer Driver

Installing the Printer Driver by Using Device Software Manager Installer

Device Software Manager is a support utility for driver installation in Windows. Device Software Manager helps you to detect the latest driver via the internet automatically according to the computer you are using and install it with a simple procedure.

Important

- **Manage Printers permission is required to install the drivers. Log on as an Administrators group member.**
- **Device Software Manager supports Windows OS only. To install the printer driver on macOS, see the following sections:**

  page 179 "Installing the Printer Driver for Network Connection (macOS)"

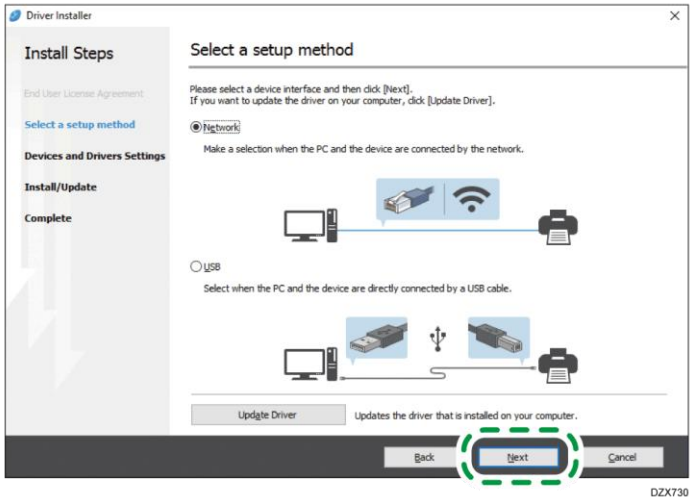
  See "Installing the Printer Driver for USB Connection (macOS)", User Guide in English.
- **Follow the instructions of the installer to connect the USB cable.**

Installing Device Software Manager from the Downloaded File

1. **Download Device Software Manager from the manufacturer's website.**
2. **Double-click the downloaded file.**
   - If the "Security Warning" screen is displayed, click [OK].
   - If the "User Account Control" screen is displayed, click [Yes] or [Allow].
3. **Select the [Run Driver Installer after installation] check box, and then click [Accept Agreement and Install].**
4. **On the "Quality Improvement Program" screen, select [I will participate in the Quality Improvement Program] or [I will not participate in the Quality Improvement Program], and then click [Next].**
5. **On the "Driver Update Notification Setting" screen, specify whether to display the message about the driver update, and then click [Next].**

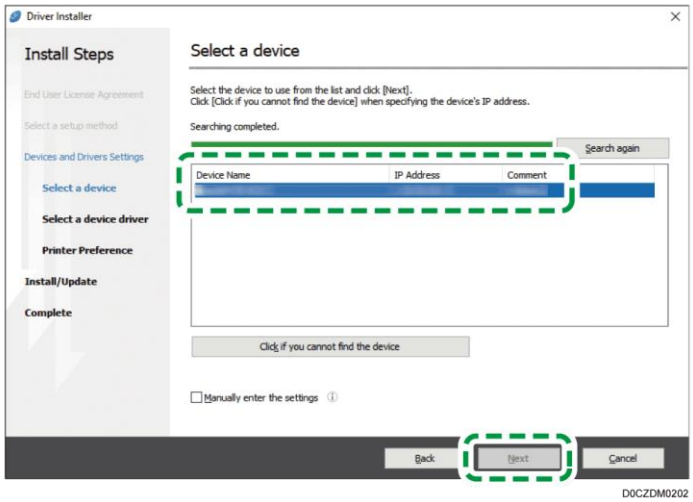
   The process of installing Device Software Manager starts.

6. **On the "End User License Agreement" screen, click [Agree and Go to Next].**
7. **Select the connection between the machine and computer, and then click [Next].**



- Network: Search for devices connected to the network.
- USB: Following the instructions on the "Connection with device" screen, connect the machine and the computer with the USB cable to search for the machine.

8. **Select this machine from among the detected devices, and then click [Next].**



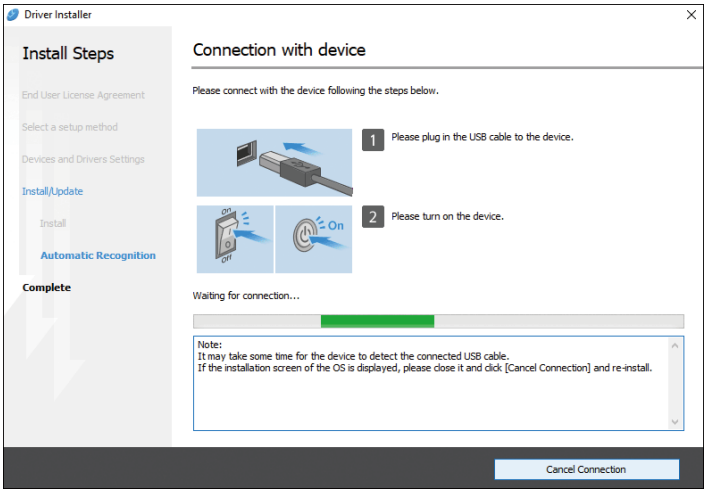
The installation of the driver starts.

- If the machine cannot be found at the network connection setup, see the following section.

  page 176 "If the Machine Cannot Be Found"

- If "The publisher could not be verified" is displayed at the beginning of installation, continue the installation. There is no problem with the started installer that is downloaded from the manufacturer's website. Continue the installation.

- When you connect the machine and the computer with a USB cable, follow the instructions on the installer screen.



If the machine is not detected, click [Cancel Connection]. Even if the connection is canceled, the installation is complete. After the installer screen is closed, the machine is added automatically when it is connected to the computer with the USB cable.

9. **When the installation is complete, click [Finish].**

Note

- Double-click the Device Software Manager icon created on the Finder of the computer to update the printer driver.

  See "Updating the Driver (Windows)", User Guide in English.



Installing the Printer Driver for Network Connection (Windows)

When the machine and the computer are connected to the same network, the installer searches for the machine to install the printer driver. If the installer cannot find the machine, specify the IP address or machine name to install the printer driver.

Important

- **Manage Printers permission is required to install the driver. Log on as an Administrators group member.**

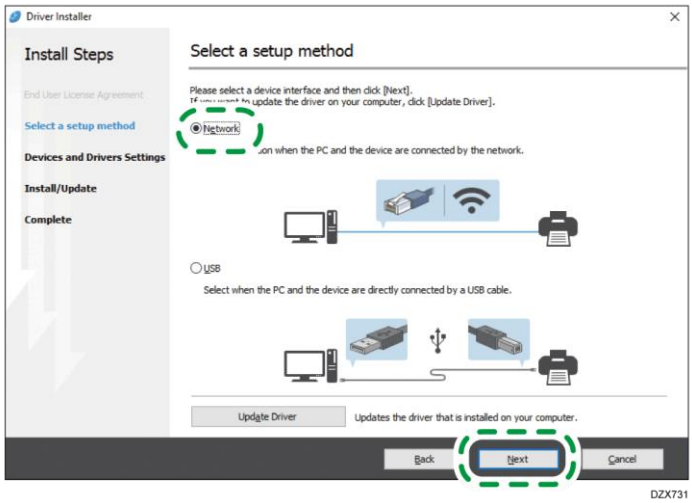
Note

- If the "User Account Control" dialog box appears during the driver installation procedure, click [Yes] or [Continue].

- If the "Windows Security" dialog box appears during the driver installation procedure, click [Install this driver software anyway].

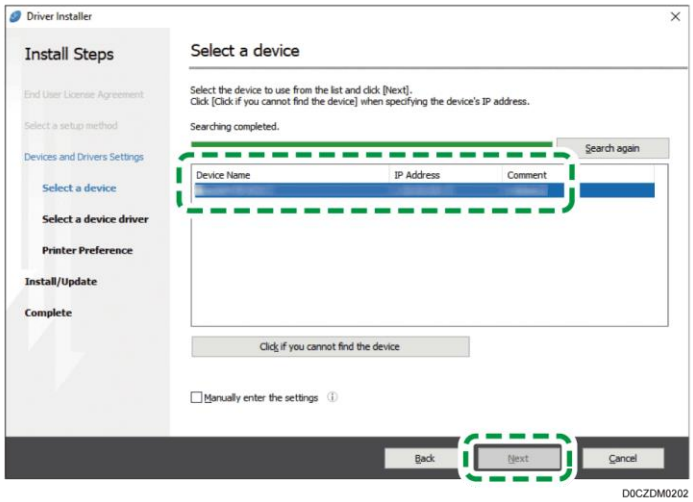
Installing the PCL 6/PostScript 3 Printer Driver from the Downloaded File

1. **Download the latest printer driver from the manufacturer's website.**
2. **Double-click the downloaded file.**
   - If the "Security Warning" screen is displayed, click [OK].
   - If the "User Account Control" screen is displayed, click [Yes] or [Allow].
3. **On the "End User License Agreement" screen, click [Agree and Go to Next].**
4. **Select [Network], and then click [Next].**



- The search detects devices connected to the network.
- If the error screen is displayed, see page 176 "If the Machine Cannot Be Found".

5. **Select this machine from among the detected devices, and then click [Next].**



Printer driver installation starts.

- If the machine cannot be found at the network connection setup, see the following section.

  page 176 "If the Machine Cannot Be Found"

6. **When prompted to select whether to install Device Software Manager, select whether to install Device Software Manager.**

   To install Device Software Manager select the [Install Device Software Manager] check box, and then click [Next]. Follow the instructions on the screen to install Device Software Manager.

   To not install Device Software Manager clear the [Install Device Software Manager] check box, and then click [Next].

7. **When the installation is complete, click [Finish].**

Installing the Printer Driver for Windows

1. **Download the latest printer driver from the manufacturer's website.**
2. **Double-click the downloaded file.**
   - If the "Security Warning" screen is displayed, click [OK].
   - If the "User Account Control" screen is displayed, click [Yes] or [Allow].

3. **Click [Cancel] to exit the installer.**
4. **Display the "Devices and Printers" screen.**

   ### Windows 11

   1. On the [Start] menu, click [All apps] ▶ [Windows Tools] ▶ [Control Panel]
   2. Click [View devices and printers].

   ### Windows 10 (version 1703 or later)

   1. On the [Start] menu, click [Windows System] ▶ [Control Panel].
   2. Click [View devices and printers].

   ### Windows 10 (earlier than version 1703)

   1. Right-click [Start], and then click [Control Panel].
   2. Click [View devices and printers].
5. **Click [Add a printer].**
6. **Click [The printer that I want isn't listed].**
7. **Select [Add a local printer or network printer with manual settings], and then click [Next].**
8. **Select [Standard TCP/IP Port] on [Create a new port:], and then click [Next].**
9. **Enter the IP address of this machine in [Host Name or IP address].**
10. **Clear the [Query the printer and automatically select the driver to use] check box, and then click [Next].**

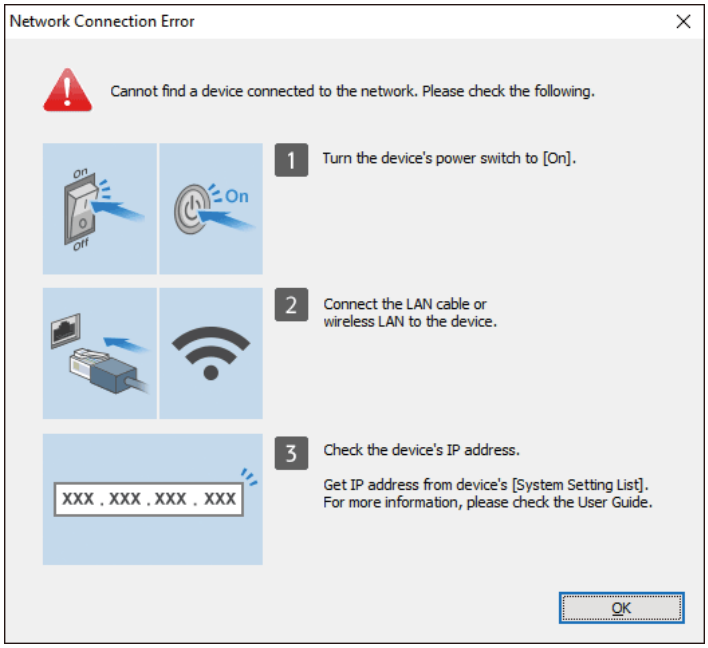
    Searching for the TCP/IP port starts.
11. **When the "Additional port information required" screen is displayed, select [RICOH Network Printer C model], and then click [Next].**
12. **Click [Have Disk...] ▶ [Browse...] to specify the driver (INF file), and then click [OK].**

    The driver is stored in the [DISK1] folder in the folder that was created when unzipping the downloaded file.
13. **Select a printer driver to install, and then click [Next].**
14. **Enter the printer name as necessary, and then click [Next].**

    Printer driver installation starts.
15. **Specify the printer as a shared printer as necessary, and then click [Next] ▶ [Finish].**

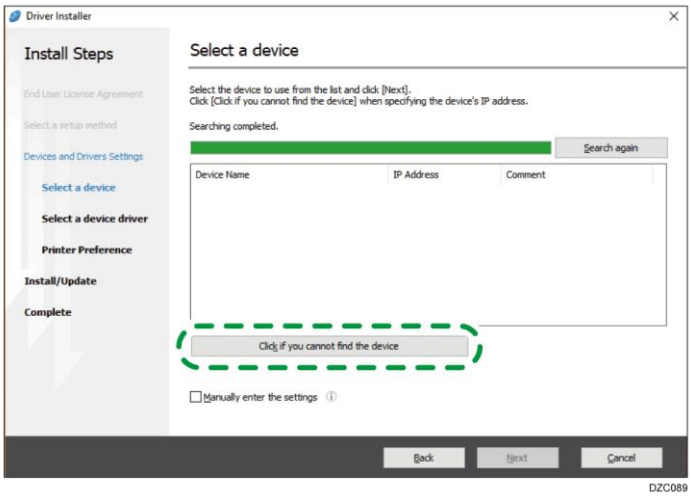
If the Machine Cannot Be Found

The "Network Connection Error" screen is displayed.



Confirm and perform 1 to 3, and then click [OK]. If the machine still cannot be found, specify the IP address or machine name to install the printer driver.

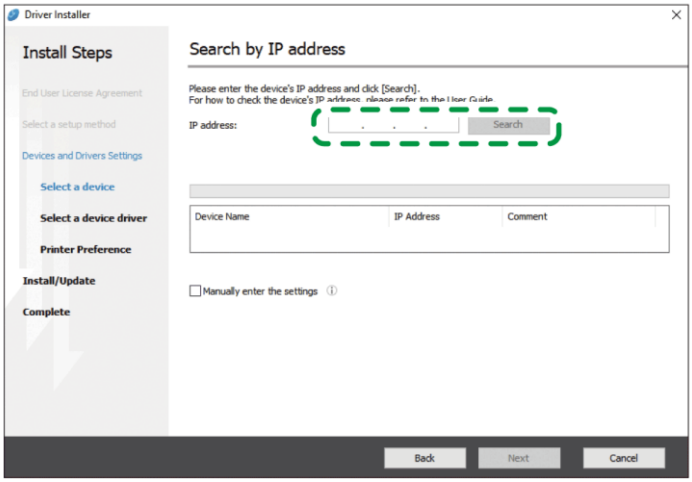
1. **Click [Click if you cannot find the device].**



2. **Select [Specify device IP address] or [Specify device name], and then click [Next].**

When specify the machine IP address

1. Enter the IP address of the machine and click [Search].



DZC091

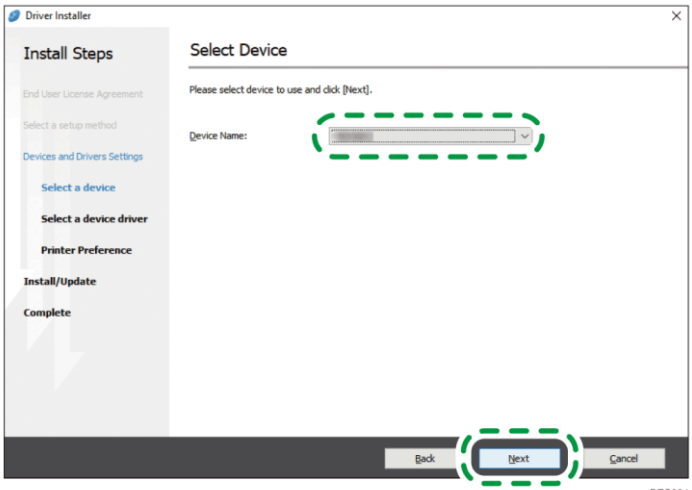
You can check the machine IP address in [Check Status]▶[Network] on the control panel.

2. When the machine is detected, click [Next].

   Printer driver installation starts.

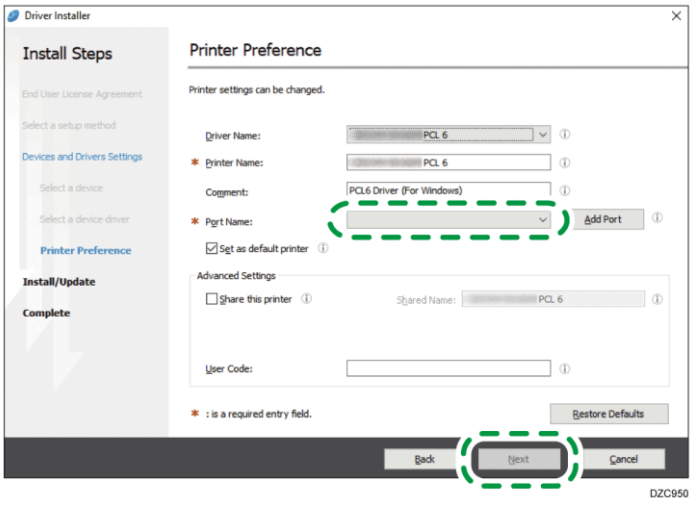
When specify the machine name

1. Select the machine to use, and then click [Next].



DZC094

2. On the "Printer Preference" screen, select one of the port names from among "Port Name", and then click [Next].



Printer driver installation starts.

For details about the procedure for specifying the IP address after installing the printer driver, see the following section:

See "When You Cannot Print a Document even if the Printer Driver is Installed", User Guide in English.

3. **When prompted to select whether to install Device Software Manager, select whether to install Device Software Manager.**

   To install Device Software Manager select the [Install Device Software Manager] check box, and then click [Next]. Follow the instructions on the screen to install Device Software Manager.

   To not install Device Software Manager clear the [Install Device Software Manager] check box, and then click [Next].

4. **When the installation is complete, click [Finish].**

Installing the Printer Driver for Network Connection (macOS)

Install the PPD file (printer driver) under macOS, and then register the machine on the computer from the system preferences.

Important

- **You need an administrator name and a password (phrase). For details, consult your network administrator.**

Note

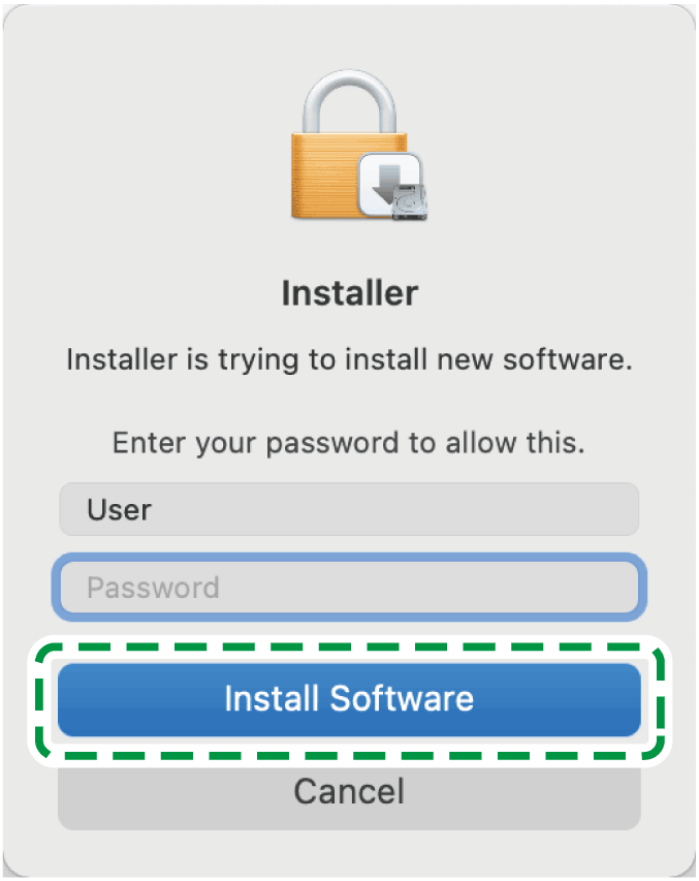
- Setting procedures using macOS 12.2 are shown as an example. The actual procedure may differ depending on the OS version you are using.

Installing the PPD file (Network Connection)

1. **Download the latest printer driver from the manufacturer's website.**
2. **Double-click the downloaded file.**
3. **Double-click the package file.**



4. **On the "Introduction" screen, click [Continue].**
5. **On the "License" screen, click [Continue] and then click [Agree].**
   - When prompted to select where to install the driver, specify the install location, and click [Continue].
6. **Click [Install].**
7. **Enter the administrator's user name and password, and then click [Install Software].**



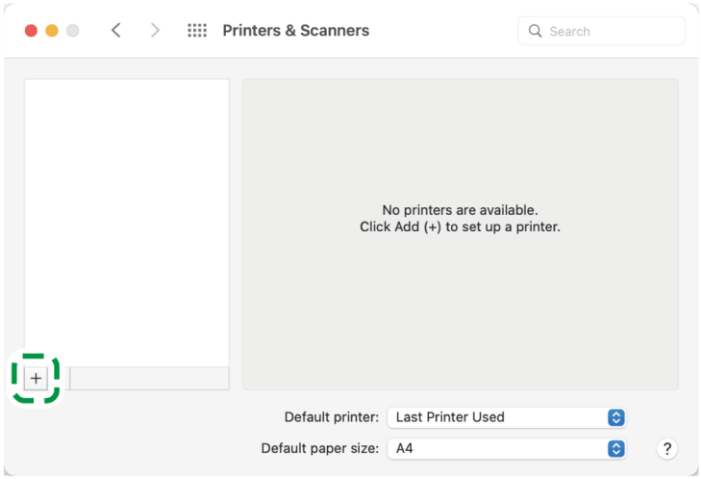
The installation of the PPD file starts.

8. **When the installation is complete, click [Close].**

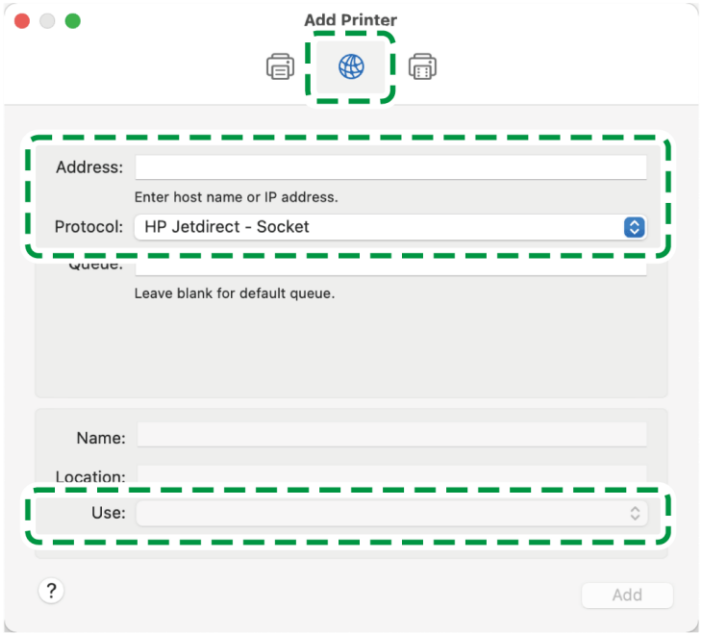
Registering the Machine in [Printers & Scanners] (Network Connection)

Register the PPD file of the machine in the system preferences to enable printing.

1. **Select [System Preferences...] from the Apple menu.**
2. **Click [Printers & Scanners].**
3. **Click [+].**



4. **Click (IP), and configure the information of the machine.**



- Address: Enter the IP address of the machine.
- Protocol: Select [HP Jetdirect-Socket].
- Use: Check that the machine name is displayed. If "Generic PostScript Printer" is displayed, the entered IP address may not be correct.

When "Generic PostScript Printer" is displayed even though the IP address is correct

Check the network connection of the machine and the computer, and then register again.

- When the machine is connected to a wired LAN.

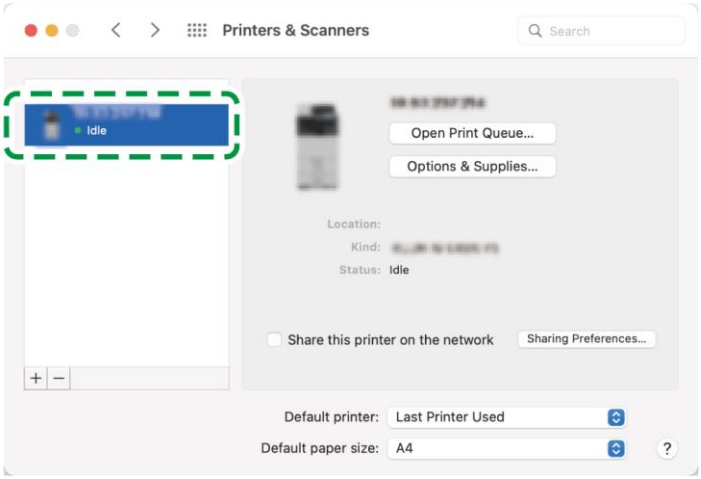
  Check that the cable is connected to the machine correctly.

5. **Click [Add].**

   The progress screen is displayed.

   - If the progress screen does not close after a while, click [Configure...] and configure the option configuration of the printer. For the procedure of the option configuration, see page 182 "Specifying the Option Configuration of the Machine to the Printer Driver (Network Connection)".

6. **Check that the machine name is added to the [Printers & Scanners] screen.**

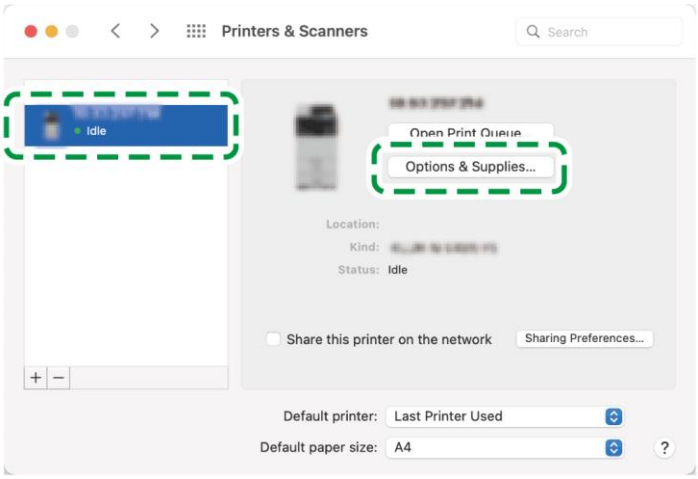


7. **Close the system preferences screen.**

Specifying the Option Configuration of the Machine to the Printer Driver (Network Connection)

If the option configuration of the machine is not automatically reflected, select the option installed on the machine in [Printers & Scanners].

1. **Select [System Preferences...] from the Apple menu.**
2. **Click [Printers & Scanners].**
3. **Select the machine from the list, and then click [Options & Supplies...].**



4. **Click [Options], select the option installed on the machine, and then click [OK].**
   - If the usable options are not displayed, the IP address has not been entered correctly or the PPD file has not been registered properly. To enter the IP address or register the PPD file, see page 181 "Registering the Machine in [Printers & Scanners]".
5. **Close the system preferences screen.**

Note

- If the option you want to select is not displayed, PPD files may not be set up correctly. To complete the setup, check the name of the PPD file displayed in the dialog box.
- To specify an optional Adobe PostScript when using a PostScript 3 printer driver, select [Adobe PostScript] in the "PostScript:" list on the [Options] tab.

9. How to use this manual

Moving pages



Click to expand or collapse all the items in the table of contents at once.

To expand or collapse items individually, click or next to each title in the table of contents.



Indicates which chapter and items are shown on the current page. You can click a page to move to it.



Click to move to the previous or next page in the table of contents.

Displaying pages with smart devices



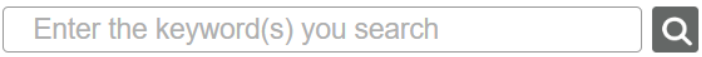
Click to display the URL of the current page as a QR code.

Changing the size of characters



Changes the size of characters in 3 stages. Each time you click, the size of the characters changes.

Searching for keywords



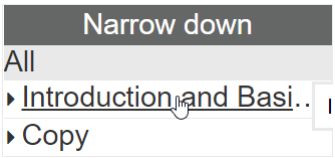
Pages including the entered keyword are displayed as the search results.

Substitute words and related keywords appear according to the entered keywords.

To refine the search results:

Enter multiple keywords (up to three keywords). (Pages including all keywords are searched for.)

- Select the title from the "Narrow down" list on the search result screen, and then click the search button (🔍) again to limit the scope of searching within the selected title.



Meanings of the used symbols

⚠WARNING

Indicates a potentially hazardous situation which, if instructions are not followed, could result in death or serious injury.

⚠CAUTION

Indicates a potentially hazardous situation which, if instructions are not followed, may result in minor or moderate injury or damage to property.

Important

Indicates points to pay attention to when using functions. This symbol indicates points that may result in the product or service becoming unusable or result in the loss of data if the instructions are not obeyed. Be sure to read these explanations.

Note

Indicates supplementary explanations of the product's functions and instructions on resolving user errors.

[ ]

Indicates the names of keys or buttons on the product or display.

#Sample screenshots are used.

MEMO

MEMO

Copyright ©2024