



Read This First

Manuals Provided with This Machine	1
Safety Information for This Machine	2
Other Information for This Machine	3
Appendix	4

Please look at the on-screen instruction manual (included in the attached CD-ROM), the manual provided on this company's website, or the manual viewable via the Smart Operation Panel for information not included in the paper instruction manual.



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

TABLE OF CONTENTS

How to Read the Manuals.....	2
Symbols Used in the Manuals.....	2
Disclaimer.....	2
Notes.....	3
Machine Types.....	3

1. Manuals Provided with This Machine

Manuals for This Machine.....	5
Manuals List.....	7
How to Use the Operating Instructions.....	9
Formats of the Operating Instructions.....	9
Reading the HTML Manuals on the CD-ROM	9
Installing and Opening the HTML Manuals	10
Reading the PDF Manuals on the CD-ROM.....	10

2. Safety Information for This Machine

Safety Information.....	13
Safety During Operation.....	13
Safety Precautions to Be Followed.....	13
Safety Labels of This Machine.....	22
Positions of WARNING and CAUTION labels.....	22
Power Switch Symbols.....	24

3. Other Information for This Machine

Laws and Regulations.....	25
Duplication and Printing Prohibited.....	25
Laser Safety.....	25
Notes to USA Users of FCC Requirements.....	25
Important Safety Instructions for Facsimile Unit.....	28
Notes to Canadian Users of Facsimile Unit.....	29
Other Information.....	30
Notes to users in the state of California (Notes to Users in USA).....	30

4. Appendix

Trademarks.....	31
-----------------	----

How to Read the Manuals

Symbols Used in the Manuals

This manual uses the following symbols:

 **Important**

Indicates points to pay attention to when using the machine, and explanations of likely causes of paper misfeeds, damage to originals, or loss of data. Be sure to read these explanations.

 **Note**

Indicates supplementary explanations of the machine's functions, and instructions on resolving user errors.

 **Reference**

This symbol is located at the end of sections. It indicates where you can find further relevant information.




Indicates the names of keys on the machine's display or control panels.




Indicates instructions stored in a file on a provided CD-ROM.



Indicates instructions in sheet form.

 **Region A** (mainly Europe and Asia), (mainly Europe), or (mainly Asia)

 **Region B** (mainly North America)

Differences in the functions of Region A and Region B models are indicated by two symbols. Read the information indicated by the symbol that corresponds to the region of the model you are using. For details about which symbol corresponds to the model you are using, see "Model-Specific Information", Getting Started .

Disclaimer

To the maximum extent permitted by applicable laws, in no event will the manufacturer be liable for any damages whatsoever arising out of failures of this machine, losses of the registered data, or the use or non-use of this product and operation manuals provided with it.

Make sure that you always copy or have backups of the data registered in this machine. Documents or data might be erased due to your operational errors or malfunctions of the machine.

In no event will the manufacturer be responsible for any documents created by you using this machine or any results from the data executed by you.

Notes

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

The manufacturer shall not be responsible for any damage or expense that might result from the use of parts other than genuine parts from the manufacturer with your office products.

For good output quality, the manufacturer recommends that you use genuine toner from the manufacturer.

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

Colors on color keys or the color circle may differ slightly from the colors of actual copies.

The color samples in this manual may differ slightly from the colors of actual copies.

Machine Types

Check the type of your machine before reading the manuals.

- Type 1: MP C2003SP/MP C2003SPG
- Type 2: MP C2503SP/MP C2503SPG

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

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

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



1. Manuals Provided with This Machine

This chapter explains manuals for this machine.

Manuals for This Machine

Read this manual carefully before you use this machine.

Refer to the manuals that are relevant to what you want to do with the machine.

★ Important

- Media differ according to manual.
- Adobe® Acrobat® Reader®/Adobe Reader must be installed in order to view the manuals as PDF files.
- A Web browser must be installed in order to view the html manuals.

User Guide

Regarding the basic usage of this machine, frequently used functions, troubleshooting when an error message appears, etc., summaries are provided below for each user manual.

Read This First

Before using the machine, be sure to read the section of this manual entitled Safety Information. It also describes how to install the included CD-ROM, each regulation, and environmental conformance.

Easy Search

You can search for a description by what you want to do. Also, this machine's distinctive functions are explained.

Getting Started

Describes preparations for using the machine, operating instructions, and character input methods.

Paper Specifications and Adding Paper

Describes how to load originals and sheets and about their specifications.

Convenient Functions

Describes how to register frequently used settings, customize the Home Screen, and display a Web page on the control panel. It also describes how to manage a job.

Maintenance and Specifications

Describes how to replace supplies and how to install and clean this machine. It also describes the specifications of the main unit and options.

Troubleshooting

Provides a guide for resolving common usage-related problems.

Copy/ Document Server

Explains Copier and Document Server functions and operations. Also refer to this manual for explanations on how to specify the settings for originals.

Fax

Explains Facsimile functions and operations.

Print

Describes how to print using the printer driver. It also describes the functions available for printing.

Scan

Describes how to scan paper data using this machine and how to send the scanned data to a computer and store the data.

Connecting the Machine/ System Settings

Explains how to connect the machine to a network, and configure and operate the machine in a network environment. Also explains how to change User Tools settings and how to register information in the Address Book.

PostScript 3

Explains how to set up and use PostScript® 3™.

Extended Feature Settings

Describes how to configure the extended features using the control panel or Web Image Monitor.

Security Guide

This manual is for administrators of the machine. It explains security functions that you can use to prevent unauthorized use of the machine, data tampering, or information leakage. For enhanced security, we recommend that you first make the following settings:

- Install the Device Certificate.
- Enable SSL (Secure Sockets Layer) Encryption.
- Change the user name and password of the administrator.

For details, see "Before Using This Machine", Security Guide .

Be sure to read this manual when setting the enhanced security functions, or user and administrator authentication.

Driver Installation Guide

Describes how to install and configure each driver. This manual is included in the drivers CD.

Other Manuals

- Quick Reference Copy Guide
- Quick Reference FAX Guide
- Quick Reference Scanner Guide

Note

- Manuals provided are specific to machine types.
- Driver Installation Guide and HTML manuals are available in English, German, French, Italian, Spanish, Dutch, and Russian.
- You can download information about the machine's certification, which is based on an IT security certification system (hereafter CC Certification), from http://support-download.com/services/device/ccmanual/mp_c2003_c2503/en/download_admin.html and http://support-download.com/services/device/ccmanual/mp_c2003_c2503/en/download_user.html. This information is about how to set up the machine. If you have purchased a CC Certified machine, be sure to read it before operating the machine so you can make the correct settings before using it.
- The following software products are referred to using general names:

Product name	General name
ScanRouter EX Professional ^{*1} and ScanRouterEX Enterprise ^{*1}	the ScanRouter delivery software

*1 The ScanRouter EX Professional and ScanRouterEX Enterprise are no longer available for sale.

Manuals List

Manual Name	Printed Manuals Provided	HTML Manuals Provided	PDF Manuals Provided
User Guide	Yes	No	Yes
Read This First	Yes	No	No
Easy Search	No	Yes	No
Getting Started	No	Yes	No
Paper Specifications and Adding Paper	No	Yes	No
Convenient Functions	No	Yes	No
Maintenance and Specifications	No	Yes	No
Troubleshooting	No	Yes	No
Copy/ Document Server	No	Yes	No
Fax	No	Yes	No

Manual Name	Printed Manuals Provided	HTML Manuals Provided	PDF Manuals Provided
Print	No	Yes	No
Scan	No	Yes	No
Connecting the Machine/ System Settings	No	Yes	No
PostScript 3	No	Yes	No
Extended Feature Settings	No	Yes	No
Security Guide	No	No	Yes
Driver Installation Guide	No	No	Yes
Quick Reference Copy Guide	No	No	Yes ^{*1}
Quick Reference FAX Guide	No	No	Yes ^{*1}
Quick Reference Scanner Guide	No	No	Yes ^{*1}

* 1 These manuals are available on our website or from authorized dealers.

Note

- Driver Installation Guide and HTML manuals are available in English, German, French, Italian, Spanish, Dutch, and Russian.
- Printed User Guide is available in English.

How to Use the Operating Instructions

This chapter describes the operating instructions of this machine.

Formats of the Operating Instructions

The operating instructions of this machine are provided in the following formats:

- Printed manuals
- HTML manuals
- PDF manuals

For details about the contents of each manual, see page 5 "Manuals for This Machine". The various manuals are available in different formats. For details about availability, see page 7 "Manuals List".

Reading the HTML Manuals on the CD-ROM

This section describes how to read the HTML manuals on the supplied manual CD-ROM.

1. **Insert the CD-ROM in the CD-ROM drive of your computer.**
2. **Select a language, and then click [OK].**
3. **Click [Read HTML manuals].**

The browser opens.

4. **Click the title of manual you want to read.**

Note

- Recommended browsers:
 - Internet Explorer 6 or later
 - Firefox 3.5 or later
 - Safari 4.0 or later
- If you want to read the HTML manuals on a Macintosh, insert the CD-ROM in the CD-ROM drive, and then open "Manuals.htm".
- If JavaScript is disabled or unavailable in your browser, you will not be able to search or use certain buttons in the HTML documentation.
- HTML manuals are available in English, German, French, Italian, Spanish, Dutch, and Russian.

Installing and Opening the HTML Manuals

This section describes how to install and open the HTML manuals on your computer.

For your convenience, we recommend you install these manuals on your computer.

1

1. Insert the CD-ROM in the CD-ROM drive of your computer.
2. Select a language, and then click [OK].
3. Click [Install manuals].
4. Install the HTML manuals by following the on-screen instructions.
5. When the installation is complete, click [Finish].
6. Click [Exit].
7. Open the HTML manuals that you installed.

To open the manuals from an icon, double-click the icon on the desktop. To open the manuals from the [Start] menu, point to [All Programs], and then click [Product Name].

8. Click the title of the manual you want to read.

↓ Note

- You need administrator permissions to install the manuals. Log in as an Administrators group member.
- The system requirements for installing the manuals are as follows:
 - Operating system: Windows XP/Vista/7/8, Windows Server 2003/2003 R2/2008/2008 R2/2012
 - Minimum display resolution: 800 × 600 pixels
- If you cannot install a manual, copy the "MANUAL_HTML" folder to your computer's hard drive, and then run "setup.exe".
- To delete an installed manual, on the [Start] menu, point to [All Programs], click [Product Name], and then uninstall the data.
- Depending on the settings made during installation, menu folder names may differ.
- HTML manuals are available in English, German, French, Italian, Spanish, Dutch, and Russian.

Reading the PDF Manuals on the CD-ROM

This section describes how to read the PDF manuals on the supplied CD-ROMs.

File path

- User Guide and Security Guide are included in the following folder on the supplied manual CD-ROM:
MANUAL_PDF*(1 language)*

- Driver Installation Guide is included in the following folder on the supplied driver CD-ROM:
MANUAL_DRIVER\(\1 language)

1. Insert the CD-ROM in the CD-ROM drive of your computer.

2. Select a language, and then click [OK].

3. Click [Read PDF manuals].

To read Driver Installation Guide, click [Driver Installation Guide]. The manual opens.

4. Click the title of the manual you want to view.

Note

- To view the PDF manuals, you need to have Adobe Acrobat Reader/Adobe Reader installed on your computer.
- If you want to read the PDF manuals on a Macintosh, insert the CD-ROM in the CD-ROM drive, and then open "Manuals.htm".
- Driver Installation Guide is available in English, German, French, Italian, Spanish, Dutch, and Russian.

2. Safety Information for This Machine

This chapter describes the safety precautions.

Safety Information

Safety During Operation

In this manual, the following important symbols are used:

- ⚠ 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.

Safety Precautions to Be Followed

This section explains safety precautions that should always be followed when using this machine.

Environments where the machine can be used

This section explains safety precautions about environments where the machine can be used.

- ⚠ WARNING**
 - Do not use flammable sprays or solvents in the vicinity of this machine. Doing so could result in fire or electric shock.
- ⚠ WARNING**
 - Do not place vases, plant pots, cups, toiletries, medicines, small metal objects, or containers holding water or any other liquids, on or close to this machine. Fire or electric shock could result from spillage or if such objects or substances fall inside this machine.
- ⚠ CAUTION**
 - Keep the machine away from humidity and dust. Otherwise a fire or an electric shock might occur.

⚠ CAUTION

- Do not place the machine on an unstable or tilted surface. If it topples over, an injury might occur.

⚠ CAUTION

- Do not place heavy objects on the machine. Doing so can cause the machine to topple over, possibly resulting in injury.

⚠ CAUTION

- Make sure the room where you are using the machine is well ventilated and spacious. Good ventilation is especially important when the machine is used heavily.

⚠ CAUTION

- Do not obstruct the machine's vents. Doing so risks fire caused by overheated internal components.

Handling power cords and power cord plugs

This section explains safety precautions about handling power cords and power cord plugs.

⚠ WARNING

- Do not use any power sources other than those that match the specifications shown. Doing so could result in fire or electric shock.

⚠ WARNING

- Do not use any frequencies other than those that match the specifications shown. Doing so could result in fire or electric shock.

⚠ WARNING

- Do not use multi-socket adaptors. Doing so could result in fire or electric shock.

⚠ WARNING

- Do not use extension cords. Doing so could result in fire or electric shock.

⚠ WARNING

- Do not use power cords that are damaged, broken, or modified. Also, do not use power cords that have been trapped under heavy objects, pulled hard, or bent severely. Doing so could result in fire or electric shock.

⚠ WARNING

- Touching the prongs of the power cable's plug with anything metallic constitutes a fire and electric shock hazard.

⚠ WARNING

- The supplied power cord is for use with this machine only. Do not use it with other appliances. Doing so could result in fire or electric shock.

⚠ WARNING

- It is dangerous to handle the power cord plug with wet hands. Doing so could result in electric shock.

⚠ WARNING

- If the power cord is damaged and its inner wires are exposed or broken, contact your service representative for a replacement. Use of damaged power cords could result in fire or electric shock.

⚠ WARNING

- Be sure to disconnect the plug from the wall outlet at least once a year and check for the following:
 - There are burn marks on the plug.
 - The prongs on the plug are deformed.
- If any of the above conditions exist, do not use the plug and consult your dealer or service representative. Use of the plug could result in fire or electric shock.

WARNING

- Be sure to disconnect the power cord from the wall outlet at least once a year and check for the following:
 - The power cord's inner wires are exposed, broken, etc.
 - The power cord's coating has a crack or dent.
 - When bending the power cord, the power turns off and on.
 - Part of the power cord becomes hot.
 - The power cord is damaged.
- If any of the above conditions exist, do not use the power cord and consult your dealer or service representative. Use of the power cord could result in fire or electric shock.

CAUTION

- Be sure to push the plug of the power cord fully into the wall outlet. Partially inserted plugs create an unstable connection that can result in unsafe buildup of heat.

CAUTION

- If this machine is not going to be used for several days or longer at a time, disconnect its power cord from the wall outlet.

CAUTION

- When disconnecting the power cord from the wall outlet, always pull the plug, not the cord. Pulling the cord can damage the power cord. Use of damaged power cords could result in fire or electric shock.

CAUTION

- Be sure to disconnect the plug from the wall outlet and clean the prongs and the area around the prongs at least once a year. Allowing dust to build up on the plug constitutes a fire hazard.

CAUTION

- When performing maintenance on the machine, always disconnect the power cord from the wall outlet.

Handling the main machine

This section explains safety precautions about handling the main machine.

⚠ WARNING

- Be sure to locate the machine as close as possible to a wall outlet. This will allow easy disconnection of the power cord in the event of an emergency.

⚠ WARNING

- If the machine emits smoke or odours, or if it behaves unusually, you must turn off its power immediately. After turning off the power, be sure to disconnect the power cord plug from the wall outlet. Then contact your service representative and report the problem. Do not use the machine. Doing so could result in fire or electric shock.

⚠ WARNING

- If metal objects, or water or other fluids fall inside this machine, you must turn off its power immediately. After turning off the power, be sure to disconnect the power cord plug from the wall outlet. Then contact your service representative and report the problem. Do not use the machine. Doing so could result in fire or electric shock.

⚠ WARNING

- Do not touch this machine if a lightning strike occurs in the immediate vicinity. Doing so could result in electric shock.

⚠ WARNING

- The following explains the warning messages on the plastic bag used in this product's packaging.
 - Keep the polythene materials (bags, etc.) supplied with this machine away from babies and small children at all times. Suffocation can result if polythene materials are brought into contact with the mouth or nose.

⚠ CAUTION

- Unplug the power cord from the wall outlet before you move the machine. While moving the machine, take care that the power cord is not damaged under the machine. Failing to take these precautions could result in fire or electric shock.

⚠ CAUTION

- If you have to move the machine when the optional paper tray unit is attached, do not push on the main unit's top section. Doing so can cause the optional paper tray unit to detach, possibly resulting in injury.

⚠ CAUTION

- After you move the machine, use the caster fixture to fix it in place. Otherwise the machine might move or come down to cause an injury.

⚠ CAUTION

- If the lower paper tray is installed, do not pull out more than one tray at a time when you are changing or replenishing paper or resolving paper jams. Pressing down forcefully on the machine's upper surfaces can result in malfunctions and/or user injury.

⚠ CAUTION

- Contact your service representative if you need to lift the machine (such as when relocating it to another floor). Do not attempt to lift the machine without the assistance of your service representative. The machine will be damaged if it topples or is dropped, resulting in malfunction and risk of injury to users.

⚠ CAUTION

- Do not look into the lamp. It can damage your eyes.

⚠ CAUTION

- Do not hold the control panel while moving the machine. Doing so may damage the control panel, cause a malfunction, or result in injury.

⚠ CAUTION

- Keep your hands away from the hinges and exposure glass when lowering the ADF. Not doing so result in an injury if your hands or fingers are pinched.

Handling the machine's interior

This section explains safety precautions about handling the machine's interior.

⚠ WARNING

- Do not remove any covers or screws other than those explicitly mentioned in this manual. Inside this machine are high voltage components that are an electric shock hazard and laser components that could cause blindness. Contact your sales or service representative if any of the machine's internal components require maintenance, adjustment, or repair.
- Do not attempt to disassemble or modify this machine. Doing so risks burns and electric shock. Note again that exposure to the laser components inside this machine risks blindness.

⚠ CAUTION

- Some of this machine's internal components get very hot. For this reason, take care when removing misfed paper. Not doing so could result in burns.

⚠ CAUTION

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

⚠ CAUTION

- When loading paper, take care not to trap or injure your fingers.

⚠ CAUTION

- While safety measures have been installed to prevent accidents, you must not touch the machine's rollers while it is operating. Doing so could cause injury.

⚠ CAUTION

- If the machine's interior is not cleaned regularly, dust will accumulate. Fire and breakdown can result from heavy accumulation of dust inside this machine. Contact your sales or service representative for details about and charges for cleaning the machine's interior.

Handling the machine's supplies

This section explains safety precautions about handling the machine's supplies.

⚠ WARNING

- Do not incinerate toner (new or used) or toner containers. Doing so risks burns. Toner will ignite on contact with naked flame.

⚠ WARNING

- Do not store toner (new or used) or toner containers anywhere near naked flames. Doing so risks fire and burns. Toner will ignite on contact with naked flame.

⚠ WARNING

- Do not use a vacuum cleaner to remove spilled toner (including used toner). Absorbed toner may cause a fire or explosion due to electrical contact flickering inside the vacuum cleaner. However, it is possible to use a vacuum cleaner that is explosion-proof and dust ignition-proof. If toner is spilled on the floor, remove the spilled toner slowly using a wet cloth, so that the toner is not scattered.

WARNING

- The following explains the warning messages on the plastic bag used in this product's packaging.
 - Keep the polythene materials (bags, etc.) supplied with this machine away from babies and small children at all times. Suffocation can result if polythene materials are brought into contact with the mouth or nose.

CAUTION

- Do not crush or squeeze toner containers. Doing so can cause toner spillage, possibly resulting in dirtying of skin, clothing, and floor, and accidental ingestion.

CAUTION

- Store toner (new or used), toner containers, and components that have been in contact with toner out of reach of children.

CAUTION

- If toner or used toner is inhaled, gargle with plenty of water and move into a fresh air environment. Consult a doctor if necessary.

CAUTION

- If toner or used toner gets into your eyes, flush immediately with large amounts of water. Consult a doctor if necessary.

CAUTION

- If toner or used toner is swallowed, dilute by drinking a large amount of water. Consult a doctor if necessary.

CAUTION

- When replacing a toner or waste toner container or consumables with toner, make sure that the toner does not splatter. Put the waste consumables in a bag after they are removed. For consumables with a lid, make sure that the lid is shut.

CAUTION

- When removing jammed paper or replacing toner, avoid getting toner (new or used) on your clothing. If toner comes into contact with your clothing, wash the stained area with cold water. Hot water will set the toner into the fabric and make removing the stain impossible.

⚠ CAUTION

- When removing jammed paper or replacing toner, avoid getting toner (new or used) on your skin. If toner comes into contact with your skin, wash the affected area thoroughly with soap and water.

⚠ CAUTION

- Do not attempt to print on stapled sheets, aluminum foil, carbon paper, or any kind of conductive paper. Doing so risks fire.

⚠ CAUTION

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

Safety Labels of This Machine

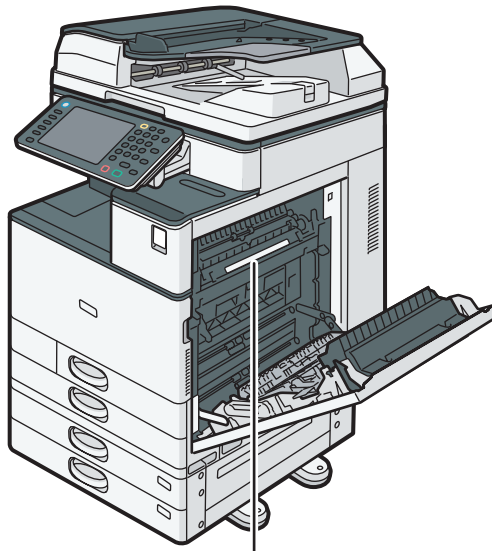
This section explains the machine's safety information labels.

2

Positions of WARNING and CAUTION labels

This machine has labels for ⚠WARNING and ⚠CAUTION at the positions shown below. For safety, please follow the instructions and handle the machine as indicated.

Main unit



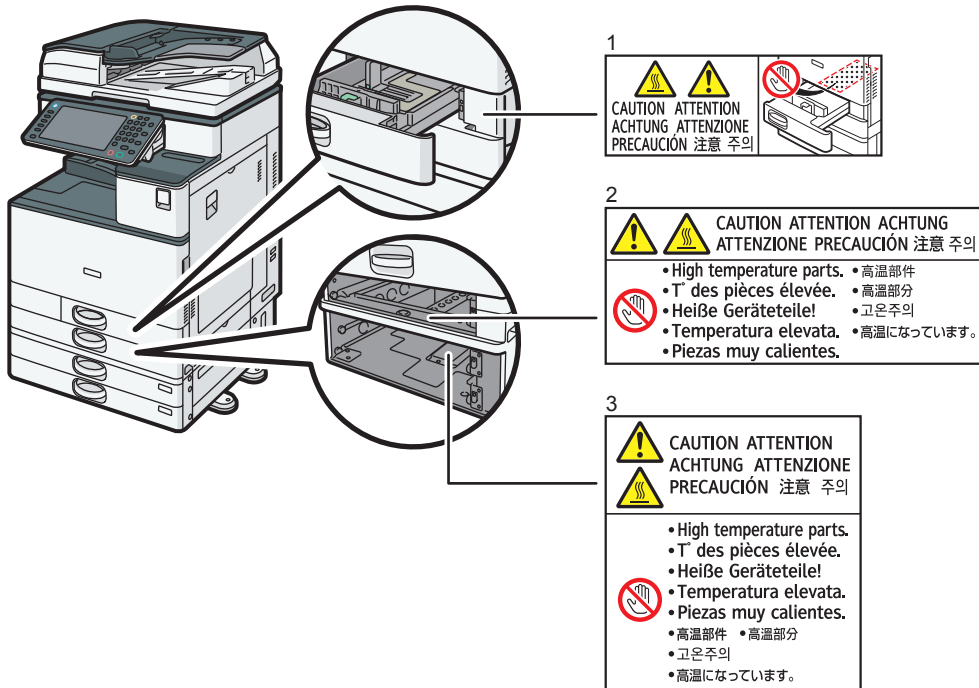
1

		120°C		CAUTION ACHTUNG ATTENTION ATTENZIONE PRECAUCIÓN 注意高温 高温注意 고온주의 高温注意
--	--	-------	--	--

DAR001

1. Do not touch the parts a label indicates. The inside of the machine could be very hot. Caution should be taken when removing misfed paper.

Paper trays



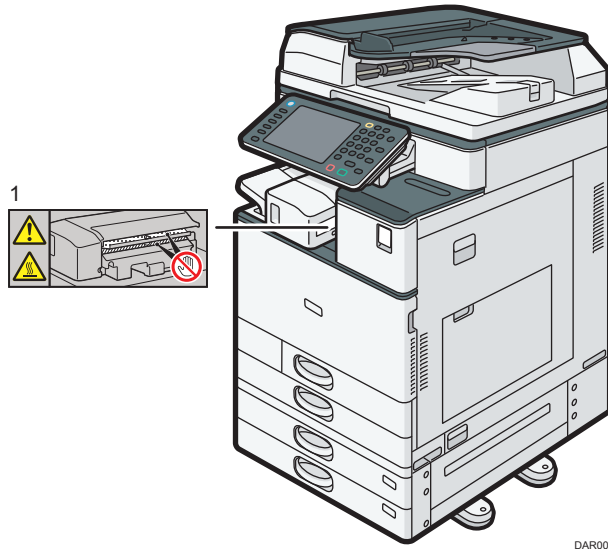
1, 2, and 3.

The inside of the machine could be very hot. Do not touch the parts which a label is put on. Otherwise, an injury might occur.

DAR002

Internal Finisher SR3180

2



DAR003

1.

The inside of the machine could be very hot. Do not touch the parts which a label is put on. Otherwise, an injury might occur.

Power Switch Symbols

The meanings of the symbols for the switches on this machine are as follows:

- I : POWER ON
- ⏻ : STANDBY

3. Other Information for This Machine

This chapter describes laws and regulations related to this machine.

Laws and Regulations

Duplication and Printing Prohibited

Do not copy or print any item for which reproduction is prohibited by law.

Copying or printing the following items is generally prohibited by local law:

bank notes, revenue stamps, bonds, stock certificates, bank drafts, checks, passports, driver's licenses.

The preceding list is meant as a guide only and is not inclusive. We assume no responsibility for its completeness or accuracy. If you have any questions concerning the legality of copying or printing certain items, consult with your legal advisor.

This machine is equipped with a function that prevents making counterfeit bank bills. Due to this function the original images similar to bank bills may not be copied properly.

Laser Safety

CDRH Regulations

This equipment complies with requirements of 21 CFR Subchapter J for class I laser product. This equipment contains four AlGaInP laser diodes, 655–663 nanometer wavelength for each emitter. The beam divergence angle is 21 degrees (minimum) and 29 degrees (maximum) in the vertical direction, and 7 degrees (minimum) and 11 degrees (maximum) in the horizontal direction, and laser beams are generated in Continuous Wave (CW) mode. The maximum output power of the light source is 10 milliwatt.

Caution:

Use of controls or adjustments or performance of procedures other than those specified in the manuals might result in hazardous radiation exposure.

Notes to USA Users of FCC Requirements

Part 15 of the FCC Rules

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection

against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio /TV technician for help.

Caution:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Declaration of Conformity

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible party: Ricoh Americas Corporation

Address: 5 Dedrick Place, West Caldwell, NJ 07006

Telephone number: 973-882-2000

Product Name: Multi Function Peripheral

Model Number:

- MP C2003SP/MP C2003SPG
- MP C2503SP/MP C2503SPG

Installing the Ferrite Core

A telephone line cable with a ferrite core must be used for RF interference suppression.

Part 68 of the FCC Rules regarding Facsimile Unit

1. This equipment complies with Part 68 of the FCC rules and requirements adopted by the ACTA. On the cover of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXXX. If requested, this number must be provided to the telephone company.

2. This equipment uses the RJ11C USOC jack.
3. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for detail.
4. The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. The REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3).
5. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
6. The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
7. If trouble is experienced with this equipment, for repair or warranty information, please contact Ricoh Americas Corporation Customer Support Department at 1-800-FASTFIX. If this device is causing problems with your telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.
8. In the event of operation problems (document jam, copy jam, communication error indication), see the manual provided with this machine for instruction on resolving the problem.
9. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
10. If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this equipment does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

WHEN PROGRAMMING EMERGENCY NUMBERS AND/OR MAKING TEST CALLS TO EMERGENCY NUMBERS:

1. Remain on the line and briefly explain to the dispatcher the reason for the call before hanging up.
2. Perform such activities in the off-peak hours, such as early morning hours or late evenings.

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device, including FAX machines, to send any message unless such message clearly

contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business or other entity, or other individual sending the message and the telephone number of the sending machine or such business, other entity, or individual. (The telephone number provided may not be a 900 number or any other number for which charges exceed local or long-distance transmission charges.)

In order to program this information into your FAX machine, you should complete the following steps: Follow the FAX HEADER programming procedure in the Programming chapter of the operating instructions to enter the business identification and telephone number of the terminal or business. This information is transmitted with your document by the FAX HEADER feature. In addition to the information, be sure to program the date and time into your machine.

3

Important Safety Instructions for Facsimile Unit

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use a telephone in the vicinity of a gas leak to report the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.

Save these instructions.

IMPORTANTES MESURES DE SÉCURITÉ de l'unité Fax

Certaines mesures de sécurité doivent être prises pendant l'utilisation de matériel téléphonique afin de réduire les risques d'incendie, de choc électrique et de blessures. En voici quelques-unes:

- Ne pas utiliser l'appareil près de l'eau, p.ex., près d'une baignoire, d'un lavabo, d'un évier de cuisine, d'un bac à laver, dans un sous-sol humide ou près d'une piscine.
- Éviter d'utiliser le téléphone (sauf s'il s'agit d'un appareil sans fil) pendant un orage électrique. Ceci peut présenter un risque de choc électrique causé par la foudre.
- Ne pas utiliser l'appareil téléphonique pour signaler une fuite de gaz s'il est situé près de la fuite.
- Utiliser seulement le cordon d'alimentation et le type de piles indiqués dans ce manuel. Ne pas jeter les piles dans le feu: elles peuvent exploser. Se conformer aux règlements pertinents quant à l'élimination des piles.

Conserver ces instructions.

Notes to Canadian Users of Facsimile Unit

This product meets the applicable Industry Canada technical specifications.

The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

Remarques à l'attention des utilisateurs canadiens de l'unité Fax

Le présent matériel est conforme aux spécifications techniques applicables d'Industrie Canada.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Other Information

Notes to users in the state of California (Notes to Users in USA)

Perchlorate Material - special handling may apply. See: www.dtsc.ca.gov/hazardouswaste/perchlorate

4. Appendix

This appendix describes trademarks for the machine.

Trademarks

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

Firefox is a registered trademark of the Mozilla Foundation.

Macintosh and Safari are trademarks of Apple Inc., registered in the United States and other countries.

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

The SD is a trademark of SD-3C, LLC.

The proper name of Internet Explorer 6 is Microsoft® Internet Explorer® 6.

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

- The product names of Windows XP are as follows:

Microsoft® Windows® XP Professional

Microsoft® Windows® XP Home Edition

Microsoft® Windows® XP Media Center Edition

Microsoft® Windows® XP Tablet PC Edition

- The product names of Windows Vista are as follows:

Microsoft® Windows Vista® Ultimate

Microsoft® Windows Vista® Business

Microsoft® Windows Vista® Home Premium

Microsoft® Windows Vista® Home Basic

Microsoft® Windows Vista® Enterprise

- The product names of Windows 7 are as follows:

Microsoft® Windows® 7 Home Premium

Microsoft® Windows® 7 Professional

Microsoft® Windows® 7 Ultimate

Microsoft® Windows® 7 Enterprise

- The product names of Windows 8 are as follows:

Microsoft® Windows® 8

Microsoft® Windows® 8 Pro

Microsoft® Windows® 8 Enterprise

- The product names of Windows Server 2003 are as follows:
Microsoft® Windows Server® 2003 Standard Edition
Microsoft® Windows Server® 2003 Enterprise Edition
- The product names of Windows Server 2003 R2 are as follows:
Microsoft® Windows Server® 2003 R2 Standard Edition
Microsoft® Windows Server® 2003 R2 Enterprise Edition
- The product names of Windows Server 2008 are as follows:
Microsoft® Windows Server® 2008 Standard
Microsoft® Windows Server® 2008 Enterprise
- The product names of Windows Server 2008 R2 are as follows:
Microsoft® Windows Server® 2008 R2 Standard
Microsoft® Windows Server® 2008 R2 Enterprise
- 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

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.





User Guide

What You Can Do with This Machine	1
Getting Started	2
Copy	3
Fax	4
Print	5
Scan	6
Document Server	7
Web Image Monitor	8
Adding Paper and Toner	9
Troubleshooting	10



For information not in this manual, refer to the HTML/PDF files on the supplied CD-ROM.








TABLE OF CONTENTS



How to Read the Manuals.....	6
Symbols Used in the Manuals.....	6
Model-Specific Information.....	7
Names of Major Features.....	8

1. What You Can Do with This Machine

Reducing my Costs.....	9
Converting Documents to Electronic Formats Easily.....	10
Registering Destinations.....	11
Operating the Machine More Effectively.....	12
Customizing the [Home] Screen.....	13
Making Copies Using Various Functions.....	14
Printing Data Using Various Functions.....	16
Utilizing Stored Documents.....	17
Sending and Receiving Faxes without Paper.....	18
Sending and Receiving Faxes via the Internet.....	20
Sending and Receiving Faxes by Using the Machine without Fax Unit Installed.....	22
Using the Facsimile and the Scanner in a Network Environment.....	23
Embedding Text Information in Scanned Files.....	24
Preventing Information Leakage (Security Functions).....	25
Centrally Controlling Scan Conditions and Distribution.....	26
Monitoring and Setting the Machine Using a Computer.....	27
Preventing Unauthorized Copying.....	28

2. Getting Started

Guide to Names and Functions of Components.....	29
Guide to Components  Region A (mainly Europe and Asia).....	29
Guide to Components  Region B (mainly North America).....	32
Guide to Functions of the Machine's Options.....	36
Guide to Functions of the Machine's External Options  Region A (mainly Europe).....	36
Guide to Functions of the Machine's External Options  Region A (mainly Asia).....	37
Guide to Functions of the Machine's External Options  Region B (mainly North America).....	39
Guide to the Names and Functions of the Machine's Control Panel (When Using the Standard Operation Panel).....	41

Guide to the Names and Functions of the Machine's Control Panel (When Using the Smart Operation Panel).....	44
Changing the Display Language.....	46
Changing the Display Language (When Using the Smart Operation Panel).....	46
How to Use the [Home] Screen (When Using the Standard Operation Panel).....	47
Adding Icons to the [Home] Screen (When Using the Standard Operation Panel).....	48
How to Use the [Home] Screen (When Using the Smart Operation Panel).....	52
Adding Icons to the [Home] Screen (When Using the Smart Operation Panel).....	53
Registering Functions in a Program.....	57
Example of Programs.....	60
Turning On/Off the Power.....	63
Turning On the Main Power.....	63
Turning Off the Main Power.....	63
When the Authentication Screen is Displayed.....	64
User Code Authentication Using the Control Panel.....	64
Logging In Using the Control Panel (When Using the Standard Operation Panel).....	64
Logging In Using the Control Panel (When Using the Smart Operation Panel).....	65
Logging Out Using the Control Panel (When Using the Standard Operation Panel).....	66
Logging Out Using the Control Panel (When Using the Smart Operation Panel).....	66
Placing Originals.....	67
Placing Originals on the Exposure Glass  Region A (mainly Europe and Asia).....	67
Placing Originals on the Exposure Glass  Region B (mainly North America).....	67
Placing Originals in the Auto Document Feeder.....	68

3. Copy

Basic Procedure.....	71
Auto Reduce / Enlarge.....	73
Duplex Copying.....	75
Specifying the Original and Copy Orientation.....	77
Combined Copying.....	79
One-Sided Combine.....	80
Two-Sided Combine.....	81
Copying onto Custom Size Paper from the Bypass Tray.....	84
Copying onto Envelopes.....	85

Copying onto Envelopes from the Bypass Tray.....	85
Copying onto Envelopes from the Paper Tray.....	86
Sort.....	87
Changing the Number of Sets.....	88
Storing Data in the Document Server.....	90

4. Fax

Basic Procedure for Transmissions (Memory Transmission).....	91
Sending Originals Using the Exposure Glass (Memory Transmission).....	93
Registering a Fax Destination.....	94
Deleting a Fax Destination.....	95
Transmitting while Checking Connection to Destination (Immediate Transmission).....	97
Sending Originals Using the Exposure Glass (Immediate Transmission).....	98
Canceling a Transmission.....	100
Canceling a Transmission Before the Original Is Scanned.....	100
Canceling a Transmission While the Original Is Being Scanned.....	100
Canceling a Transmission After the Original Is Scanned.....	101
Storing a Document.....	103
Sending Stored Documents.....	104
Printing the Journal Manually.....	106

5. Print

Quick Install.....	107
Displaying the Printer Driver Properties.....	108
Standard Printing.....	109
When Using the PCL 6 Printer Driver.....	109
Printing on Both Sides of Sheets.....	110
When Using the PCL 6 Printer Driver.....	110
Types of 2 sided Printing.....	110
Combining Multiple Pages into Single Page.....	111
When Using the PCL 6 Printer Driver.....	111
Types of Combine Printing.....	111
Printing on Envelopes.....	113
Configuring Envelope Settings Using the Control Panel.....	113
Printing on Envelopes Using the Printer Driver.....	114

Saving and Printing Using the Document Server.....	115
Storing Documents in Document Server.....	115
Managing Documents Stored in Document Server.....	116

6. Scan

Basic Procedure When Using Scan to Folder.....	117
Creating a Shared Folder on a Computer Running Windows/Confirming a Computer's Information.....	118
Registering an SMB Folder.....	120
Deleting an SMB Registered Folder.....	124
Entering the Path to the Destination Manually.....	125
Basic Procedure for Sending Scan Files by E-mail.....	126
Registering an E-mail Destination.....	127
Deleting an E-mail Destination.....	129
Entering an E-mail Address Manually.....	130
Basic Procedure for Storing Scan Files.....	131
Checking a Stored File Selected from the List.....	132
Specifying the File Type.....	134
Specifying Scan Settings.....	135

7. Document Server

Storing Data.....	137
Printing Stored Documents.....	139

8. Web Image Monitor

Displaying Top Page.....	141
--------------------------	-----

9. Adding Paper and Toner

Precautions for Loading Paper.....	143
Loading Paper into Paper Trays.....	144
Loading Paper into the Bypass Tray.....	146
Printing from the Bypass Tray Using the Printer Function.....	147
Loading Orientation-fixed Paper or Two-sided Paper.....	152
Recommended Paper Sizes and Types.....	155
Thick Paper.....	162
Envelopes.....	163
Adding Toner.....	167

Sending Faxes or Scanned Documents When Toner Has Run Out.....	169
Disposing of Used Toner.....	169
10. Troubleshooting	
When a Status Icon Is Displayed.....	171
When the Indicator Lamp for the [Check Status] Key Is Lit or Flashing.....	173
When the Machine Makes a Beeping Sound.....	175
When You Have Problems Operating the Machine.....	176
When Multiple Functions Cannot Be Executed Simultaneously.....	181
Messages Displayed When Using the Copy/Document Server Function.....	182
Messages Displayed When Using the Facsimile Function.....	186
When There Is a Problem Specifying the Network Settings.....	187
When the Remote Fax Function Cannot Be Used.....	193
Messages Displayed When Using the Printer Function.....	196
Messages Displayed on the Control Panel When Using the Printer Function.....	196
Messages Printed on the Error Logs or Reports When Using the Printer Function.....	199
Messages Displayed When Using the Scanner Function.....	209
Messages Displayed on the Control Panel When Using the Scanner Function.....	209
Messages Displayed on the Client Computer.....	218
When Other Messages Appear.....	225
When There Is a Problem Scanning or Storing Originals.....	226
When the Home Screen Cannot Be Edited (When Using the Standard Operation Panel).....	227
When the Address Book Is Updated.....	228
When Data Cannot Be Sent Due to a Problem with the Destination.....	229
When the Machine Cannot Be Operated Due to a Problem with the User Certificate.....	229
When Problems Occur While Logging In.....	231
When the User Lacks Privileges to Perform an Operation.....	231
When the LDAP Server Cannot Be Used.....	231
INDEX	233

How to Read the Manuals

Symbols Used in the Manuals

This manual uses the following symbols:

 **Important**

Indicates points to pay attention to when using the machine, and explanations of likely causes of paper misfeeds, damage to originals, or loss of data. Be sure to read these explanations.

 **Note**


Indicates supplementary explanations of the machine's functions, and instructions on resolving user errors.

 **Reference**

This symbol is located at the end of sections. It indicates where you can find further relevant information.

[]

Indicates the names of keys on the machine's display or control panels.

 **Region A** (mainly Europe and Asia), (mainly Europe), or (mainly Asia)

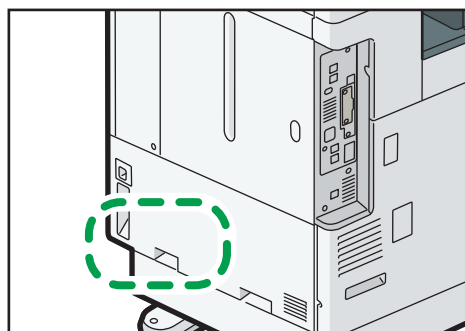
 **Region B** (mainly North America)

Differences in the functions of Region A and Region B models are indicated by two symbols. Read the information indicated by the symbol that corresponds to the region of the model you are using. For details about which symbol corresponds to the model you are using, see page 7 "Model-Specific Information".

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 -25, -27, -29
- 220–240 V

Region **B** (mainly North America)

If the label contains the following, your machine is a region B model:

- CODE XXXX -17, -18
- 120–127 V

Note

- Dimensions in this manual are given in two units of measure: metric and inch. If your machine is a Region A model, refer to the metric units. If your machine is a Region B model, refer to the inch units.
- If your machine is a region A model and "CODE XXXX -25, -27" is printed on the label, see " Region **A** (mainly Europe)" also.
- If your machine is a region A model and "CODE XXXX -29" is printed on the label, see " Region **A** (mainly Asia)" also.

Names of Major Features

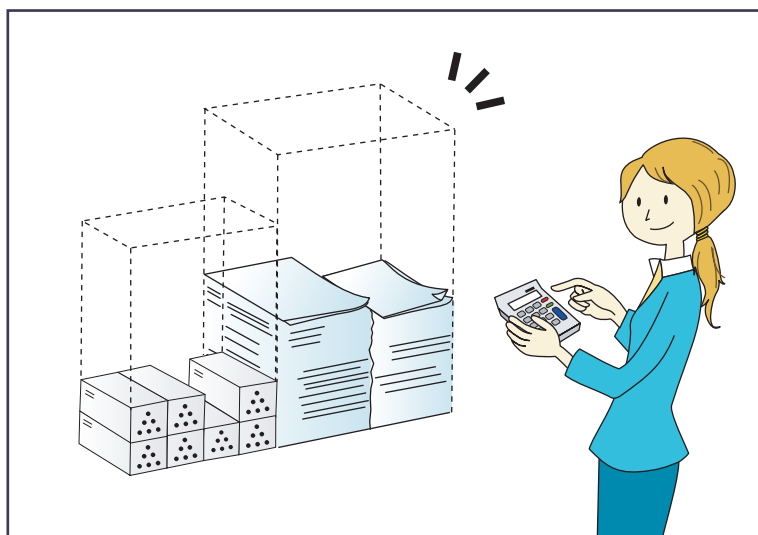
In this manual, major features of the machine are referred to as follows:

- Auto Document Feeder → ADF

1. What You Can Do with This Machine

You can search for a description by what you want to do.

Reducing my Costs



BRL059S

Printing multi-page documents on both sides of sheets (Duplex Copy)

⇒ See "Duplex Copying", Copy/ Document Server.

Printing multi-page documents and received faxes on a single sheet (Combine (Copier/Fax))

⇒ See "Combined Copying", Copy/ Document Server.

⇒ See "Combine Two Originals", Fax.

Printing received faxes on both sides of sheets (2 Sided Print)

⇒ See "Two-Sided Printing", Fax.

Converting received faxes to electronic formats (Paperless Fax)

⇒ See "Confirming/Printing/Deleting Received and Stored Documents", Fax.

Sending files from the computer without printing them (LAN-Fax)

⇒ See "Sending Fax Documents from Computers", Fax.

Checking how much paper is saved ([Information] screen)

⇒ See "How to Use the [Information] Screen", Getting Started.

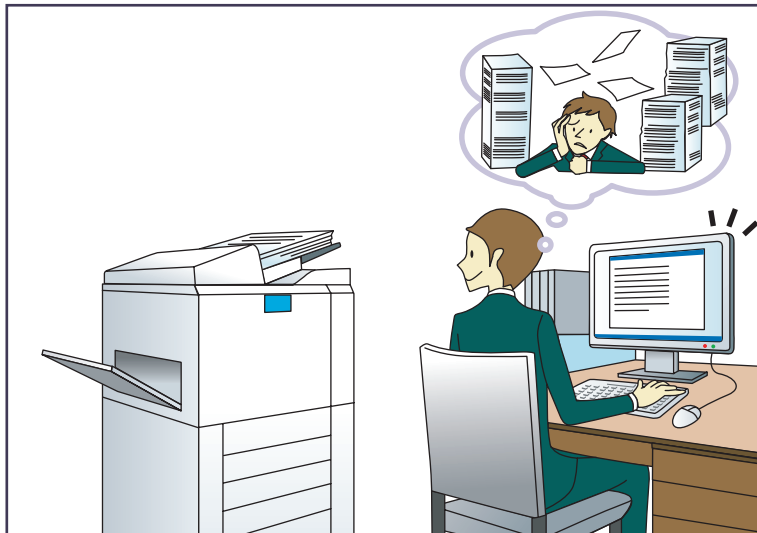
Reducing electricity consumption

⇒ See "Saving Energy", Getting Started.

⇒ See "Timer Settings", Connecting the Machine/ System Settings.

Converting Documents to Electronic Formats Easily

1



BQX138S

Sending scan files

⇒ See "Basic Procedure for Sending Scan Files by E-mail", Scan.

Sending the URL of the folder in which scan files are stored

⇒ See "Sending the URL by E-mail", Scan.

Storing scan files in a shared folder

⇒ See "Basic Procedure When Using Scan to Folder", Scan.

Storing scan files on media

⇒ See "Basic Procedure for Saving Scan Files on a Memory Storage Device", Scan.

Embedding text information in scanned files

⇒ See "Embedding Text Information in Scanned Data", Scan.

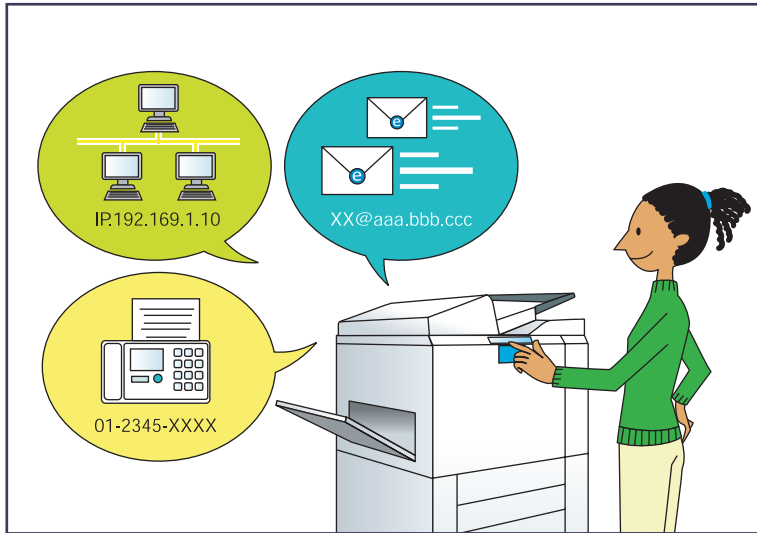
Converting transmitted faxes to electronic formats and sending them to a computer

⇒ See "Overview of Folder Transmission Function", Fax.

Managing and using documents converted to electronic formats (Document Server)

⇒ See "Relationship between Document Server and Other Functions", Copy/ Document Server.

Registering Destinations



Using the control panel to register destinations in the Address Book

- ⇒ See "Registering Entered Destinations to the Address Book", Fax.
- ⇒ See "Registering a destination in the address book manually", Scan.

Using Web Image Monitor to register destinations from a computer

- ⇒ See "Registering Internet Fax Destination Information Using Web Image Monitor", Fax.

Downloading destinations registered in the machine to the LAN-Fax driver destination list

- ⇒ See "Using the machine's Address Book as the LAN-Fax destination list", Fax.

Operating the Machine More Effectively

1



Registering and using frequently-used settings (Program)

⇒ See "Registering Functions in a Program", Convenient Functions.

Registering frequently-used settings as initial settings (Program as Defaults (Copier/Document Server/Fax/Scanner))

⇒ See "Changing the Default Functions of the Initial Screen", Convenient Functions.

Registering frequently-used printing settings to the printer driver

⇒ See "Using One Click Presets", Print.

Changing the initial settings of the printer driver to frequently-used printing settings

⇒ See "Displaying the Printing Preferences Dialog Box", Print.

Adding shortcuts to frequently used programs or Web pages

⇒ See "Adding Icons to the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions.

⇒ See "Adding Icons to the [Home] Screen (When Using the Smart Operation Panel)", Convenient Functions.

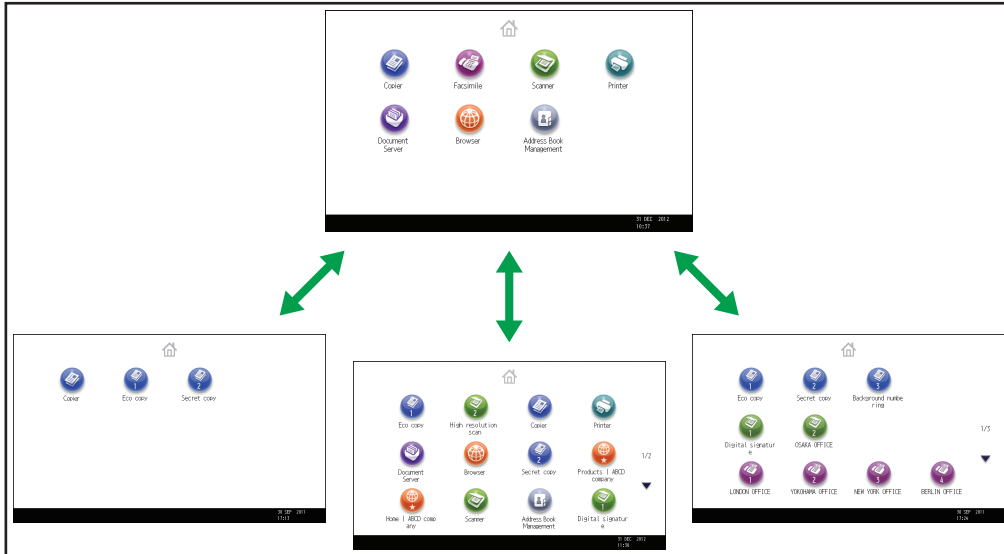
Changing the order of the function and shortcut icons

⇒ See "Changing the Order of Icons on the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions.

⇒ See "Changing the Order of Icons on the [Home] Screen (When Using the Smart Operation Panel)", Convenient Functions.

Customizing the [Home] Screen

The icons of each function are displayed on the [Home] screen.



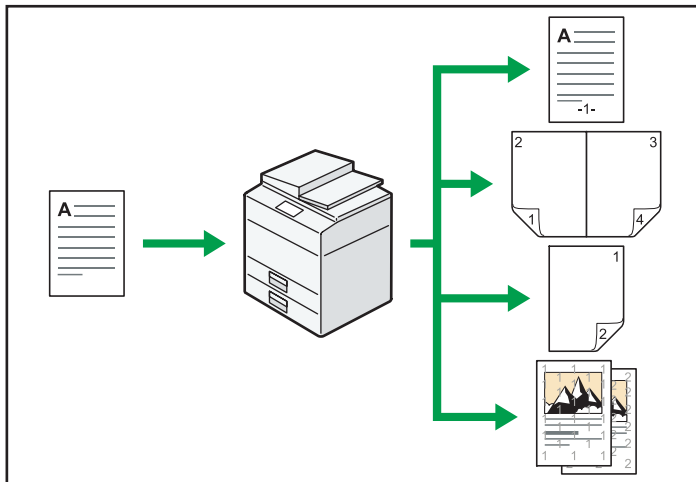
CUM001

- You can add shortcuts to often used programs or Web pages to the [Home] screen. The programs or Web pages can be recalled easily by pressing the shortcut icons.
- You can display only the icons of functions and shortcuts that you use.
- You can change the order of the function and shortcut icons.

Reference

- For details about the features on the [Home] screen, see "How to Use the [Home] Screen (When Using the Standard Operation Panel)" and "How to Use the [Home] Screen (When Using the Smart Operation Panel)", Getting Started.
- For details about how to customize the [Home] screen, see "Types of [Home] Screens and How to Customize Them (When Using the Standard Operation Panel)" and "How to Customize the [Home] Screen (When Using the Smart Operation Panel)", Convenient Functions.

Making Copies Using Various Functions

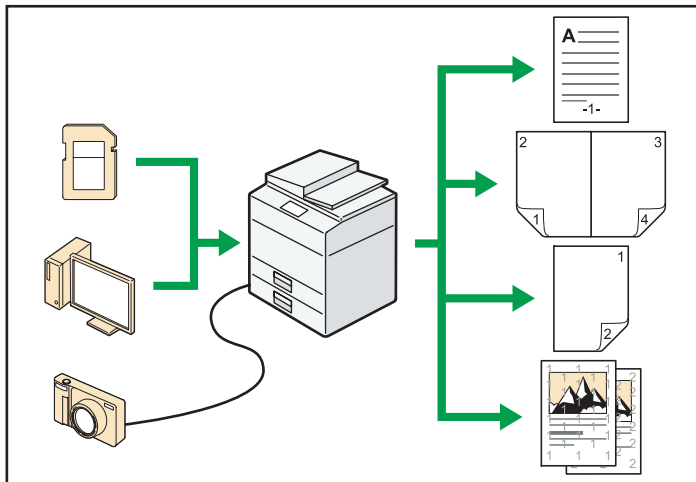


CJ0601

- You can make copies in full color. You can switch the color copy mode depending on the type of originals used and the desired finish.
⇒ See "Copying in Color", Copy/ Document Server.
- You can print stamps on copies. Stamps can include background numbers, scanned images, dates, and page numbers.
⇒ See "Stamps", Copy/ Document Server.
- You can adjust the color tones and image quality of your copies.
⇒ For details about a color adjustment, see "Adjusting Color", Copy/ Document Server.
⇒ For details about an image adjustment, see "Image Adjustment", Copy/ Document Server.
- You can reduce or enlarge the copy image. Auto Reduce / Enlarge function enables the machine to detect the original size automatically. Also, it enables the machine to select an appropriate reproduction ratio based on the paper size you specify. If the orientation of the original is different from that of the paper you are copying onto, the machine rotates the original image by 90 degrees to match it with the copy paper.
⇒ See "Reducing or Enlarging Originals", Copy/ Document Server.
- Copier functions such as Duplex, Combine, Booklet, and Magazine allow you to save on paper by copying multiple pages onto single sheets.
⇒ For details about duplex copying, see "Duplex Copying", Copy/ Document Server.
⇒ For details about combined copying, see "Combined Copying", Copy/ Document Server.
⇒ For details about combined copying, see "Booklet/Magazine", Copy/ Document Server.
- You can copy onto various types of paper such as envelopes and OHP transparencies.
⇒ See "Copying onto Various Types of Paper", Copy/ Document Server.

- The finisher allows you to sort, staple, and punch holes in your copies.
⇒ See "Finishing", Copy/ Document Server.

Printing Data Using Various Functions

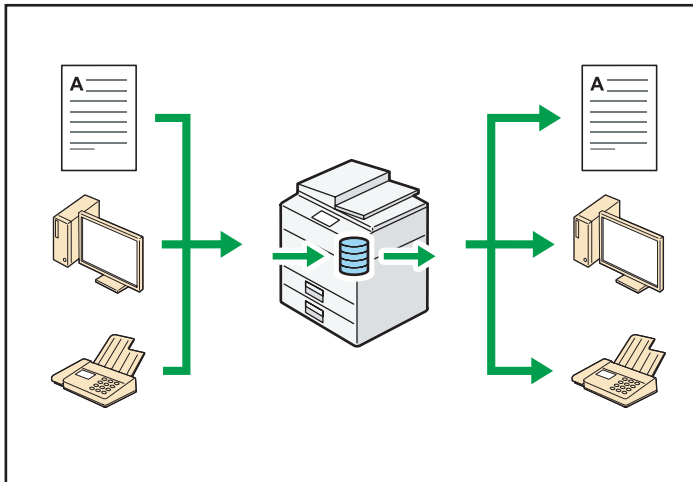


CJQ602

- This machine supports network and local connections.
- You can send PDF files directly to the machine for printing, without having to open a PDF application.
 - ⇒ See "Printing a PDF File Directly", Print.
- You can print or delete print jobs stored on the machine's hard disk, which have been previously sent from computers using the printer driver. The following types of print jobs can be selected: Sample Print, Locked Print, Hold Print, and Stored Print.
 - ⇒ See "Storing Documents in the Hard Disk Drive and Printing them", Print.
- The finisher allows you to collate, staple, and punch holes in your prints.
 - ⇒ For details about stapling, see "Staple", Print.
 - ⇒ For details about punching, see "Punch", Print.
- If the PictBridge card is installed, you can connect a PictBridge-compatible digital camera to this machine using a USB cable. This allows you to print the photographs stored on the camera using the camera's own interface.
 - ⇒ See "Direct Printing from a Digital Camera (PictBridge)", Print.
- You can print files stored on a removable memory device and specify print conditions such as print quality and print size.
 - ⇒ See "Direct Printing from a Memory Storage Device", Print.

Utilizing Stored Documents

You can store files scanned in copier, facsimile, printer, or scanner mode on the machine's hard disk. Web Image Monitor allows you to use your computer to search for, view, print, delete, and send stored files via the network. You can also change print settings and print multiple documents (Document Server).



CJQ603

- You can retrieve stored documents scanned in scanner mode to your computer.
- Using the file format converter, you can download documents stored in copier, Document Server, or printer mode to your computer.

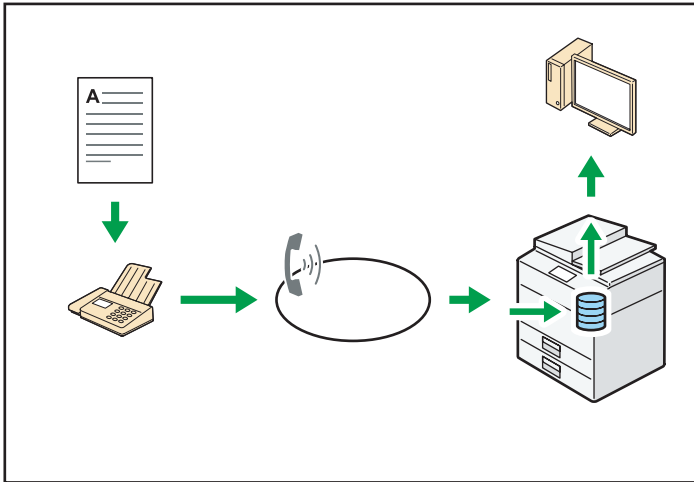
Reference

- For details about how to use the Document Server, see "Storing Data in the Document Server", Copy/ Document Server
- For details about the Document Server in copier mode, see "Document Server", Copy/ Document Server.
- For details about the Document Server in printer mode, see "Saving and Printing Using the Document Server", Print.
- For details about the Document Server in fax mode, see "Storing a Document", Fax.
- For details about the Document Server in scanner mode, see "Storing and Saving the Scanned Documents", Scan.

Sending and Receiving Faxes without Paper

Reception

You can store and save received fax documents as electronic formats in the machine's hard disk without printing them.



CJQ604

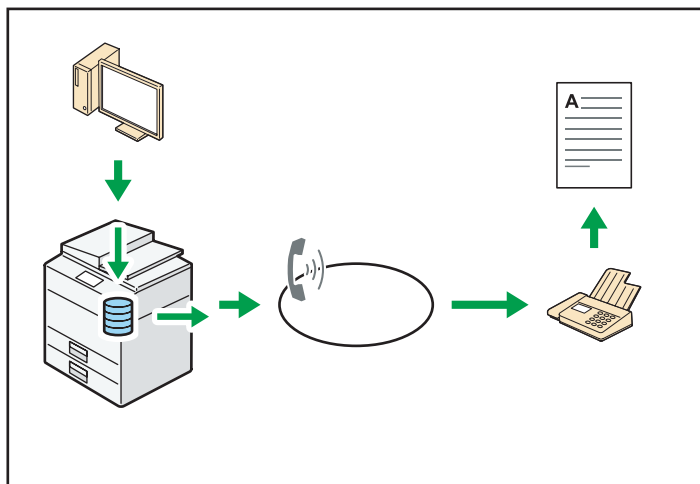
You can use Web Image Monitor to check, print, delete, retrieve, or download documents using your computer (Storing received documents).

Reference

- See "Confirming/Printing/Deleting Received and Stored Documents", Fax.

Transmission

You can send a fax from your computer over the network (Ethernet or wireless LAN) to this machine, which then forwards the fax via its telephone connection (LAN-Fax).



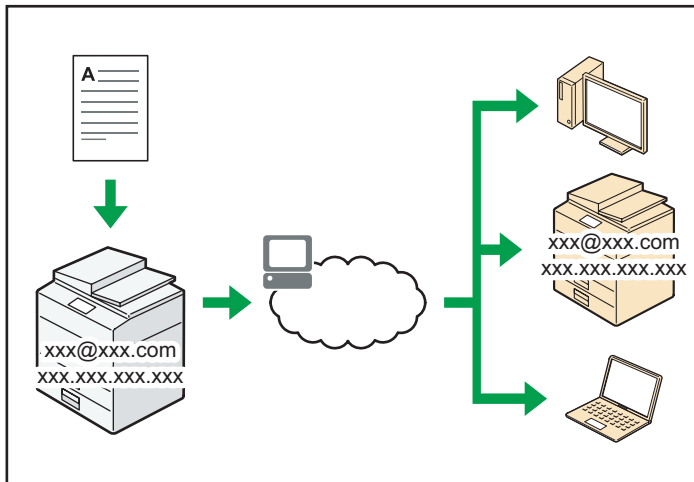
CJQ605

- To send a fax, print from the Windows application you are working with, select LAN-Fax as the printer, and then specify the destination.
- You can also check the sent image data.

Reference

- For details about the machine's settings, see "Network Settings Requirements", Connecting the Machine/ System Settings.
- For details about how to use the function, see "Sending Fax Documents from Computers", Fax.

Sending and Receiving Faxes via the Internet



CJ0606

E-mail Transmission and Reception

This machine converts scanned document images to e-mail format, and transmits and receives the e-mail data over the Internet.

- To send a document, specify an e-mail address instead of dialing the destination telephone number (Internet Fax and e-mail transmission).
⇒ See "Specifying an Internet Fax Destination by Entering It Manually", Fax.
- This machine can receive e-mail messages via Internet Fax or from computers (Internet Fax Reception and Mail to Print).
⇒ See "Receiving E-mail by Internet Fax/Mail to Print", Fax
- Internet Fax compatible machines and computers that have e-mail addresses can receive e-mail messages via Internet Fax.

IP-Fax

The IP-Fax function sends or receives documents between two facsimiles directly via a TCP/IP network.

- To send a document, specify an IP address or host name instead of a fax number (IP-Fax Transmission).
⇒ See "Specifying an IP-Fax Destination by Entering It Manually", Fax.
- This machine can receive documents sent via Internet Fax (IP-Fax Reception).
⇒ See "Types of Reception", Fax.
- Using a VoIP gateway, this machine can send to G3 facsimiles connected to the public switched telephone network (PSTN).

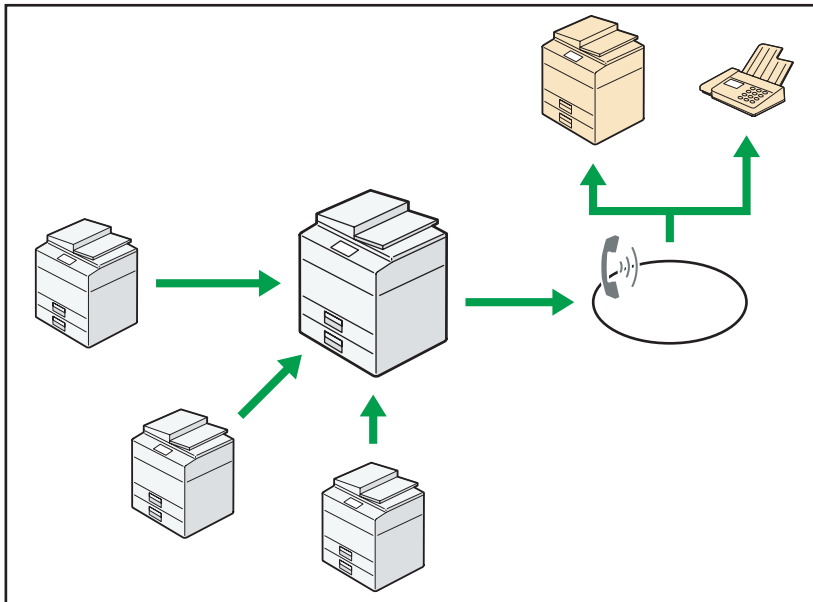
 **Reference**

- For details about the machine's settings, see "Network Settings Requirements", Connecting the Machine/ System Settings.

Sending and Receiving Faxes by Using the Machine without Fax Unit Installed

1

You can send and receive faxes through a different machine's fax functions via a network (Remote Fax).



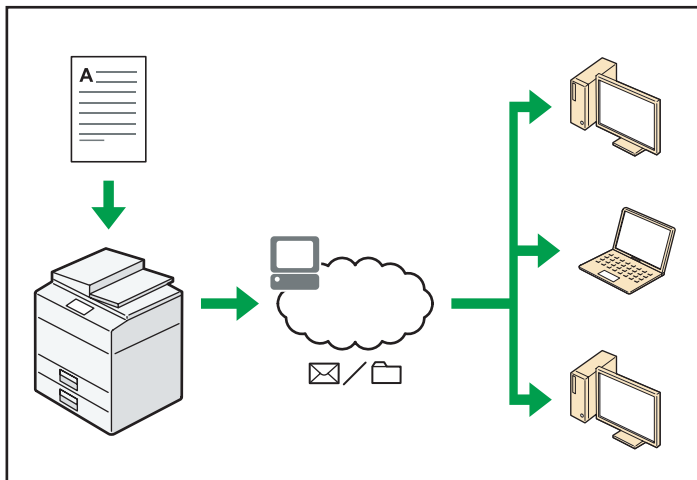
CJ0612

- To use the remote fax function, install the fax connection unit on the main-machine and sub-machine.
- The procedure for sending faxes is as same as that of for the machine with the fax unit. When a job has finished, confirm results displayed on sending history or printed on reports.
- You can forward documents received by the main machine with the facsimile function to sub-machines.

Reference

- For details, see "Sending/Receiving Documents Using a Remote Machine (Remote Fax)", Fax.

Using the Facsimile and the Scanner in a Network Environment



CJ0607

- You can send scan files to a specified destination using e-mail (Sending scan files by e-mail).
 - ⇒ See "Overview of E-mail Transmission Function", Fax.
 - ⇒ See "Basic Procedure for Sending Scan Files by E-mail", Scan.
- You can send scan files directly to folders (Sending scan files by Scan to Folder).
 - ⇒ See "Overview of Folder Transmission Function", Fax.
 - ⇒ See "Basic Procedure When Using Scan to Folder", Scan.
- You can use this machine as a delivery scanner for the ScanRouter delivery software^{*1} (Network delivery scanner). You can save scan files in the delivery server or send them to a folder in a computer on the same network.
 - ⇒ See "Basic Procedure for Delivering Files", Scan.
- You can use Web Services on Devices (WSD) to send scan files to a client computer.
 - ⇒ See "Basic Operating Procedure of WSD Scanner (Push Type)", Scan.

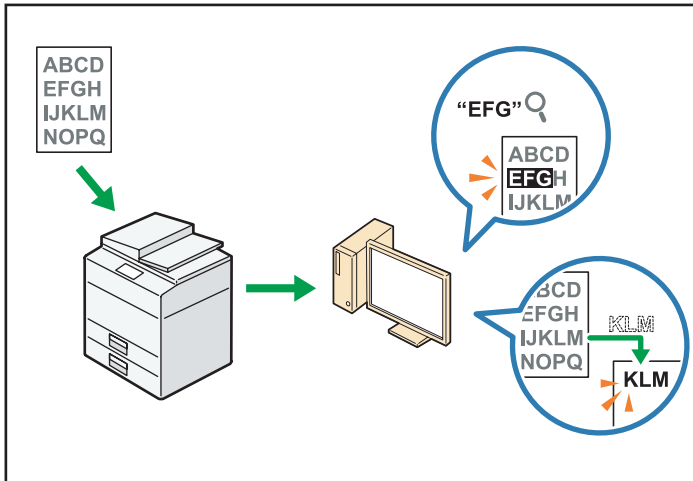
*1 The ScanRouter delivery software is no longer available for sale.

Embedding Text Information in Scanned Files

1

You can extract text information from a scanned document and embed it in the file without using a computer.

If you scan a document using this function, embedded text can be searched by using the text search function or copied to another document.



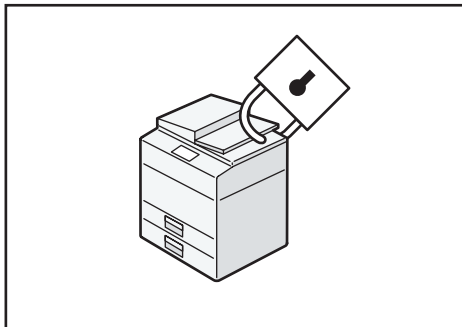
CUL003

- To use this function, the optional OCR unit is required.
- You can select a file type from [PDF], [High Compression PDF], or [PDF/A].
- This function can optically recognize characters in various languages and up to approximately 40,000 characters a page.

Reference

- See "Embedding Text Information in Scanned Data", Scan.

Preventing Information Leakage (Security Functions)



CJ0608

- You can protect documents from unauthorized access and stop them from being copied without permission.
- You can control the use of the machine, as well as prevent machine settings from being changed without authorization.
- By setting passwords, you can prevent unauthorized access via the network.
- You can erase or encrypt the data on the hard disk to minimize the risk of information leakage.
- You can limit the usage of functions for each user.

Reference

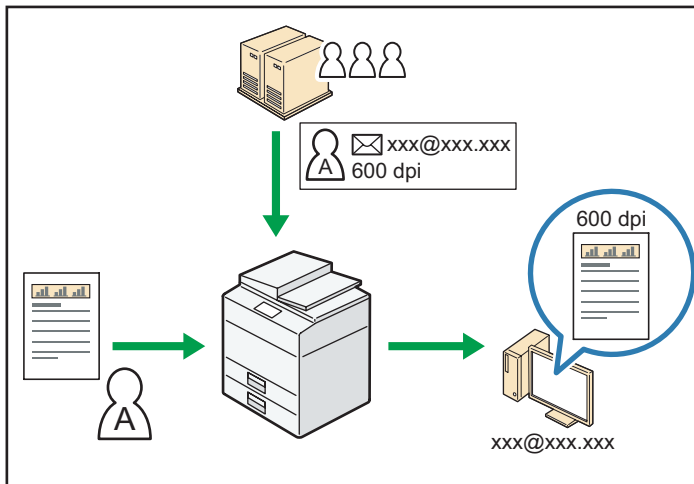
- See Security Guide.

Centrally Controlling Scan Conditions and Distribution

1

You can use the distributed scan management (DSM) system in Windows Server 2008 R2 to manage the destinations and scan settings for each individual user in a group and to use the information when distributing scanned data.

You can also use this system to centrally manage information about people using the network and the machine's scanner functions. Both delivered files and user information can be controlled.



CUL004

- You must set up and configure a Windows server to use the distributed scan management system. This system is supported under Windows Server 2008 R2.

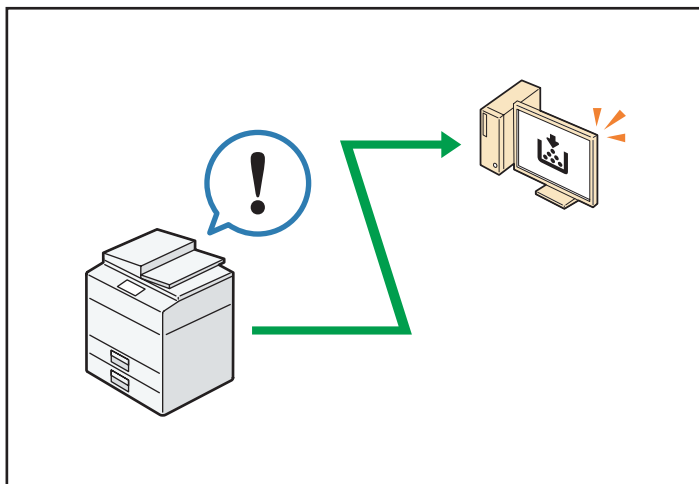
Reference

- For details about how to deliver files using the distributed scan management system, see "Managing Scan Conditions and Other Settings in the Block using Distributed Scan Management", Scan.

Monitoring and Setting the Machine Using a Computer

1

Using Web Image Monitor, you can check the machine's status and change the settings.



You can check which tray is running out of paper, register information in the Address Book, specify the network settings, configure and change the system settings, manage jobs, print the job history, and configure the authentication settings.

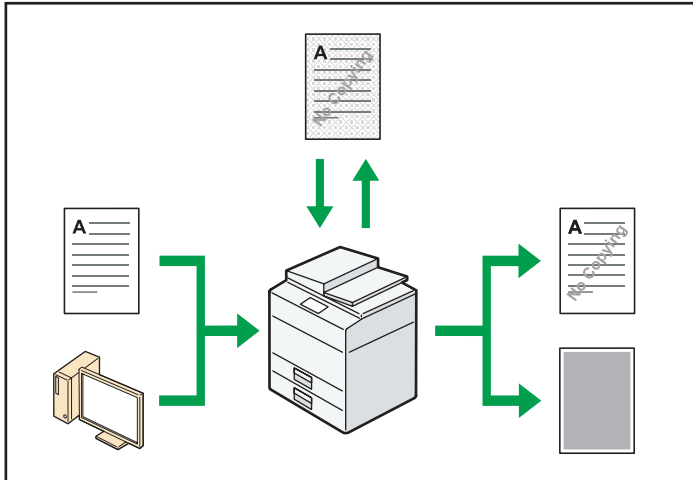
Reference

- See "Using Web Image Monitor", Connecting the Machine/ System Settings.
- See Web Image Monitor Help.

Preventing Unauthorized Copying

You can print embedded patterns on printouts to prevent unauthorized copying.

1



- Using the copier function or the printer driver, you can embed a pattern in the printed document. If the document is copied on a machine with the Copy Data Security unit, protected pages are grayed out in the copy. This can minimize the risk of confidential information being copied. Protected fax messages are grayed out before being transmitted or stored. If a document protected by unauthorized copy guard is copied on a machine that is equipped with the Copy Data Security unit, the machine beeps to notify users that unauthorized copying is being attempted. If the document is copied on a machine without the Copy Data Security Unit, the hidden text becomes conspicuous in the copy, showing that the copy is unauthorized.
- Using the copier function or the printer driver, you can embed text in the printed document for unauthorized copy prevention. If the document is copied, scanned, or stored in a Document Server by a copier or multifunction printer, the embedded text appears conspicuous in the copy, discouraging such unauthorized copying.

Reference

- For details, see the printer driver Help and Security Guide.
- For details about this function in the copier mode, see "Preventing Unauthorized Copies", Copier/Document Server.
- For details about this function in the printer mode, see "Printing Documents that Are Not Authorized for Duplication", Print.

2. Getting Started

This chapter describes how to start using this machine.

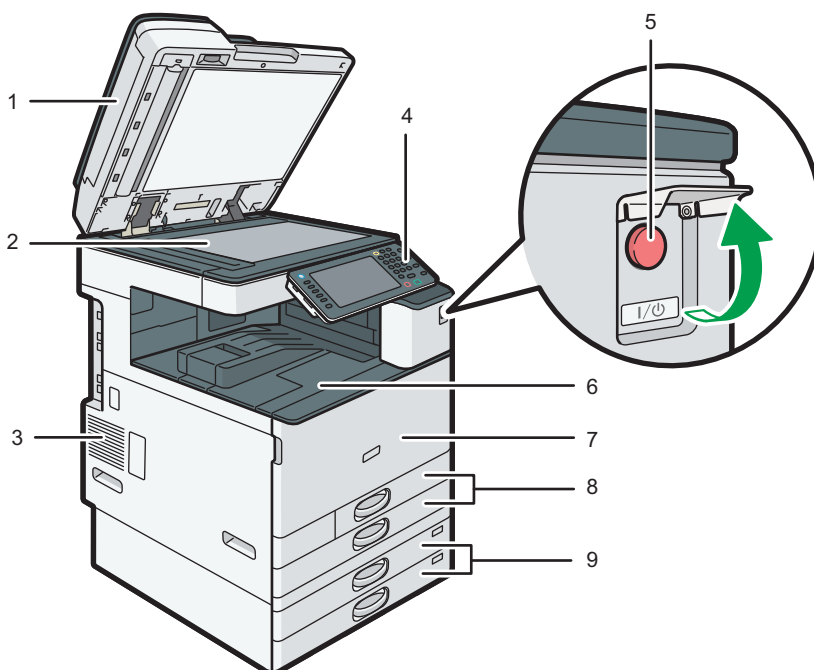
Guide to Names and Functions of Components

Guide to Components Region **A** (mainly Europe and Asia)

CAUTION

- Do not obstruct the machine's vents. Doing so risks fire caused by overheated internal components.

Front and left view



DAT001

1. Exposure glass cover or ADF

(The illustration shows ADF.)

Lower the exposure glass cover or the ADF over originals placed on the exposure glass.

If you load a stack of originals in the ADF, the ADF will automatically feed the originals one by one.

2. Exposure glass

Place originals face down here.

3. Vents

Prevent overheating.

4. Control panel

See page 41 "Guide to the Names and Functions of the Machine's Control Panel (When Using the Standard Operation Panel)" or page 44 "Guide to the Names and Functions of the Machine's Control Panel (When Using the Smart Operation Panel)".

5. Main power switch

To operate the machine, the main power switch must be on. If it is off, open the main power switch's cover and turn the switch on.

6. Internal tray 1

Copied/printed paper and fax messages are delivered here.

7. Front cover

Open to access the inside of the machine.

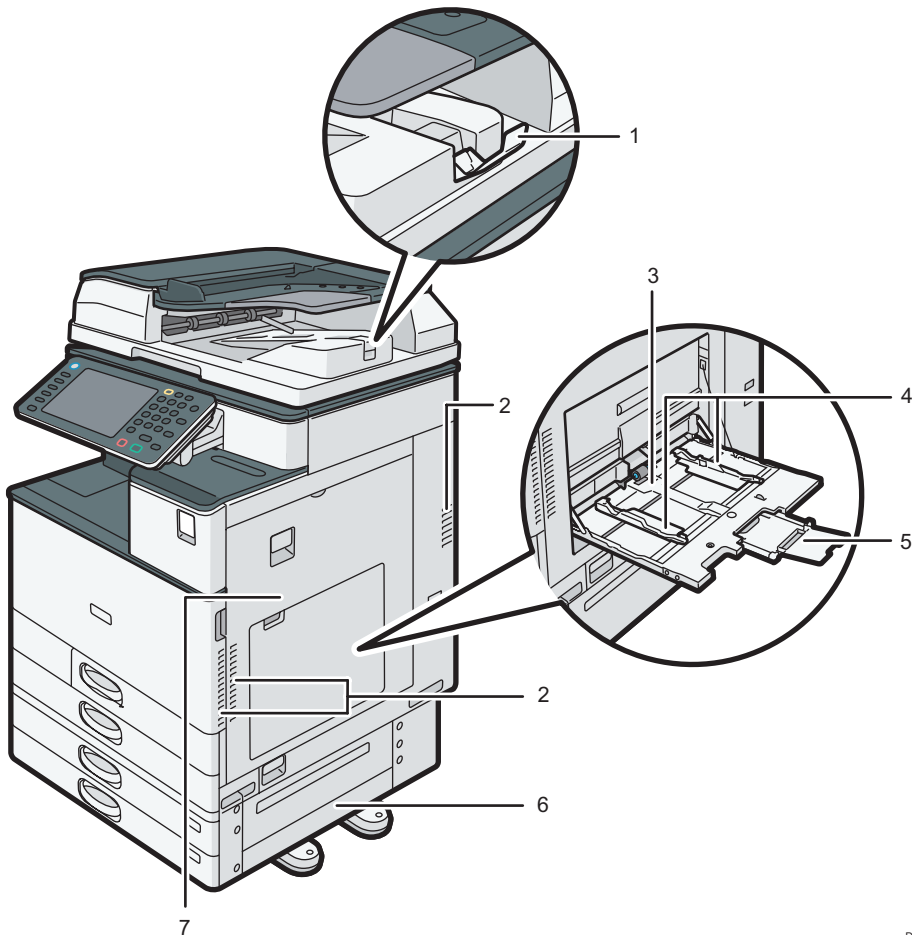
8. Paper trays (Trays 1–2)

Load paper here.

9. Lower paper trays

Load paper here.

Front and right view



DAT002

1. ADF's extender

Pull this extender to support large paper.

2. Vents

Prevent overheating.

3. Bypass tray

Use to copy or print on OHP transparencies, adhesive labels, and paper that cannot be loaded in the paper trays.

4. Paper guides

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

5. Extender

Pull this extender out when loading sheets larger than A4, $8\frac{1}{2} \times 11$ in the bypass tray.

6. Lower right cover

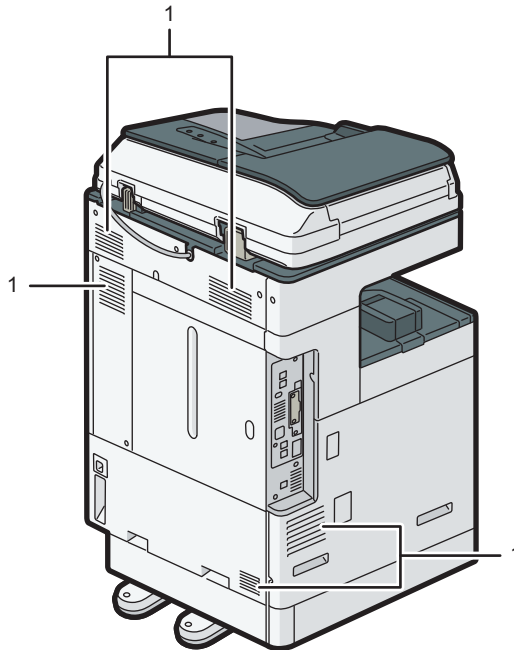
Open this cover when a paper jam occurs.

7. Right cover

Open this cover when a paper jam occurs.

Rear and left view

2



DAT003

1. Vents

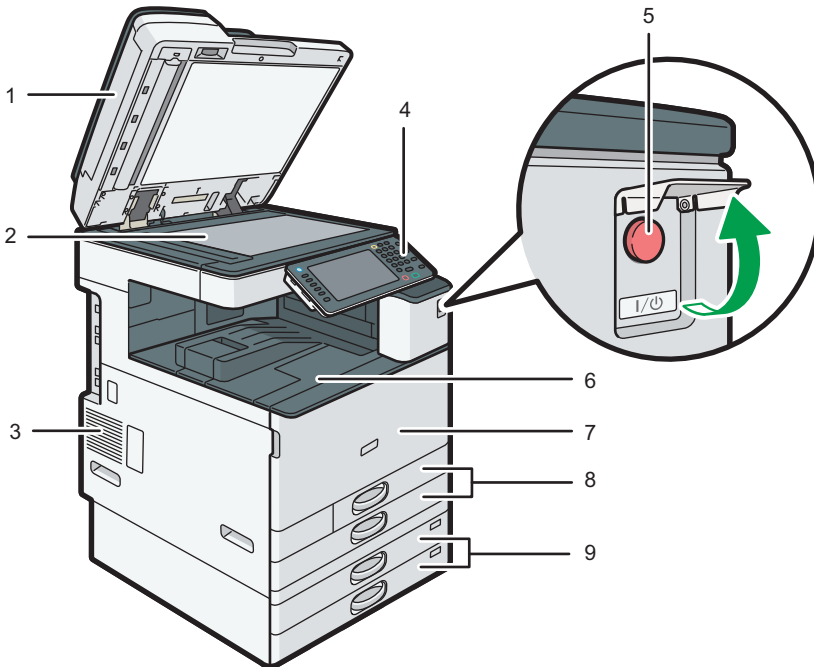
Prevent overheating.

Guide to Components  **Region B (mainly North America)**

 CAUTION

- Do not obstruct the machine's vents. Doing so risks fire caused by overheated internal components.

Front and left view



DAT001

1. ADF

Lower the ADF over originals placed on the exposure glass.

If you load a stack of originals in the ADF, the ADF will automatically feed the originals one by one.

2. Exposure glass

Place originals face down here.

3. Vents

Prevent overheating.

4. Control panel

See page 41 "Guide to the Names and Functions of the Machine's Control Panel (When Using the Standard Operation Panel)" or page 44 "Guide to the Names and Functions of the Machine's Control Panel (When Using the Smart Operation Panel)".

5. Main power switch

To operate the machine, the main power switch must be on. If it is off, open the main power switch's cover and turn the switch on.

6. Internal tray 1

Copied/printed paper and fax messages are delivered here.

7. Front cover

Open to access the inside of the machine.

8. Paper trays (Trays 1–2)

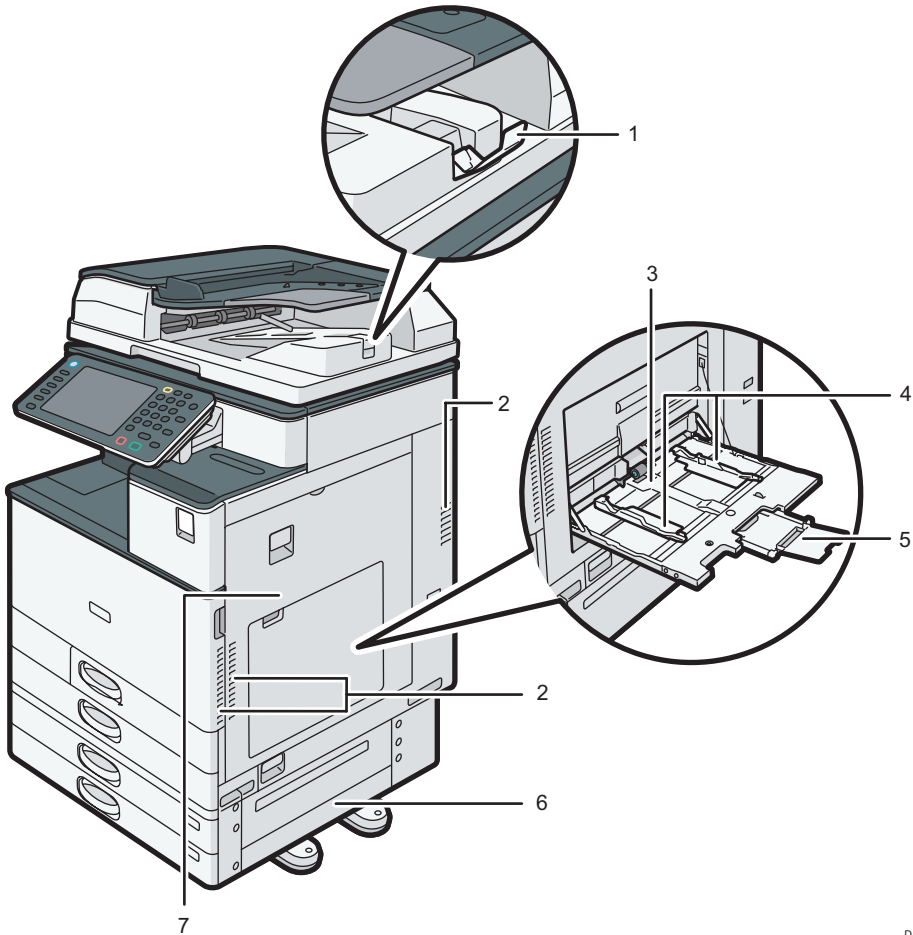
Load paper here.

9. Lower paper trays

Load paper here.

Front and right view

2



DAT002

1. ADF's extender

Pull this extender to support large paper.

2. Vents

Prevent overheating.

3. Bypass tray

Use to copy or print on OHP transparencies, adhesive labels, and paper that cannot be loaded in the paper trays.

4. Paper guides

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

5. Extender

Pull this extender out when loading sheets larger than A4, $8\frac{1}{2} \times 11$ in the bypass tray.

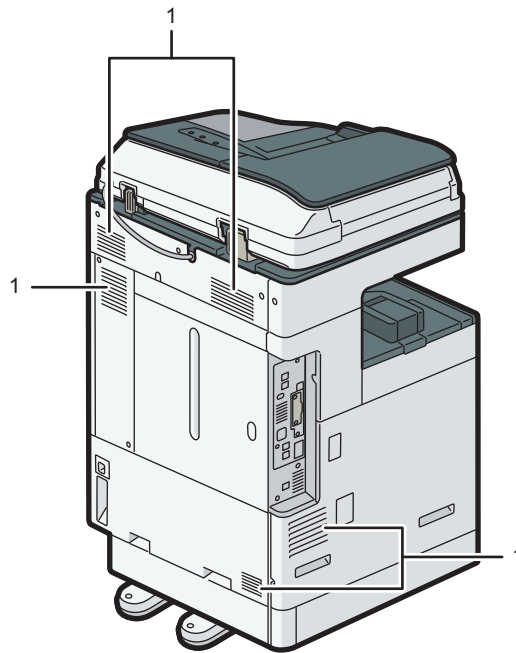
6. Lower right cover

Open this cover when a paper jam occurs.

7. Right cover

Open this cover when a paper jam occurs.

Rear and left view



DAT003

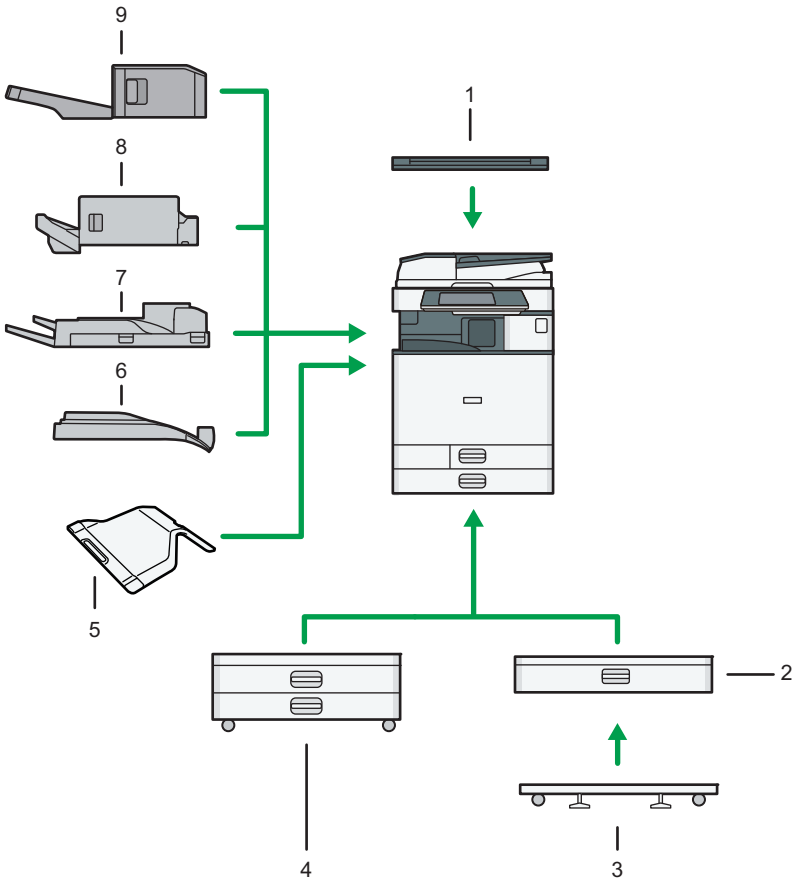
1. Vents

Prevent overheating.

Guide to Functions of the Machine's Options

Guide to Functions of the Machine's External Options Region A (mainly Europe)

2



DAT005

1. Exposure glass cover

Lower this cover over originals.

2. Lower paper tray

Holds up to 550 sheets of paper.

3. Caster table for lower paper tray

To use the lower paper tray, attach the caster table.

4. Lower paper trays

Consists of two paper trays. Holds up to 1,100 sheets of paper. Each paper tray holds 550 sheets.

5. Internal tray 2

If you select this as the output tray, copied/printed paper or fax messages are delivered here face down.

6. Internal shift tray

Sorts and stacks multiple sheets of paper.

7. External tray

If you select this as the output tray, copied/printed paper and fax messages are delivered here face down.

8. Internal Finisher SR3130

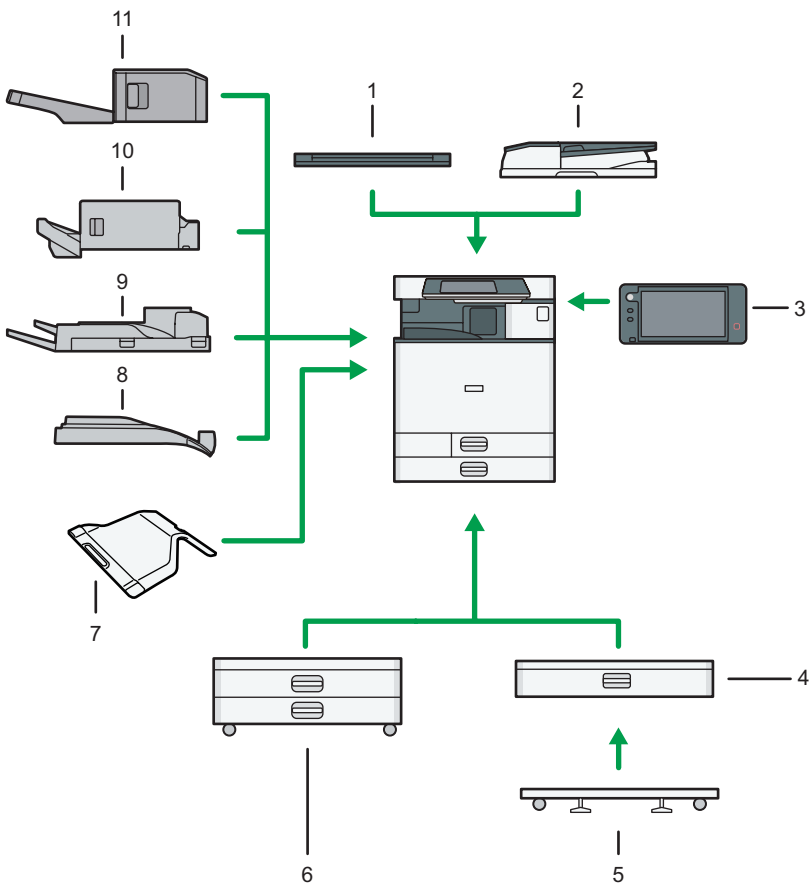
Sorts, stacks, and staples multiple sheets of paper.

Copies can be punched if the optional punch unit is installed on the finisher.

9. Internal Finisher SR3180

Sorts and stacks multiple sheets of paper, and staples them without using staples.

Guide to Functions of the Machine's External Options  **Region A (mainly Asia)**



DAT006

1. Exposure glass cover

Lower this cover over originals.

2. ADF

Load a stack of originals here. They will feed in automatically.

3. Smart Operation Panel

This control panel is provided with advanced operativity.

4. Lower paper tray

Holds up to 550 sheets of paper.

5. Caster table for lower paper tray

To use the lower paper tray, attach the caster table.

6. Lower paper trays

Consists of two paper trays. Holds up to 1,100 sheets of paper. Each paper tray holds 550 sheets.

7. Internal tray 2

If you select this as the output tray, copied/printed paper or fax messages are delivered here face down.

8. Internal shift tray

Sorts and stacks multiple sheets of paper.

9. External tray

If you select this as the output tray, copied/printed paper and fax messages are delivered here face down.

10. Internal Finisher SR3130

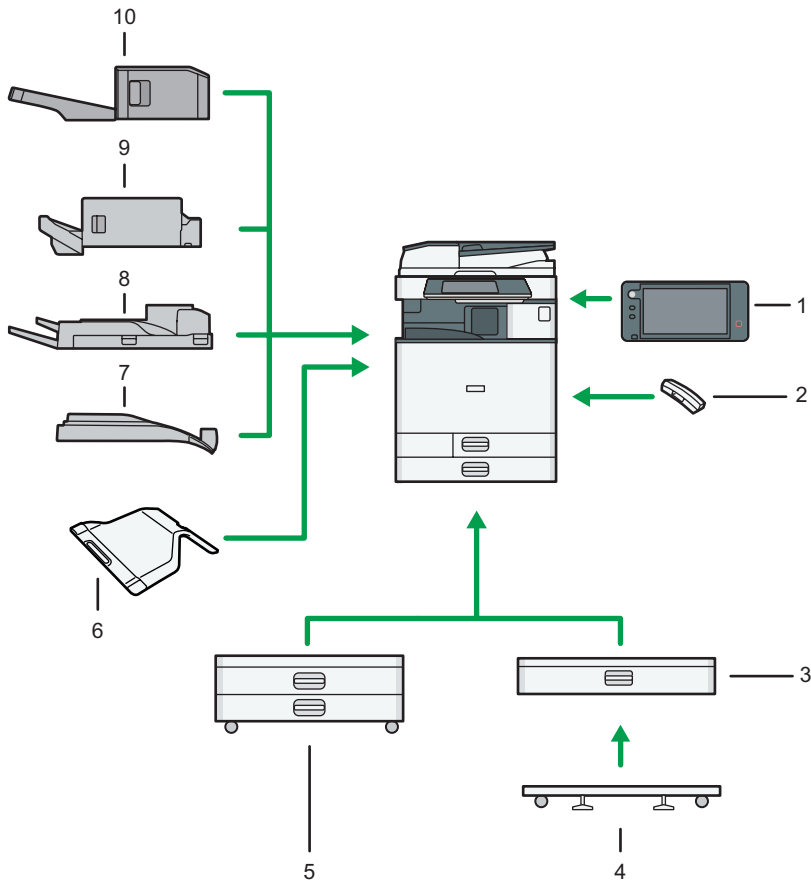
Sorts, stacks, and staples multiple sheets of paper.

Copies can be punched if the optional punch unit is installed on the finisher.

11. Internal Finisher SR3180

Sorts and stacks multiple sheets of paper, and staples them without using staples.

Guide to Functions of the Machine's External Options  **Region B (mainly North America)**



DAT007

1. Smart Operation Panel

This control panel is provided with advanced operativity.

2. Handset

Used as a receiver when a fax unit is installed.

Allows you to use the On Hook Dial and Manual Dial functions. It also allows you to use the machine as a telephone.

3. Lower paper tray

Holds up to 550 sheets of paper.

4. Caster table for lower paper tray

To use the lower paper tray, attach the caster table.

5. Lower paper trays

Consists of two paper trays. Holds up to 1,100 sheets of paper. Each paper tray holds 550 sheets.

6. Internal tray 2

If you select this as the output tray, copied/printed paper or fax messages are delivered here face down.

7. Internal shift tray

Sorts and stacks multiple sheets of paper.

8. External tray

If you select this as the output tray, copied/printed paper and fax messages are delivered here face down.

9. Internal Finisher SR3130

Sorts, stacks, and staples multiple sheets of paper.

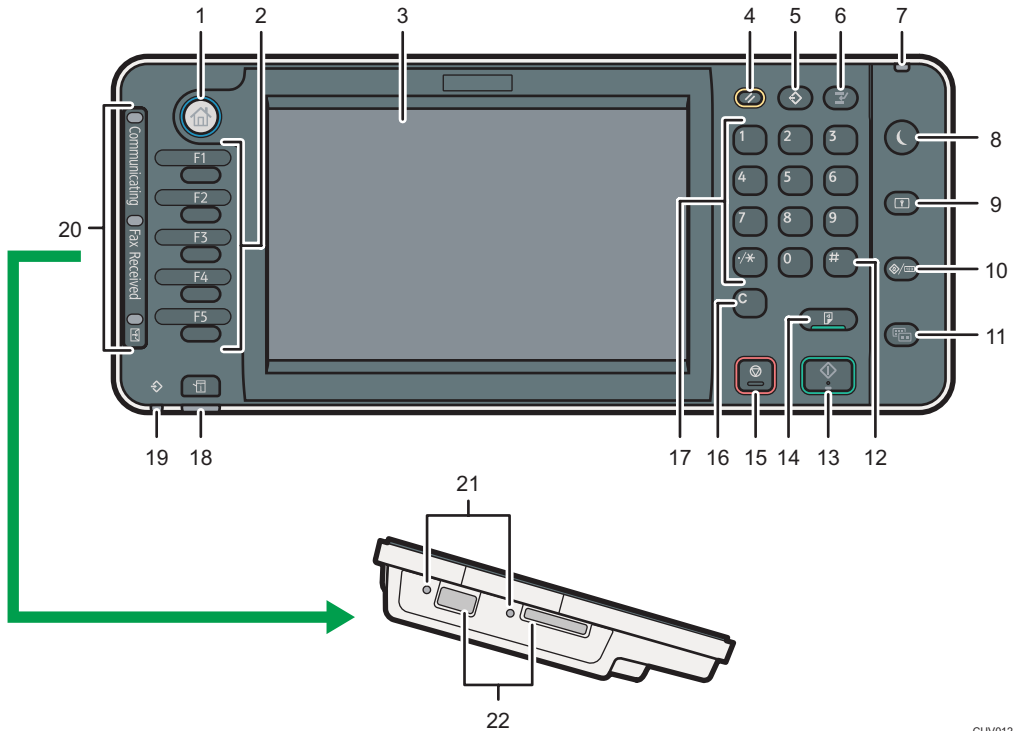
Copies can be punched if the optional punch unit is installed on the finisher.

10. Internal Finisher SR3180

Sorts and stacks multiple sheets of paper, and staples them without using staples.

Guide to the Names and Functions of the Machine's Control Panel (When Using the Standard Operation Panel)

This illustration shows the control panel of the machine with options fully installed.



CUV012

1. [Home] key

Press to display the [Home] screen. For details, see page 47 "How to Use the [Home] Screen (When Using the Standard Operation Panel)".

2. Function keys

No functions are registered to the function keys as a factory default. You can register often used functions, programs, and Web pages. For details, see "Configuring function keys (when using the standard operation panel)", Getting Started.

3. Display panel

Displays keys for each function, operation status, or messages. See "Changing Modes (When Using the Standard Operation Panel)" and "How to Use the Screens on the Control Panel", Getting Started.

4. [Reset] key

Press to clear the current settings.

5. [Program] key (copier, Document Server, facsimile, and scanner mode)

- Press to register frequently used settings, or to recall registered settings.
See "Registering Frequently Used Functions", Convenient Functions.
- Press to program defaults for the initial display when modes are cleared or reset, or immediately after the main power switch is turned on.
See "Changing the Default Functions of the Initial Screen", Convenient Functions.

6. [Interrupt] key

Press to make interrupt copies. See "Interrupt Copy", Copy/ Document Server.

7. Main power indicator

The main power indicator goes on when you turn on the main power switch.

8. [Energy Saver] key

Press to switch to and from Sleep mode. See "Saving Energy", Getting Started.
When the machine is in Sleep mode, the [Energy Saver] key flashes slowly.

9. [Login/Logout] key

Press to log in or log out.

10. [User Tools/Counter] key

- User Tools
Press to change the default settings to meet your requirements. See "Accessing User Tools", Connecting the Machine/ System Settings.
- Counter
Press to check or print the counter value. See "Counter", Maintenance and Specifications.

You can find out where to order expendable supplies and where to call when a malfunction occurs. You can also print these details. See "Checking Inquiry Using the User Tools", Maintenance and Specifications.

11. [Simple Screen] key

Press to switch to the simple screen. See "Switching Screen Patterns", Getting Started.

12. [#] key (Enter key)

Press to confirm values entered or items specified.

13. [Start] key

Press to start copying, printing, scanning, or sending.

14. [Sample Copy] key

Press to make a single set of copies or prints to check print quality before making multiple sets. See "Sample Copy", Copy/ Document Server.

15. [Stop] key

Press to stop a job in progress, such as copying, scanning, faxing, or printing.

16. [Clear] key

Press to delete a number entered.

17. Number keys

Use to enter the numbers for copies, fax numbers and data for the selected function.

18. [Check Status] key

Press to check the machine's system status, operational status of each function, and current jobs. You can also display the job history and the machine's maintenance information.

19. Data In indicator (facsimile and printer mode)

Flashes when the machine is receiving print jobs or LAN-Fax documents from a computer. See Fax and Print.

20. Communicating indicator, Fax Received indicator, Confidential File indicator

- **Communicating indicator**
Lights continuously during data transmission and reception.
- **Fax Received indicator**
Lights continuously while data other than personal box or Memory Lock file is being received and stored in the fax memory.
See "Substitute Reception", Fax.
- **Confidential File indicator**
Lights continuously while personal box data is being received.
Blinks while Memory Lock file is being received.
See "Personal Boxes" and "Printing a File Received with Memory Lock", Fax.

21. Media access lamp

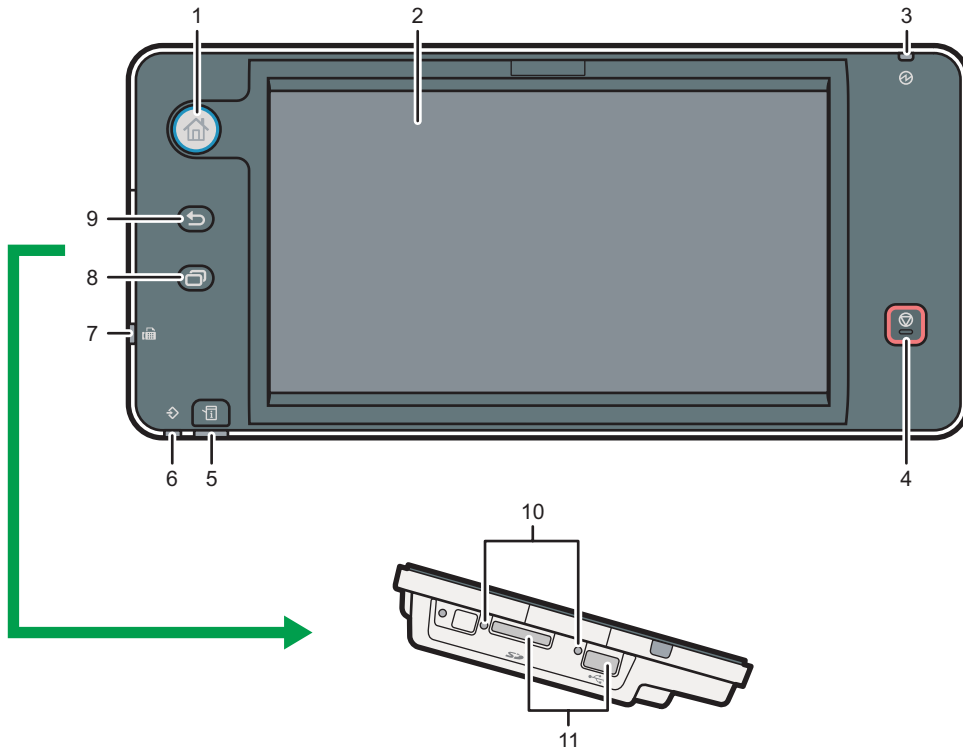
Lights up when a memory storage device is inserted in the media slot.

22. Media slots

Use to insert an SD card or a USB flash memory device.

Guide to the Names and Functions of the Machine's Control Panel (When Using the Smart Operation Panel)

2



CXV208

1. [Home] key

Press to display the [Home] screen. For details, see page 52 "How to Use the [Home] Screen (When Using the Smart Operation Panel)".

2. Display panel

This is a touch panel display that features icons, keys, shortcuts, and widgets that allow you to navigate the screens of the various functions and applications and provide you with information about operation status and other messages. See "How to Use the Standard Applications' Screen (When Using the Smart Operation Panel)", Getting Started.

3. Main power indicator

The main power indicator goes on when you turn on the main power switch. When the machine is in Fusing Unit Off mode, the main power indicator is lit. In Sleep mode, the main power indicator flashes slowly.

4. [Stop] key

Press to stop a job in progress, such as copying, scanning, faxing, or printing.

5. [Check Status] key

Press to check the machine's system status, operational status of each function, and current jobs. You can also display the job history and the machine's maintenance information.

6. Data In indicator (facsimile and printer mode)

Flashes when the machine is receiving print jobs or LAN-Fax documents from a computer. See Fax and Print.

7. Fax indicator

Indicates the status of the fax functions. Flashes during data transmission and reception. Stays lit when receiving a fax via Confidential or Substitute Reception.

8. [Menu] key

Displays the menu screen while Screen Features are enabled or applications available only on the Smart Operation Panel are used.

9. [Return] key

Press this key to return to the previous screen while Screen Features are enabled or applications available only on the Smart Operation Panel are used.

10. Media access lamp

Lights up when a memory storage device is inserted in the media slot.

11. Media slots

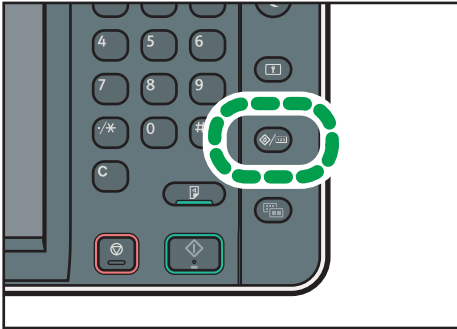
Use to insert an SD card or a USB flash memory device.

Changing the Display Language

You can change the language used on the display. English is set as default.

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.



CXX005

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press language key until the language you want to display appears.

3. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Changing the Display Language (When Using the Smart Operation Panel)

You can change the language used on the display. English is set as default.

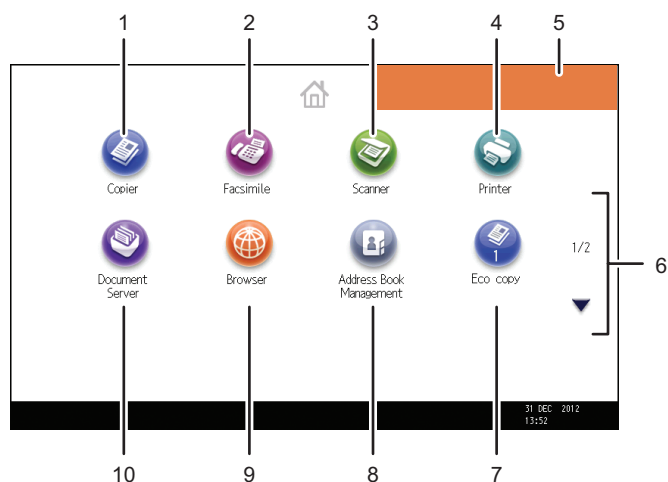
- Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the Change Languages Widget on the Home screen 4.
- Select the language you want to display.
- Press [OK].

How to Use the [Home] Screen (When Using the Standard Operation Panel)

The icons of each function are displayed on the [Home] screen.

You can add shortcuts to frequently used programs or Web pages to the [Home] screen. The icons of added shortcuts appear on the [Home] screen. The programs or Web pages can be recalled easily by pressing the shortcut icons.

To display the [Home] screen, press the [Home] key.



CUV215

1. [Copier]

Press to make copies.

For details about how to use the copy function, see Copy/ Document Server.

2. [Facsimile]

Press to send or receive faxes.

For details about how to use the fax function, see Fax.

3. [Scanner]

Press to scan originals and save images as files.

For details about how to use the scanner function, see Scan.

4. [Printer]

Press to make settings for using the machine as a printer.

For details about how to make settings for the printer function, see Print.

5. Home screen image

You can display an image on the [Home] screen, such as a corporate logo. To change the image, see "Displaying an Image on the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions.

6. ▲/▼

Press to switch pages when the icons are not displayed on one page.

7. **Shortcut icon**

You can add shortcuts to programs or Web pages to the [Home] screen. For details about how to register shortcuts, see "Adding Icons to the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions. The program number appears on the bottom of the shortcut icon.

8. **[Address Book Management]** 

Press to display the Address Book.

For details about how to use the Address Book, see "Address Book", Connecting the Machine/ System Settings.

9. **[Browser]** 

Press to display Web pages.

For details about how to use the browser function, see Convenient Functions.

10. **[Document Server]** 

Press to store or print documents on the machine's hard disk.

For details about how to use the Document Server function, see Copy/ Document Server.

Adding Icons to the [Home] Screen (When Using the Standard Operation Panel)

You can add shortcuts to programs stored in copier, facsimile, or scanner mode, or Web pages registered in Favorites using the browser function.

You can also review icons of functions and embedded software applications that you deleted from the [Home] screen.

 **Note**

- Shortcuts to programs stored in Document Server mode cannot be registered to the [Home] screen.
- Shortcut names of up to 32 characters can be displayed in a standard screen. If the name of the shortcut is longer than 32 characters, the 32nd character is replaced with "...". Only 30 characters can be displayed in a simple screen. If the name of the shortcut is longer than 30 characters, the 30th character is replaced with "...".
- For details about how to make a program, see page 57 "Registering Functions in a Program".
- For details about the procedure for registering Web pages to Favorites, see "Specifying the Settings for Favorites", Convenient Functions.
- Shortcuts to Web pages that are registered to Common Favorites can be registered to the [Home] screen. When user authentication is enabled, shortcuts to Web pages that are registered to Favorites by User can also be registered to a user's [Home] screen.
- For details about the procedure for registering a shortcut using the [Program] screen, see "Registering a Shortcut to a Program to the [Home] Screen", Convenient Functions.

- You can register up to 72 function and shortcut icons. Delete unused icons if the limit is reached. For details see "Deleting an Icon on the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions.
- You can change the position of icons. For details, see "Changing the Order of Icons on the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions.

Adding icons to the [Home] screen using Web Image Monitor (when using the standard operation panel)

2

1. Start Web Image Monitor.

For details, see "Using Web Image Monitor", Connecting the Machine/ System Settings.

2. Log in to Web Image Monitor as an administrator.

For details, see Security Guide.

3. Point to [Device Management], and then click [Device Home Management].

4. Click [Edit Icons].

5. Point to [+Icon can be added.] of the position that you want to add, and then click [+ Add].

6. Select the function or shortcut icon you want to add.

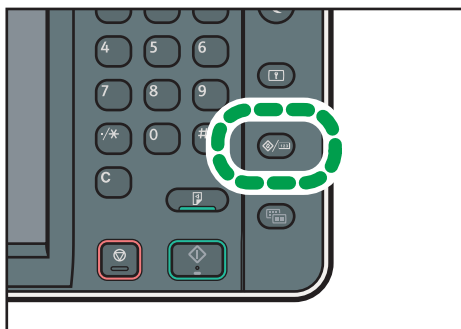
7. Click [OK] four times.

Adding icons to the [Home] screen using the User Tools (When using the standard operation panel)

In the following procedure, a shortcut to a copier program is registered to the [Home] screen.

1. Register a program.

2. Press the [User Tools/Counter] key.

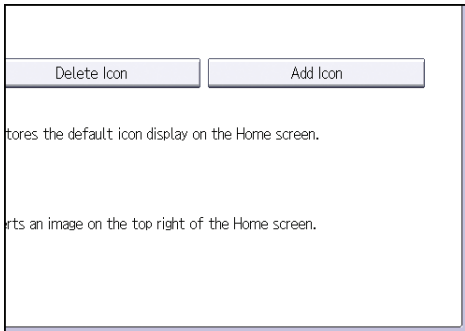


CXX005

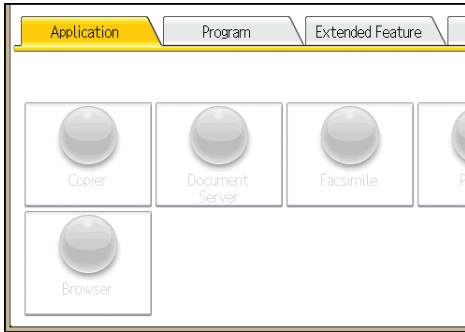
3. Press [Edit Home].



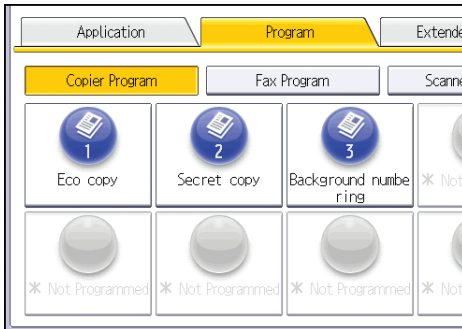
4. Press [Add Icon].



5. Press the [Program] tab.

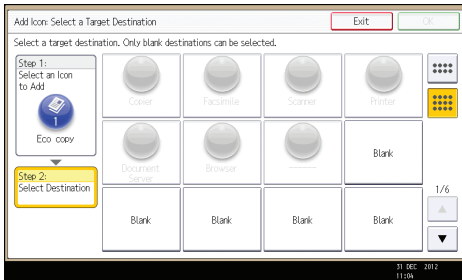


6. Make sure that [Copier Program] is selected.

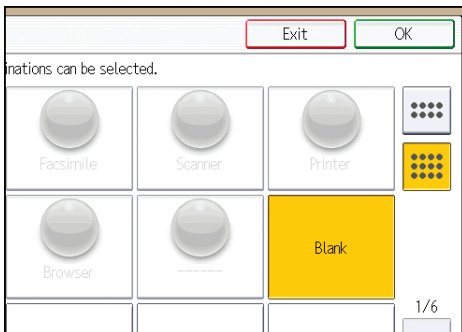


7. Select the program you want to add.

8. Specify the position where [Blank] is displayed.




9. Press [OK].



10. Press the [User Tools/Counter] key.

Note

- Press  on the upper-right corner of the screen to check the position on the simple screen.

How to Use the [Home] Screen (When Using the Smart Operation Panel)

To display the [Home] screen, press the [Home] key on the control panel.

One icon is assigned to each function, and these icons are displayed on the [Home] screen. You can add shortcuts to frequently used functions or Web pages to the [Home] screen. Also, you can register widgets such as the Change Languages Widget to it.

★ Important

- Do not apply strong impact or force to the screen, or it may be damaged. Maximum force allowable is approx. 30N (approx. 3 kgf). (N = Newton, kgf = Kilogram force. 1 kgf = 9.8N.)

The [Home] screen of the Smart Operation Panel consists of five screens, from Home screen 1 to Home screen 5. Home screen 3 is the default screen that appears first after you press the [Home] key.

To switch between screens, flick your finger to the right or left on the screen.



CZP157

1. The name of the user who is logged in

Displays the name of the user currently logging in to the machine. The name of the user is displayed only when user authentication is enabled.

2. [Login]/[Logout]

These keys are displayed when user authentication is enabled. When you press [Login], the authentication screen appears. If you have been already logged in to the machine, [Logout] appears. To log out of the machine, press [Logout].

For details about how to log in and out, see page 64 "When the Authentication Screen is Displayed".

3. Energy Saver

Press to switch to and from Sleep mode.

For details about the modes, see "Saving Energy", Getting Started.

4. Icon display area

Displays the function or application icons and widgets. Displayed icons differ between the five home screens. For details about icons on each screen, see "Main Icons on the [Home] Screen (When Using the Smart Operation Panel)", Getting Started.


You can also add shortcuts and arrange icons using folders. For details, see "Customizing the [Home] Screen", Convenient Functions.

5. Application list icon 

Press to display the application list. The list contains all the applications that are installed on the Smart Operation Panel. You can create shortcuts to the applications to the [Home] screen. For details, see "Customizing the [Home] Screen", Convenient Functions.

6. Icons to switch between screens 

Press to switch between the five home screens. The icons appear at the bottom right and left of the screen, the number of icons indicates the number of screens on each side of the current screen. For example, when you view Home screen 3, two icons are displayed at both the right and left sides.

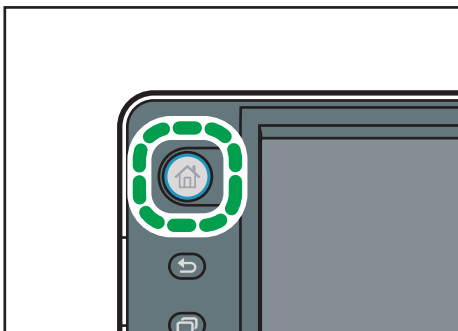
To view thumbnails of all five home screens, hold down .

Adding Icons to the [Home] Screen (When Using the Smart Operation Panel)

Adding shortcuts to the [Home] screen (When using the Smart Operation Panel)

You can add shortcuts to the machine's functions.

You can display the icons for the machine's functions and the embedded software applications after you delete them from the [Home] screen.

1. Press the [Home] key.

CZP155

- 2. Select the screen to which you want to add a shortcut.**
- 3. Press and hold down an area on the screen where no icons are displayed.**
- 4. Press [Icon] on the [Add to Home] screen.**

5. Press [Application] or [Machine Application].

Press [Machine Application] to select copier mode, fax mode, or some other of the machine's applications.

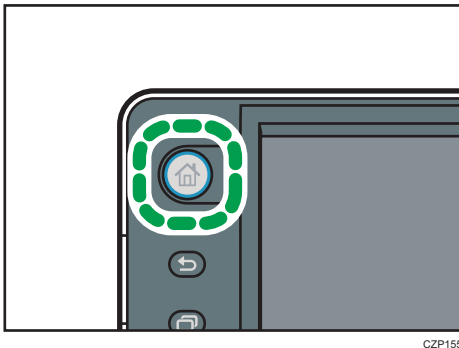
Press [Application] to select widgets, quick applications, or other Smart Operation Panel applications.

6. Select the application you want to add from the list.

Adding shortcuts to bookmarks on the [Home] screen (When using the Smart Operation Panel)

You can add shortcuts to bookmarks that have been registered in favorites in the Web Browser to the [Home] screen.

1. Press the [Home] key.



2. Select the screen to which you want to add a shortcut.

3. Press and hold down an area on the screen where no icons are displayed.

4. Press [Icon] on the [Add to Home] screen.

5. Press [Bookmark].

6. Select the bookmark you want to add from the list.

Adding shortcuts to programs to the [Home] screen (When using the Smart Operation Panel)

You can add shortcuts to programs registered on Copier, Facsimile, or Scanner mode.

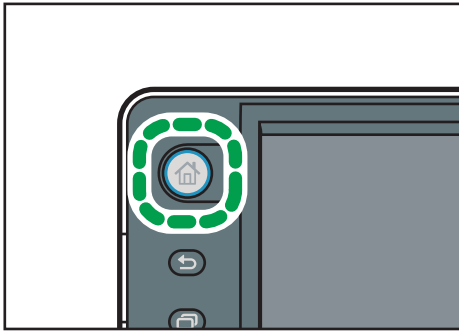
Even if you press [Program to Home] on the [Program] screen of each function, the shortcuts are not displayed on the [Home] screen.

1. Display the function screen to which you want to register a program.

2. Press [Recall/Program/Change Program] on the bottom left of the screen.

3. Register a program.

4. Press the [Home] key.



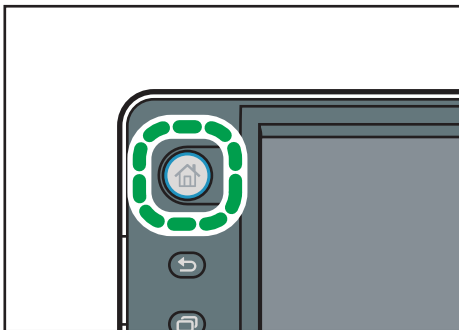
CZP155

5. Select the screen to which you want to add a shortcut.
6. Press and hold down an area on the screen where no icons are displayed.
7. Press [Icon] on the [Add to Home] screen.
8. Press [Machine Application].
9. Select the program you want to add from the list.


Adding shortcuts from the application list screen (When using the Smart Operation Panel)

You can add shortcuts of applications installed on the Smart Operation Panel.

1. Press the [Home] key.



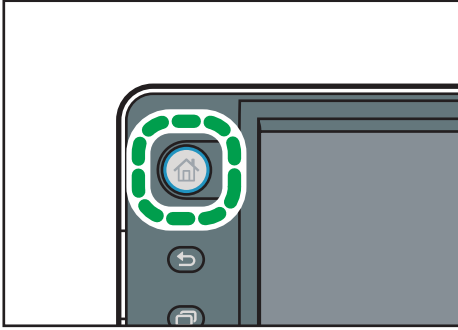
CZP155

2. Select the screen to which you want to add a shortcut.
3. Press .
4. Press and hold the icon you want to add to the [Home] screen.

Adding widgets to the [Home] screen (When using the Smart Operation Panel)

You can add widgets to the [Home] screen to show the remaining amount of toner or change the display language.

1. Press the [Home] key.



CZP155

2. Select the screen to which you want to add a widget.
3. Press and hold down an area on the screen where no icons are displayed.
4. Press [Widget] on the [Add to Home] screen.
5. Select the widget you want to add from the list.

Registering Functions in a Program

Depending on the functions, the number of programs that can be registered is different.

- Copier: 25 programs
- Document Server: 25 programs
- Facsimile: 100 programs
- Scanner: 25 programs

The following settings can be registered to programs:

Copier:

Color mode, original type, density, Special Original, paper tray, Store File (except for User Name, File Name, and Password), Auto Reduce / Enlarge, Create Margin, Finishing, Cover/Slip Sheet, Edit / Color, Dup./Combine/Series, Reduce / Enlarge, number of copies

Document Server (on the initial document print screen):

2 Sided Copy Top to Top, 2 Sided Copy Top to Bottom, Booklet, Magazine, Finishing, Cover/Slip Sheet (except for Main Sheet Tray in Designate / Chapter), Edit / Stamp, number of prints

Facsimile:

Scan Settings, density, Original Feed Type, File Type, Store File (except for User Name, File Name, and Password), Preview, transmission type, destinations (except for folder destinations), Select Line, Adv.Features, memory transmission/immediate transmission, Communi. Result Rep., TX Mode (except for Subject)

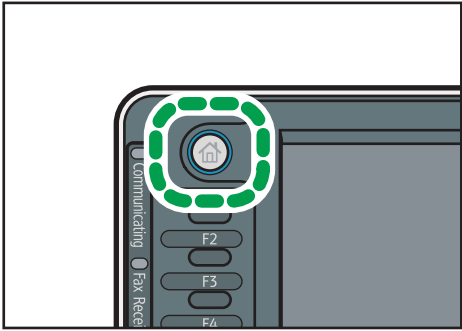
Scanner:

Scan Settings, density, Original Feed Type, Send File Type / Name (except for Security Settings and Start No.), Store File (except for User Name, File Name, and Password), Preview, Destinations selected from the Address Book, Text, Subject, Security, Receipt Notice

This section explains how to register functions in a program using copier function as an example.

1. Display the initial copy screen.

- When using the standard operation panel
Press the [Home] key on the top left of the control panel, and press the [Copier] icon on the [Home] screen.



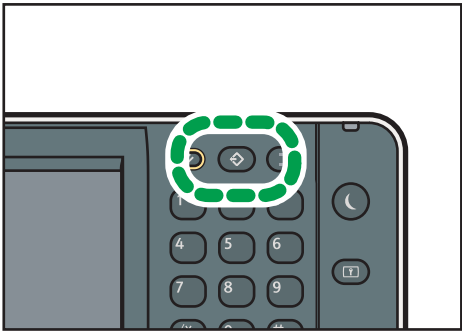
CXX002

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Copier] icon on the Home screen 4.

2. Edit the copy settings so all functions you want to store in a program are selected.

3. Display the program screen.

- When using the standard operation panel
Press the [Program] key.



CXV045

- When using the Smart Operation Panel
Press [Recall/Program/Change Program] on the bottom left of the screen.

4. Press [Program].

5. Press the program number you want to register.

Program (Copier)

Select No. to program.

001	* Not Programmed	002	* Not Programmed
003	* Not Programmed	004	* Not Programmed
005	* Not Programmed	006	* Not Programmed
007	* Not Programmed	008	* Not Programmed
009	* Not Programmed	010	* Not Programmed
011	* Not Programmed	012	* Not Programmed


6. Enter the program name.

7. Press [OK].

8. Press [Exit].

Note

- The number of characters you can enter for a program name varies depending on the functions as follows:
 - Copier: 34 characters
 - Document Server: 34 characters
 - Facsimile: 20 characters
 - Scanner: 34 characters
- When a specified program is registered as the default, its values become the default settings, which are displayed without pressing the [Program] key, when modes are cleared or reset, and after the machine is turned on. See "Changing the Default Functions of the Initial Screen", Convenient Functions.
- When the paper tray you specified in a program is empty and if there is more than one paper tray with the same size paper in it, the paper tray prioritized under [Paper Tray Priority: Copier] or [Paper Tray Priority: Facsimile] in the [Tray Paper Settings] tab will be selected first. For details, see "System Settings", Connecting the Machine/ System Settings.
- Destinations that are registered in the machine's Address Book can be registered to a program of the scanner mode.
- Destinations can be registered to a program of the scanner mode only when [Include Destinations] is selected for [Program Setting for Destinations] in [Scanner Features]. For details about the setting, see "General Settings", Scan.
- Folder destinations that have protection codes cannot be registered to a program of the scanner mode.
- Programs are not deleted by turning the power off or by pressing the [Reset] key unless the program is deleted or overwritten.

- Program numbers with  next to them already have settings made for them.
- Programs can be registered to the [Home] screen, and can be recalled easily. For details, see "Registering a Shortcut to a Program to the [Home] Screen", Convenient Functions and page 48 "Adding Icons to the [Home] Screen (When Using the Standard Operation Panel)". Shortcuts to programs stored in Document Server mode cannot be registered to the [Home] screen.

Example of Programs

Copier mode

Program name	Program description	Effect
Eco copy	Specify [Combine 2 Sides] in [Dup./Combine/Series].	You can save paper and toner.
Dated confidential copy	In [Edit / Color], specify [CONFIDENTIAL] under [Preset Stamp], and [Date Stamp].	You can increase security awareness by printing "CONFIDENTIAL" and the date on copies.
Conference material copy	Specify [Combine 2 Sides] in [Dup./Combine/Series] and [Staple] in [Finishing].	You can copy conference materials efficiently.
Unified-size copy	Specify [Mixed Sizes] in [Special Original] and [Auto Reduce / Enlarge] in the initial display.	You can print various size copies onto one size of paper, so they are easier to manage.
Stamping corporate name copy	Specify [User Stamp] in [Edit / Color].	You can stamp the name of your company on copies of working or architectural drawings. Your company name needs to be pre-registered in the machine.
Thumbnail copy	Specify [Combine 1 Side] in [Dup./Combine/Series].	You can copy up to eight pages onto one side of a sheet, so that you can save paper.
Storage copy: XXXX (replace XXXX by a folder name)	Specify a folder in [Target Folder to Store] in [Store File].	You can use folders to organize stored files by user name or intended use.

Scanner mode

Program name	Program description	Effect
Easy PDF scan	Select [Full Color: Text / Photo] in [Scan Settings]. In [Send File Type / Name], select [PDF] under [File Type] and enter the business details such as "London branch: daily report" under [File Name].	You can scan documents efficiently.
High compression PDF scan	Select [Full Color: Text / Photo] in [Scan Settings] and [High Compression PDF] in [Send File Type / Name].	You can compress the data size of scanned documents, so that you can send and store them.
Long-term storage scan	Select [PDF/A] in [Send File Type / Name].	You can easily digitize documents to "PDF/A" file format, which is suitable for long-term storage.
Unified-size scan	In [Scan Settings], select [Mixed Original Sizes] in [Scan Size] and specify the finished size of scanned data in [Reduce / Enlarge] under [Edit].	You can skip this procedure to unify the size when reprinting scanned data.
Digital signature scan	In [Send File Type / Name], specify [PDF] in [File Type], and also specify [Digital Signature].	You can add a digital signature to an important document such as a contract, so that any data tampering can be detected.
Dividing file scan	Specify [Divide] in [Original Feed Type].	You can scan a multiple page original as one file by splitting it into groups of a specified number of pages.
High resolution scan	Specify settings to save scanned data in TIFF format. Also, specify a higher resolution in [Scan Settings].	Scanned documents maintain much of the detail of the originals, but the size of the data may be quite large.
Batch document scan	Select [Batch] in [Original Feed Type].	You can apply multiple scans to a large volume of originals and send the scanned originals as a single job.

Program name	Program description	Effect
Scan to XXXX (replace XXXX by a destination name)	Select e-mail or folder destinations from the list that is registered in the machine's Address Book, and then specify the scan settings.	If you register destinations and scan settings that you use often, you can skip the procedures to specify them when sending a scanned file.
Storage scan: XXXX (replace XXXX by a folder name)	Specify a folder in [Target Folder to Store] in [Store File].	You can use folders to organize stored files by user name or intended use.

Facsimile mode

Program name	Program description	Effect
Transmission result notification fax	Select [Preview] in the initial display and specify [E-mail TX Results] in [TX Mode].	You can check whether the transmission settings are correct before and after transmission.
Specified time fax transmission	Specify [Send Later] in [TX Mode].	You can send a fax at a specified time.
Departmental fax transmission	Specify [Fax Header Print] in [TX Mode].	This setting can be used if the receiver specifies forwarding destinations by senders.

↓ Note

- Depending on the options installed, some functions cannot be registered. For details, see "Functions Requiring Optional Configurations", Getting Started.
- The names of programs given above are just examples. You can assign any name to a program according to your objectives.
- Depending on your business details or the type of documents to be scanned, registering a program cannot be recommended.

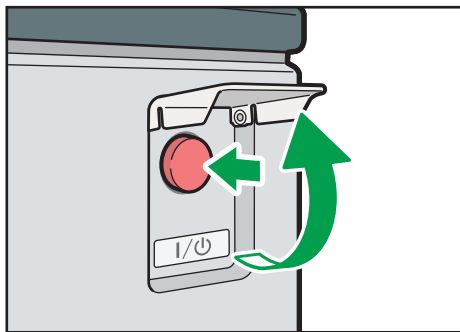
Turning On/Off the Power

The main power switch is on the right side of the machine. When this switch is turned on, the main power turns on and the main power indicator on the right side of the control panel lights up. When this switch is turned off, the main power turns off and the main power indicator on the right side of the control panel goes out. When this is done, machine power is off. When the fax unit is installed, fax files in memory may be lost if you turn this switch off. Use this switch only when necessary.

Turning On the Main Power

1. Make sure the power cord is firmly plugged into the wall outlet.
2. Open the main power switch cover, and push the main power switch.

The main power indicator goes on.



CUV031

Turning Off the Main Power

⚠ CAUTION

- When disconnecting the power cord from the wall outlet, always pull the plug, not the cord. Pulling the cord can damage the power cord. Use of damaged power cords could result in fire or electric shock.

★ Important

- Do not turn off the power while the machine is in operation.
- Do not hold down the main power switch while turning off the main power. Doing so forcibly turns off the machine's power and may damage the hard disk or memory and cause malfunctions.

1. Open the main power switch cover, and then push the main power switch.

The main power indicator goes out. The main power turns off automatically when the machine shuts down. If the screen on the control panel does not disappear, contact your service representative.

When the Authentication Screen is Displayed

If Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is active, the authentication screen appears on the display. The machine only becomes operable after entering your own Login User Name and Login Password. If User Code Authentication is active, you cannot use the machine until you enter the User Code.

If you can use the machine, you can say that you are logged in. When you go out of the operable state, you can say that you are logged out. After logging in the machine, be sure to log out of it to prevent unauthorized usage.

★ Important

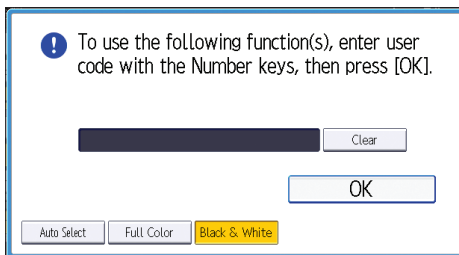
- Ask the user administrator for the Login User Name, Login Password, and User Code. For details about user authentication, see Security Guide.
- User Code to enter on User Code Authentication is the numerical value registered in the Address Book as "User Code".

User Code Authentication Using the Control Panel

This section explains the procedure for logging in to the machine using the control panel while User Code Authentication is active.

If User Code Authentication is active, a screen prompting you to enter a User Code appears.

1. Enter a User Code (up to eight digits), and then press [OK].



Logging In Using the Control Panel (When Using the Standard Operation Panel)

This section explains the procedure for logging in to the machine when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set.

1. Press [Login].



2. Enter a Login User Name, and then press [OK].

3. Enter a Login Password, and then press [OK].

When the user is authenticated, the screen for the function you are using appears.

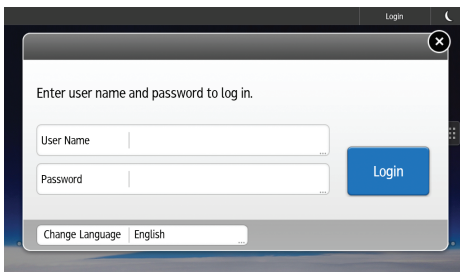
Logging In Using the Control Panel (When Using the Smart Operation Panel)

This section explains the procedure for logging in to the machine when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set.

1. Press [Login] on the top right on the screen.



2. Press [User Name].



3. Enter a Login User Name, and then press [Done].

4. Press [Password].

5. Enter a Login Password, and then press [Done].

6. Press [Login].

Logging Out Using the Control Panel (When Using the Standard Operation Panel)

This section explains the procedure for logging out the machine when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set.

★ Important

- To prevent use of the machine by unauthorized persons, always log out when you have finished using the machine.

1. Press the [Login/Logout] key.



CXV044

2. Press [Yes].

Logging Out Using the Control Panel (When Using the Smart Operation Panel)

This section explains the procedure for logging out the machine when Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication is set.

★ Important

- To prevent use of the machine by unauthorized persons, always log out when you have finished using the machine.

1. Press [Logout] on the top right on the screen.



2. Press [OK].

Placing Originals

Placing Originals on the Exposure Glass Region A (mainly Europe and Asia)

CAUTION

- Keep your hands away from the hinges and exposure glass when lowering the ADF. Not doing so may result in an injury if your hands or fingers are pinched.

Important

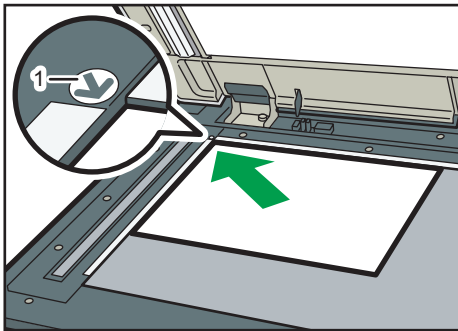
- Do not lift the ADF forcefully. Otherwise, the cover of the ADF might open or be damaged.

1. Lift the ADF or the exposure glass cover.

Be sure to lift the ADF or the exposure glass cover by more than 30 degrees. Otherwise, the size of the original might not be detected correctly.

2. Place the original face down on the exposure glass. The original should be aligned to the rear left corner.

Start with the first page to be scanned.



CVA054

1. Positioning mark

3. Lower the ADF or the exposure glass cover.

Placing Originals on the Exposure Glass Region B (mainly North America)

CAUTION

- Keep your hands away from the hinges and exposure glass when lowering the ADF. Not doing so may result in an injury if your hands or fingers are pinched.

★ Important

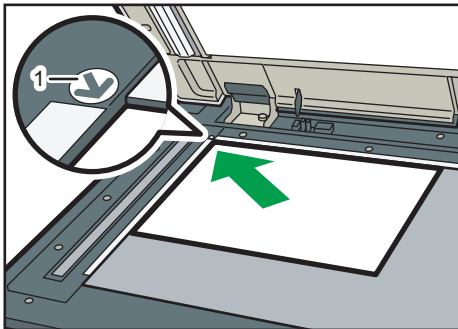
- Do not lift the ADF forcefully. Otherwise, the cover of the ADF might open or be damaged.

1. Lift the ADF.

Be sure to lift the ADF by more than 30 degrees. Otherwise, the size of the original might not be detected correctly.

2. Place the original face down on the exposure glass. The original should be aligned to the rear left corner.

Start with the first page to be scanned.



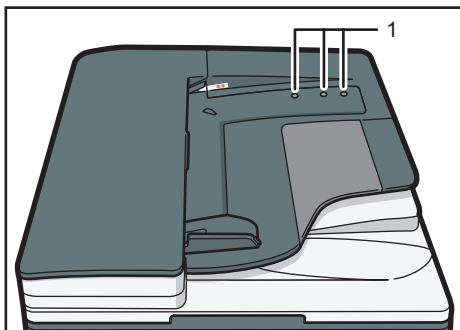
CVA054

1. Positioning mark

3. Lower the ADF.

Placing Originals in the Auto Document Feeder

Be sure not to block the sensor or load the original untidily. Doing so may cause the machine to detect the size of the original incorrectly or display a paper misfeed message. Also, be sure not to place originals or other objects on the top cover. Doing so may cause a malfunction.



CSN003

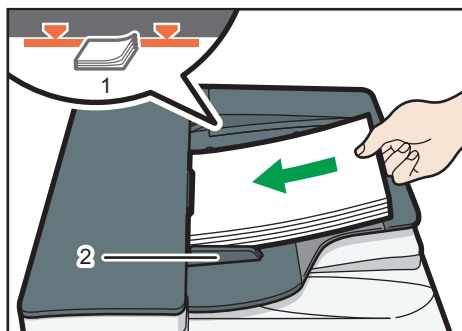
1. Sensors

1. Adjust the original guide to the original size.

2. Place the aligned originals squarely face up in the ADF.

Do not stack originals beyond the limit mark.

The first page should be on the top.



CSN004

1. Limit mark
2. Original guide

3. Copy


This chapter describes frequently used copier functions and operations. For the information not included in this chapter, see Copy/ Document Server on the supplied CD-ROM.

Basic Procedure


To make copies of originals, place them on the exposure glass or in the ADF.

When placing the original on the exposure glass, start with the first page to be copied. When placing the original in the ADF, place them so that the first page is on the top.

 **Region A** (mainly Europe and Asia)

For details about placing the original on the exposure glass, see page 67 "Placing Originals on the Exposure Glass  (mainly Europe and Asia)".

 **Region B** (mainly North America)

For details about placing the original on the exposure glass, see page 67 "Placing Originals on the Exposure Glass  (mainly North America)".

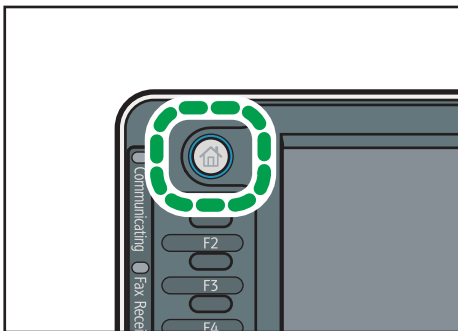
For details about placing the original in the ADF, see page 68 "Placing Originals in the Auto Document Feeder".

To copy onto paper other than plain paper, specify the paper type in User Tools according to the weight of the paper you are using. For details, see "Tray Paper Settings", Connecting the Machine/ System Settings.

1. Display the initial copy screen.

- When using the standard operation panel

Press the [Home] key on the top left of the control panel, and press the [Copier] icon on the [Home] screen.



CXX002

- When using the Smart Operation Panel

Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Copier] icon on the Home screen 4.

2. Make sure that no previous settings remain.

When there are previous settings remaining, press the [Reset] key.

3. Place the originals.

4. Make desired settings.

5. Enter the number of copies with the number keys.

The maximum copy quantity that can be entered is 999.

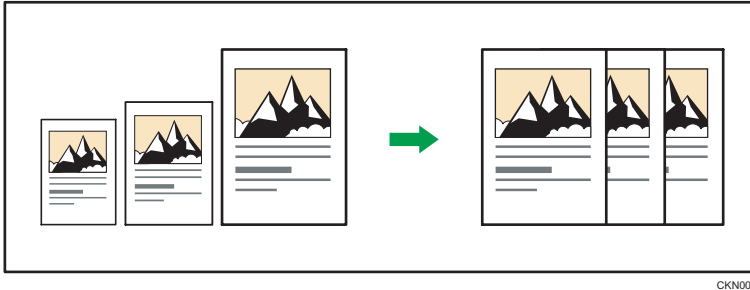
6. Press the [Start] key.

When placing the original on the exposure glass, press the [#] key after all originals are scanned. Some functions such as Batch mode may require that you press the [#] key when placing originals in the ADF. Follow the messages that appear on screen.

7. When the copy job is finished, press the [Reset] key to clear the settings.

Auto Reduce / Enlarge

The machine automatically detects the original size and then selects an appropriate reproduction ratio based on the paper size you select.



CKN008

★ Important

- If you select a reproduction ratio after pressing [Auto Reduce / Enlarge], [Auto Reduce / Enlarge] is canceled and the image cannot be rotated automatically.

This is useful to copy different size originals to the same size paper.

If the orientation in which your original is placed is different from that of the paper you are copying onto, the machine rotates the original image by 90 degrees and fits it on the copy paper (Rotate Copy). For example, to reduce A3 (11 × 17)☐ originals to fit onto A4 (8½ × 11)☐ paper, select a paper tray containing A4 (8½ × 11)☐ paper, and then press [Auto Reduce / Enlarge]. The image is automatically rotated. For details about Rotate Copy, see "Rotate Copy", Copy/ Document Server.

The original sizes and orientations you can use with this function are as follows:

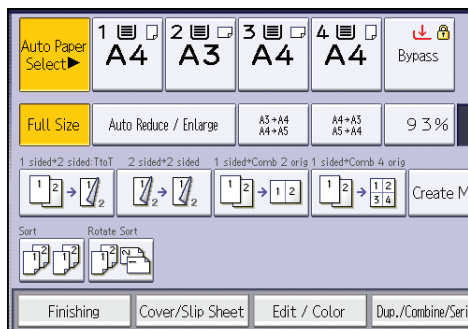
🌐 Region A (mainly Europe and Asia)

Original location	Original size and orientation
Exposure glass	A3☐, B4 JIS☐, A4☐☐, B5 JIS☐☐, A5☐, 8½ × 13☐
ADF	A3☐, B4 JIS☐, A4☐☐, B5 JIS☐☐, A5☐☐, B6 JIS☐☐, 11 × 17☐, 8½ × 11☐☐, 8½ × 13☐

🌐 Region B (mainly North America)

Original location	Original size and orientation
Exposure glass	11 × 17☐, 8½ × 14☐, 8½ × 11☐☐, 5½ × 8½☐
ADF	11 × 17☐, 8½ × 14☐, 8½ × 11☐☐, 5½ × 8½☐☐, 10 × 14☐, 7¼ × 10½☐, A3☐, A4☐☐

1. Press [Auto Reduce / Enlarge].



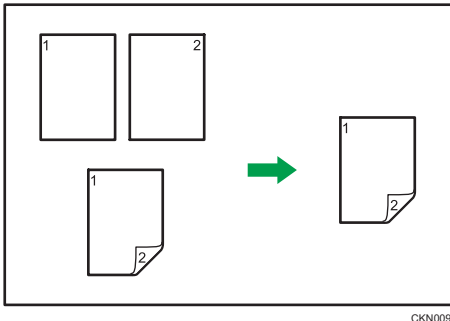
3

2. Select the paper size.

3. Place the originals, and then press the [Start] key.

Duplex Copying

Copies two 1-sided pages or one 2-sided page onto a 2-sided page. During copying, the image is shifted to allow for the binding margin.



CKN009

There are two types of Duplex.

1 Sided → 2 Sided

Copies two 1-sided pages on one 2-sided page.

2 Sided → 2 Sided

Copies one 2-sided page on one 2-sided page.

The resulting copy image will differ according to the orientation in which you place your originals (□ or □).

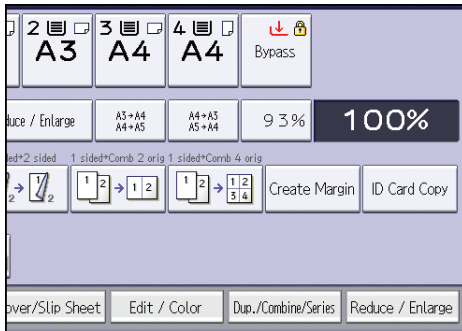
Original orientation and completed copies

To copy on both sides of the paper, select the original and copy orientation according to how you want the printout to appear.

Original	Placing originals	Original Orientation	Orientation	Copy
			Top to Top	
			Top to Bottom	

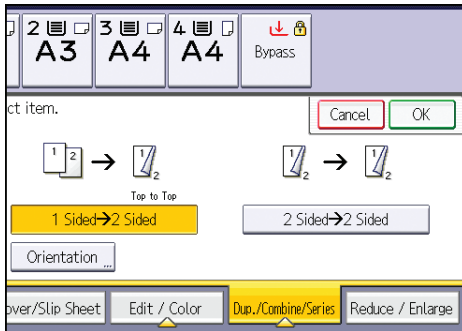
Original	Placing originals	Original Orientation	Orientation	Copy
			Top to Top	
			Top to Bottom	

1. Press [Dup./Combine/Series].



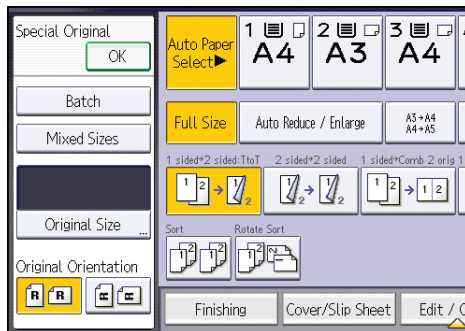
2. Make sure that [Duplex] is selected. If [Duplex] is not selected, press [Duplex].
3. Select [1 Sided → 2 Sided] or [2 Sided → 2 Sided] according to how you want the document to be output.

To change the original or copy orientation, press [Orientation].



4. Press [OK].
5. Place the originals.
6. Press [Special Original].

7. Select the original orientation, and then press [OK].

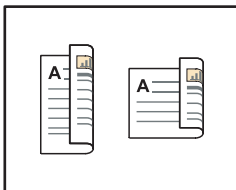


8. Press the [Start] key.

Specifying the Original and Copy Orientation

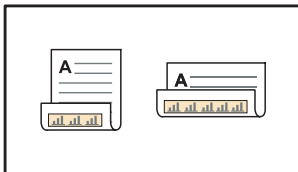
Select the orientation of the originals and copies if the original is two-sided or if you want to copy onto both sides of the paper.

- Top to Top



CKN011

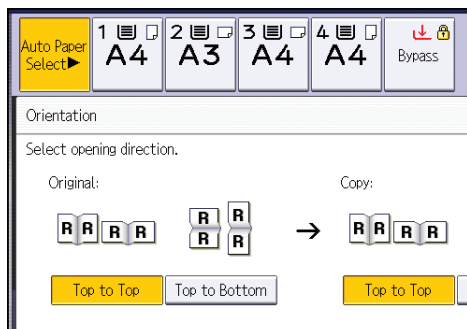
- Top to Bottom



CKN012

1. Press [Orientation].

2. Select [Top to Top] or [Top to Bottom] for [Original:] if the original is two-sided.



3. Select [Top to Top] or [Top to Bottom] for [Copy:].
4. Press [OK].

Combined Copying

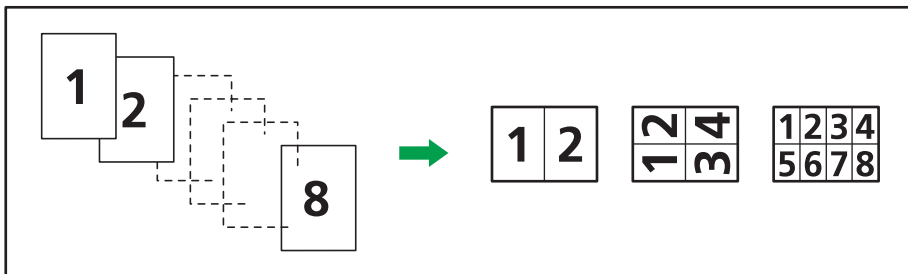
This mode can be used to select a reproduction ratio automatically and copy the originals onto a single sheet of copy paper.

The machine selects a reproduction ratio between 25 and 400%. If the orientation of the original is different from that of the copy paper, the machine will automatically rotate the image by 90 degrees to make copies properly.

Orientation of the original and image position of Combine

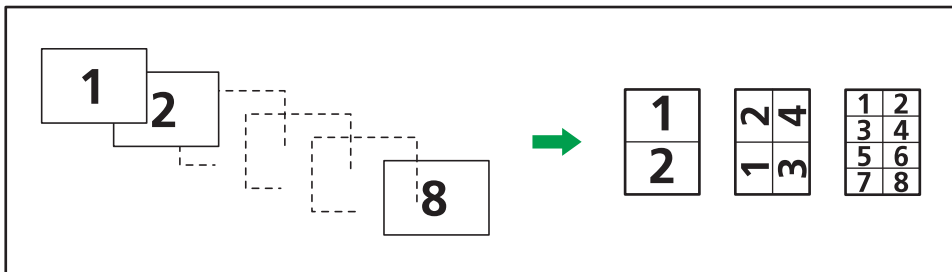
The image position of Combine differs according to original orientation and the number of originals to be combined.

- Portrait (📄) originals



CKN015

- Landscape (📄) originals

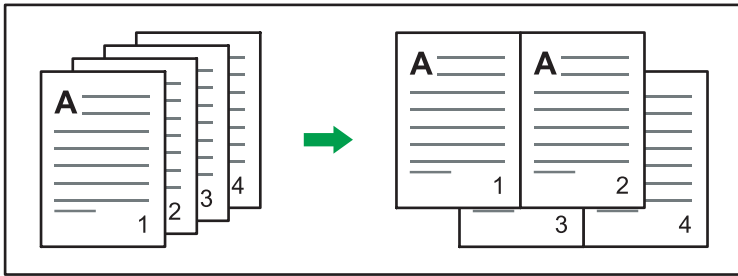


CKN016

Placing originals (originals placed in the ADF)

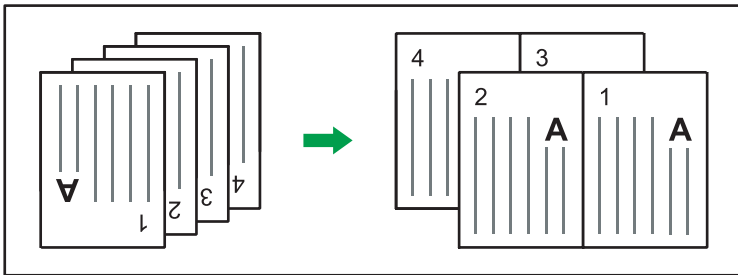
The default value for the copy order in the Combine function is [From Left to Right]. To copy originals from right to left in the ADF, place them upside down.

- Originals read from left to right



CKN010

- Originals read from right to left



CKN017

One-Sided Combine

Combine several pages onto one side of a sheet.



CKN014

There are six types of One-Sided Combine.

1 Sided 2 Originals → Combine 1 Side

Copies two 1-sided originals to one side of a sheet.

1 Sided 4 Originals → Combine 1 Side

Copies four 1-sided originals to one side of a sheet.

1 Sided 8 Originals → Combine 1 Side

Copies eight 1-sided originals to one side of a sheet.

2 Sided 2 Pages → Combine 1 Side

Copies one 2-sided original to one side of a sheet.

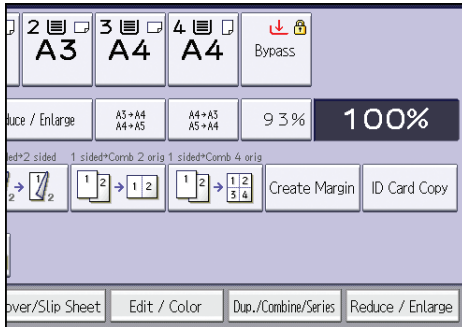
2 Sided 4 Pages → Combine 1 Side

Copies two 2-sided originals to one side of a sheet.

2 Sided 8 Pages → Combine 1 Side

Copies four 2-sided originals to one side of a sheet.

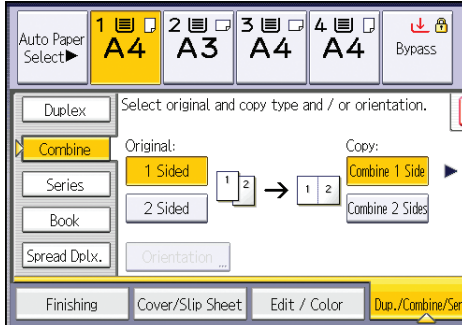
1. Press [Dup./Combine/Series].



2. Press [Combine].

3. Select [1 Sided] or [2 Sided] for [Original:].

If you selected [2 Sided], you can change the orientation.



4. Press [Combine 1 Side].

5. Select the number of originals to combine.

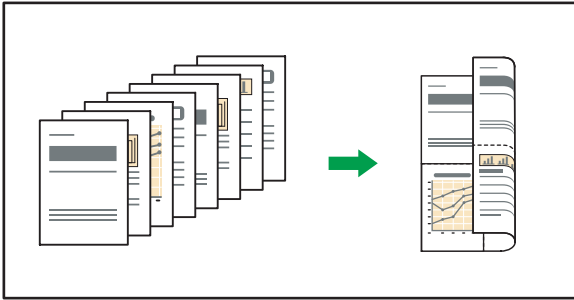
6. Press [OK].

7. Select the paper size.

8. Place the originals, and then press the [Start] key.

Two-Sided Combine

Combines various pages of originals onto two sides of one sheet.



CKN074

3

There are six types of Two-Sided Combine.

1 Sided 4 Originals → Combine 2 Sides

Copies four 1-sided originals to one sheet with two pages per side.

1 Sided 8 Originals → Combine 2 Sides

Copies eight 1-sided originals to one sheet with four pages per side.

1 Sided 16 Originals → Combine 2 Sides

Copies 16 1-sided originals to one sheet with eight pages per side.

2 Sided 4 Pages → Combine 2 Sides

Copies two 2-sided originals to one sheet with two pages per side.

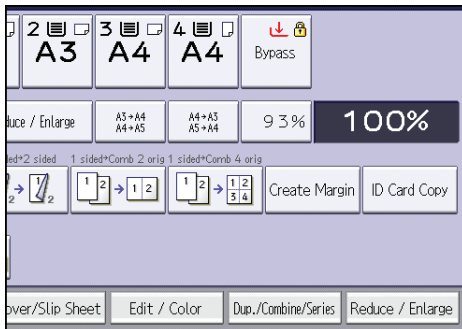
2 Sided 8 Pages → Combine 2 Sides

Copies four 2-sided originals to one sheet with four pages per side.

2 Sided 16 Pages → Combine 2 Sides

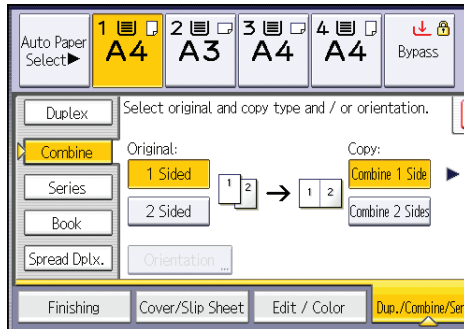
Copies eight 2-sided originals to one sheet with eight pages per side.

1. Press [Dup./Combine/Series].



2. Press [Combine].

3. Select [1 Sided] or [2 Sided] for [Original:].



4. Press [Combine 2 Sides].

5. Press [Orientation].

6. Select [Top to Top] or [Top to Bottom] for [Original:] and/or [Copy:], and then press [OK].

7. Select the number of originals to combine.

8. Press [OK].


9. Select the paper size.

10. Place the originals, and then press the [Start] key.

Copying onto Custom Size Paper from the Bypass Tray

Paper that has a horizontal length of 148.0–457.2 mm (5.83–18.00 inches) and a vertical length of 90.0–320.0 mm (3.55–12.59 inches) can be fed in from the bypass tray.

1. Load the paper face down in the bypass tray.

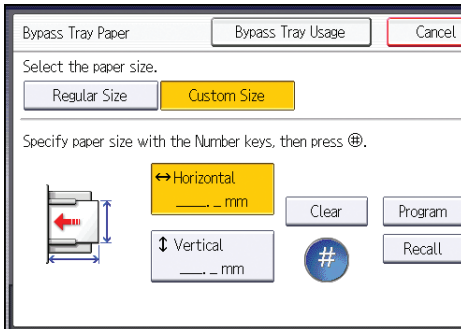
The bypass tray () is automatically selected.

2. Press the [#] key.

3. Press [Paper Size].

4. Press [Custom Size].

5. Enter the horizontal size with the number keys, and then press [#].



6. Enter the vertical size with the number keys, and then press [#].

7. Press [OK] twice.

8. Place the originals, and then press the [Start] key.

Copying onto Envelopes

This section describes how to copy onto regular size and custom size envelopes. Place the original on the exposure glass and place the envelope in the bypass tray or paper tray.

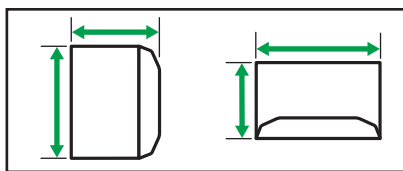
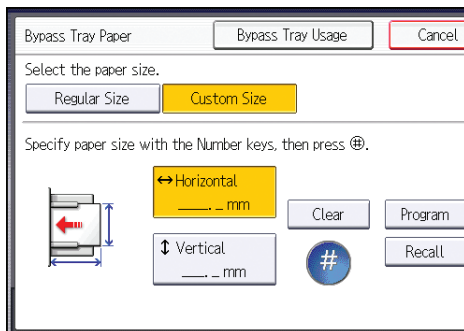
Specify the thickness of the paper according to the weight of the envelopes you are printing on. For details about the relationship between paper weight and paper thickness and the sizes of envelopes that can be used, see page 155 "Recommended Paper Sizes and Types".

About handling envelopes, supported envelope types, and how to load envelopes, see page 163 "Envelopes".

★ Important

- **The Duplex function cannot be used with envelopes. If the Duplex function is specified, press [1 sided → 2 sided:TtoT] to cancel the setting.**

To copy onto custom size envelopes, you must specify the envelope's dimensions. Specify the horizontal and vertical length of the envelope.



CJF005

↔: Horizontal

↑↓: Vertical

Be sure to include the fully open flap in the horizontal dimension.

Copying onto Envelopes from the Bypass Tray

Before using this function, select [Envelope] for the paper type under [Tray Paper Settings] in User Tools. For details, see "Tray Paper Settings", Connecting the Machine/ System Settings.

1. Load the envelopes face down in the bypass tray.

The bypass tray (≡) is automatically selected.

2. Press the [#] key.

3. Press [Paper Size].

4. Specify the envelope size, and then press [OK] twice.

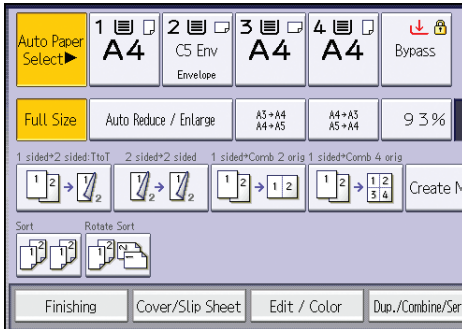
5. Place the originals, and then press the [Start] key.

3

Copying onto Envelopes from the Paper Tray

Before using this function, specify the paper size and type under [Tray Paper Settings] in User Tools. For the paper type, select [Envelope]. For details, see "Tray Paper Settings", Connecting the Machine/System Settings.

1. Select the paper tray where the envelopes are loaded.



2. Place the originals, and then press the [Start] key.

Sort

The machine assembles copies as sets in sequential order.

★ Important

- You cannot use the bypass tray with Rotate Sort.

Sort/Shift Sort

Copies are assembled as sets in sequential order.

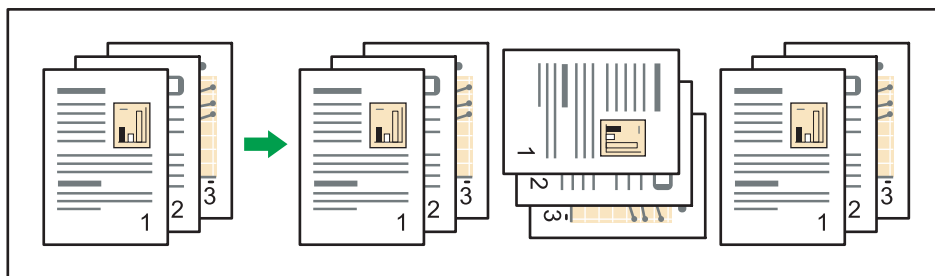
To use Shift Sort, a finisher or the internal shift tray is required. Each time the copies of one set or a job are delivered, the next copy is shifted to separate each set or job.



CKN018

Rotate Sort

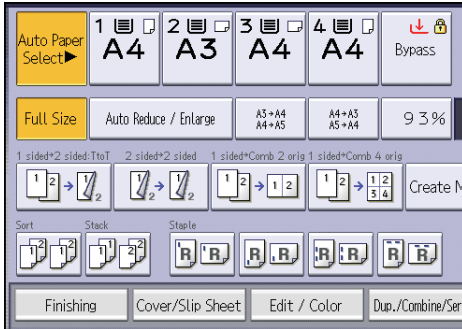
Every other copy set is rotated by 90 degrees (↻) and delivered to the copy tray.



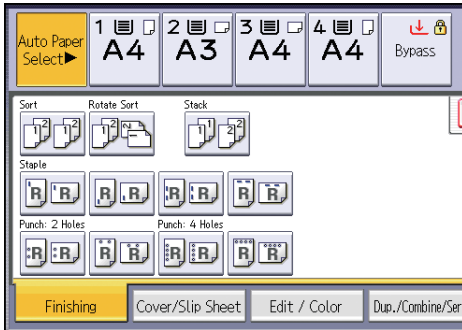
CKN019

To use the Rotate Sort function, two paper trays loaded with paper of the same size and type, but in different orientation (↻), are required. For details, see "Tray Paper Settings", Connecting the Machine/ System Settings.

1. Press [Finishing].



2. Select [Sort] or [Rotate Sort], and then press [OK].



3. Enter the number of copy sets using the number keys.

4. Place the originals.

To confirm the type of finishing, press the [Sample Copy] key.

5. Press the [Start] key.

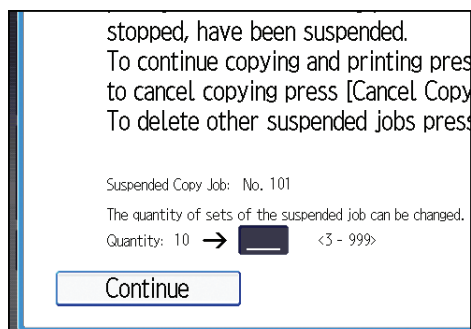
Changing the Number of Sets

You can change the number of copy sets during copying.

★ Important

- This function can be used only when the Sort function is selected.

1. While "Copying..." is displayed, press the [Stop] key.

2. Enter the number of copy sets with the number keys.**3. Press [Continue].**

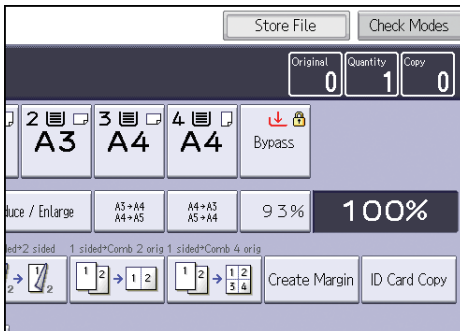
Copying starts again.

Storing Data in the Document Server

The Document Server enables you to store documents being read with the copy feature on the hard disk of this machine. Thus you can print them later applying necessary conditions.

You can check the stored documents on the Document Server screen. For details about the Document Server, see page 137 "Storing Data".

1. Press [Store File].



2. Enter a user name, file name, or password if necessary.
3. Specify a folder in which to store the document if necessary.
4. Press [OK].
5. Place the originals.
6. Make the scanning settings for the original.
7. Press the [Start] key.

Stores scanned originals in memory and makes one set of copies. If you want to store another document, do so after copying is complete.

4. Fax

This chapter describes frequently used facsimile functions and operations. For the information not included in this chapter, see Fax on the supplied CD-ROM.

Basic Procedure for Transmissions (Memory Transmission)

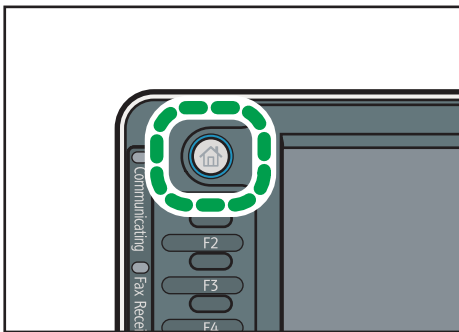
This section describes the basic procedure for transmitting documents using Memory Transmission. You can specify the fax, IP-Fax, Internet Fax, e-mail, or folder destinations. Multiple types of destination can be specified simultaneously.

★ Important

- It is recommended that you call the receivers and confirm with them when sending important documents.
- If there is a power failure (the main power switch is turned off) or the machine is unplugged for about one hour, all the documents stored in memory are deleted. As soon as the main power switch is turned on, the Power Failure Report is printed to help you check the list of deleted files. See "When an Error Is Notified via a Report or E-mail", Troubleshooting.

1. Display the initial facsimile screen.

- When using the standard operation panel
Press the [Home] key on the top left of the control panel, and press the [Facsimile] icon on the [Home] screen.

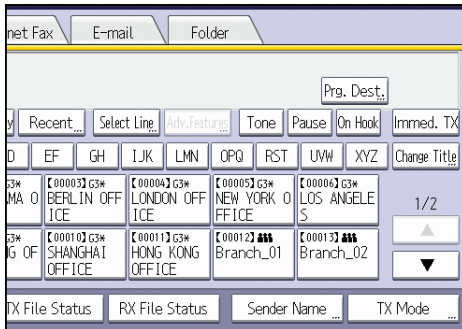


CXX002

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Fax] icon on the Home screen 4.

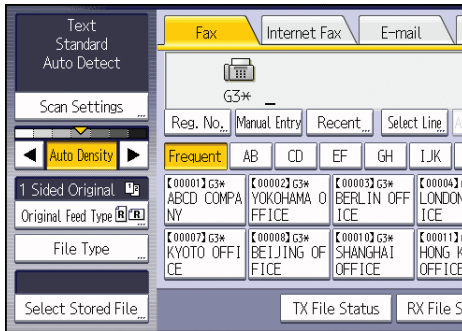
2. Make sure "Ready" appears on the screen.

3. Make sure [Immed. TX] is not highlighted.



4. Place the original into the ADF.

5. Make the scan settings such as scan size and resolution.

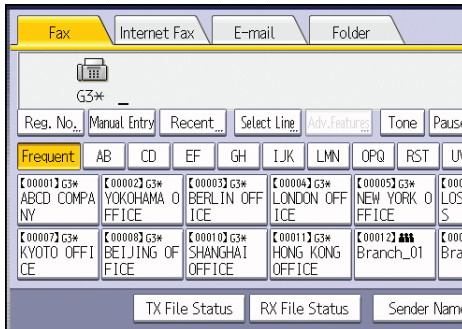


6. Configure the transmission settings such as [TX Mode] as necessary.

7. Specify a destination.

You can enter the destination's number or address directly or select from the Address Book by pressing the destination key.

If you make a mistake, press the [Clear] key, and then enter again.

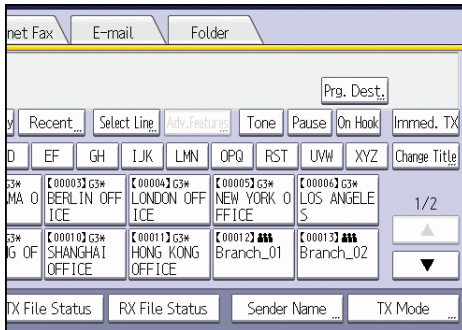


8. When sending the same original to several destinations (broadcasting), specify the next destination.

9. If you send documents to Internet Fax or e-mail destinations or enable the E-mail TX Results function, specify a sender.
10. Press the [Start] key.

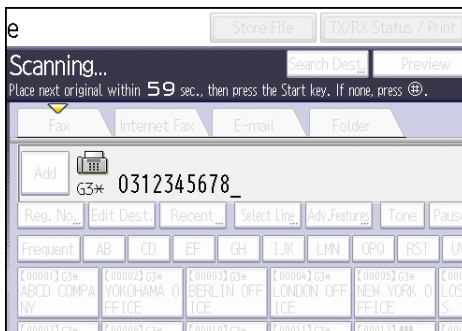
Sending Originals Using the Exposure Glass (Memory Transmission)

1. Make sure [Immed. TX] is not highlighted.



2. Place the first page of the original face down on the exposure glass.
3. Specify a destination.
4. Make the scan settings you require.
5. Press the [Start] key.
6. Place the next original on the exposure glass within 60 seconds when you send multiple originals, and then repeat Steps 4 and 5.

Repeat this step for each page.



7. Press the [#] key.

The machine dials the destination and starts transmission.

Registering a Fax Destination

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press [Address Book Mangmnt].

3. Check that [Program / Change] is selected.

4. Press [New Program].

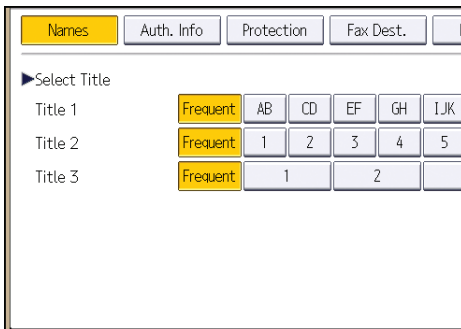
5. Press [Change] under "Name".

The name entry display appears.

6. Enter the name, and then press [OK].

7. Press [▼Next].

8. Press the key for the classification you want to use under "Select Title".



The keys you can select are as follows:

- [Frequent]: Added to the page that is displayed first.
- [AB], [CD], [EF], [GH], [IJK], [LMN], [OPQ], [RST], [UVW], [XYZ], [1] to [10]: Added to the list of items in the selected title.

You can select [Frequent] and one more key for each title.

9. Press [Fax Dest.].

10. Press [Change] under "Fax Destination".

11. Enter the fax number using the number keys, and then press [OK].



12. Specify optional settings such as "SUB Code", "SEP Code", and "International TX Mode".

13. Press [OK].

14. Press [Exit].

15. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Deleting a Fax Destination

★ Important

- If you delete a destination that is a specified delivery destination, messages to its registered Personal Box, for example, cannot be delivered. Be sure to check the settings in the fax function before deleting any destinations.

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press [Address Book Mangmnt].

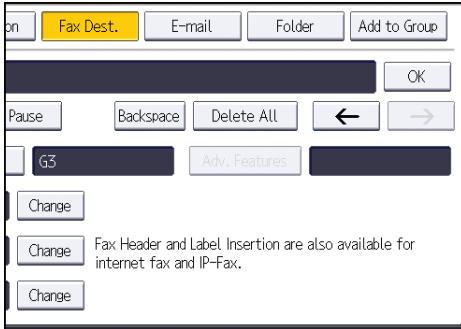
3. Check that [Program / Change] is selected.

4. Select the name whose fax destination you want to delete.

Press the name key, or enter the registered number using the number keys.

You can search by the registered name, user code, fax number, folder name, e-mail address, or IP-Fax destination.

5. Press [Fax Dest.].
6. Press [Change] under "Fax Destination".
7. Press [Delete All], and then press [OK] under "Fax Destination".



8. Press [OK].
9. Press [Exit].
10. Close the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.
 - When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Transmitting while Checking Connection to Destination (Immediate Transmission)

Using Immediate Transmission, you can send documents while checking the connection to the destination.

You can specify fax or IP-Fax destinations.

If you specify Internet Fax, e-mail, folder destinations, and group or multiple destinations, the transmission mode is automatically switched to Memory Transmission.

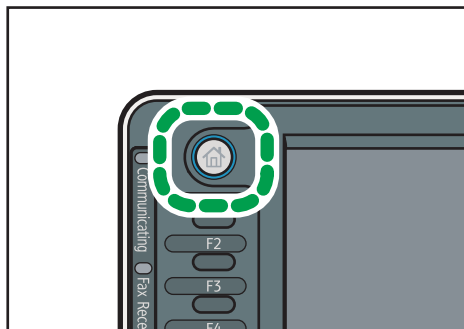
★ Important

- It is recommended that you call the receivers and confirm with them when sending important documents.

1. Display the initial facsimile screen.

- When using the standard operation panel

Press the [Home] key on the top left of the control panel, and press the [Facsimile] icon on the [Home] screen.

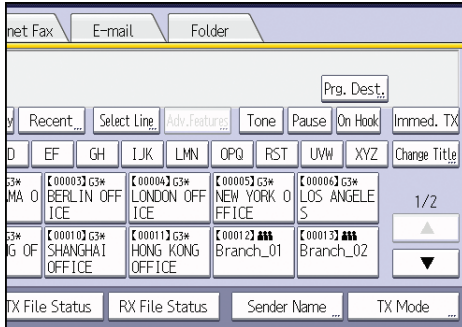


- When using the Smart Operation Panel

Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Fax] icon on the Home screen 4.

2. Make sure "Ready" appears on the screen.

3. Press [Immed. TX].



4. Place the original into the ADF.

5. Select the scan settings you require.

6. Specify a destination.

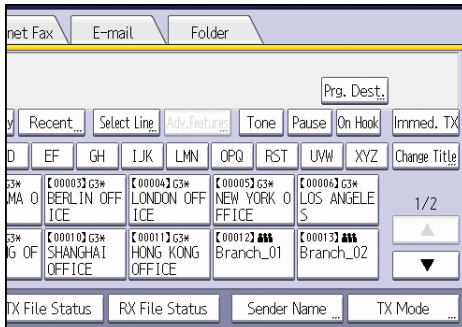
If you make a mistake, press the [Clear] key, and then enter again.

7. Press the [Start] key.

4

Sending Originals Using the Exposure Glass (Immediate Transmission)

1. Press [Immed. TX].



2. Place the first page face down on the exposure glass.

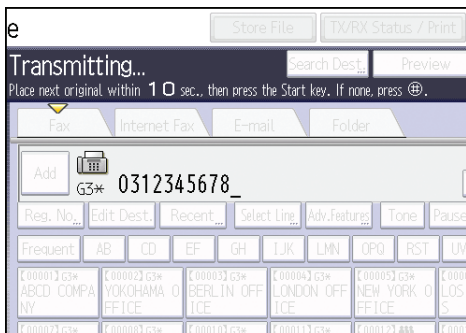
3. Specify a destination.

4. Make the scan settings you require.

5. Press the [Start] key.

6. Place the next original on the exposure glass within 10 seconds when you send multiple originals, and then repeat Steps 4 and 5.

Repeat this step for each page.



7. Press the [#] key.

Canceling a Transmission

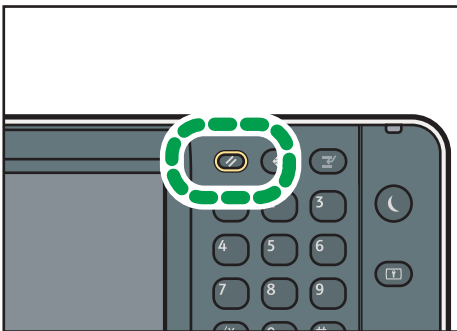
This section explains how to cancel a fax transmission.

Canceling a Transmission Before the Original Is Scanned

Use this procedure to cancel a transmission before pressing the [Start] key.

1. Cancel sending.

- When using the standard operation panel
Press the [Reset] key.



CX2001

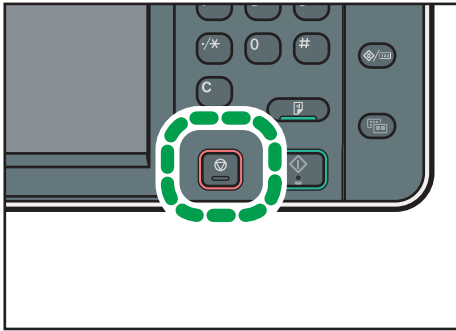
- When using the Smart Operation Panel
Press [Reset] on the top right of the screen.

Canceling a Transmission While the Original Is Being Scanned

Use this procedure to cancel scanning or transmitting of the original while it is being scanned.

If you cancel a transmission using the standard memory transmission function, you need to follow a different procedure to cancel the transmission. See page 101 "Canceling a Transmission After the Original Is Scanned".

1. Press the [Stop] key.



CXX006

2. Press [Cancel Scanning] or [Cancel TX].

Depending on the transmission mode and function you use, either [Cancel Scanning] or [Cancel TX] is displayed.

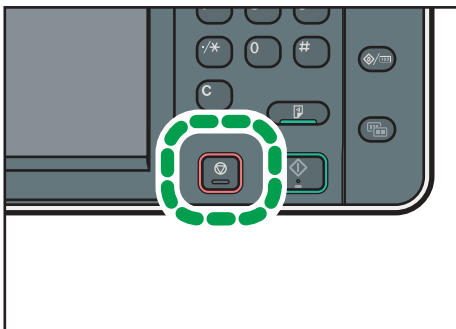
4

Canceling a Transmission After the Original Is Scanned

Use this procedure to cancel a transmission after the original is scanned.

You can cancel transmission of a file while the file is being sent, stored in memory, or if it fails to transmit. All the scanned data is deleted from memory.

1. Press the [Stop] key.



CXX006

You can also press [TX/RX Status / Print], and then [Check / Stop Transmission File].

2. If a confirmation message appears, press [Standby File List].
3. Select the file you want to cancel.

If the desired file is not shown, press [▲] or [▼] to find it. To cancel transmission of a file stored in the memory, press the [File List] tab.

4. Press [Stop Transmission].

5. Press [OK].

To cancel another file, repeat Steps 3 through 5.

6. Press [Exit].

After pressing [Check / Stop Transmission File] under [TX/RX Status / Print] in Step 1, press [Exit] twice.

Storing a Document

You can store and send a document at the same time. You can also just store a document.

The following information can be set for the stored documents as necessary:

User Name

You can set this function if necessary to know who and what departments stored documents in the machine. A user name can be selected from the Address Book or entered manually.

File Name

You can specify a name for a stored document. If you do not specify a name, scanned documents will be automatically assigned names such as "FAX0001" or "FAX0002".

Password

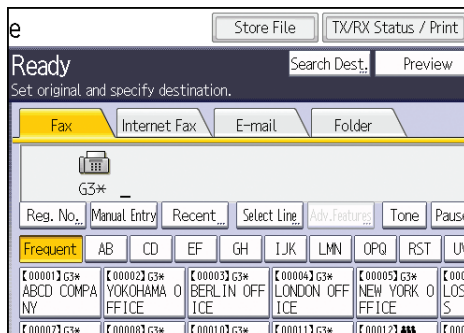
You can set this function so as not to send to unspecified people. A four to eight digit number can be specified as a password.

You can also change the file information after storing files.

1. Place the original, and then specify the scan settings you require.

Specify the [Original Orientation] setting correctly. If you do not, the top/bottom orientation of the original will not be displayed correctly in the preview.

2. Press [Store File].

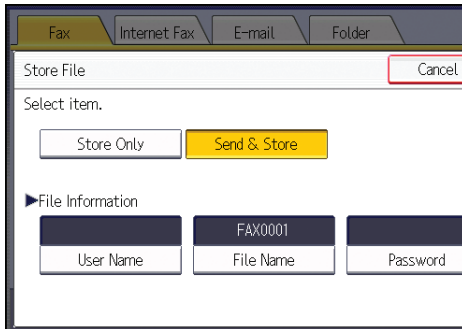


3. Select [Send & Store] or [Store Only].

Select [Send & Store] to send documents after they are stored.

Select [Store Only] to store documents.

4. Set the user name, file name, and password as necessary.



- **User Name**
Press [User Name], and then select a user name. To specify an unregistered user name, press [Manual Entry], and then enter the name. After specifying a user name, press [OK].
- **File Name**
Press [File Name], enter a file name, and then press [OK].
- **Password**
Press [Password], enter a password using the number keys, and then press [OK]. Re-enter the password for confirmation, and then press [OK].

5. Press [OK].

6. If you have selected [Send & Store], specify the receiver.

7. Press the [Start] key.

Sending Stored Documents

The machine sends documents stored with the facsimile function in the Document Server.

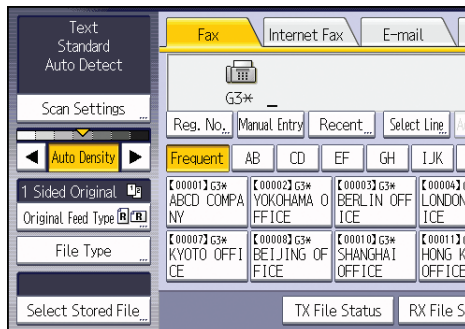
The documents stored in the Document Server can be sent again and again until they are deleted.

The stored documents are sent with the scan settings made when they were stored.

You cannot use the following transmission methods:

- Immediate Transmission
- Parallel Memory Transmission
- On Hook Dial
- Manual Dial

1. Press [Select Stored File].



2. Select the documents to be sent.

When multiple documents are selected, they are sent in the order of selection.

- Press [User Name] to place the documents in order by programmed user name.
- Press [File Name] to place the documents in alphabetical order.
- Press [Date] to place the documents in order of programmed date.
- Press [Queue] to arrange the order of the documents to be sent.

To view details about stored documents, press [Details].

Press the Thumbnails key to switch the screen to thumbnail display.

3. If you select a document with a password, enter the password using the number keys, and then press [OK].
4. When you want to add your originals to stored documents and send them all at once, press [Original + Stored File] or [Stored file + Original].

When [Original + Stored File] is pressed, the machine sends the originals, and then stored files.
When [Stored file + Original] is pressed, the machine sends the stored files, and then originals.

5. Press [OK].
6. To add an original to stored documents, place the original, and then select any scan settings you require.
7. Specify the destination, and then press the [Start] key.

Printing the Journal Manually

To print the Journal manually, select the printing method: [All], [Print per File No.], or [Print per User].

All

Prints the results of communications in the order made.

Print per File No.

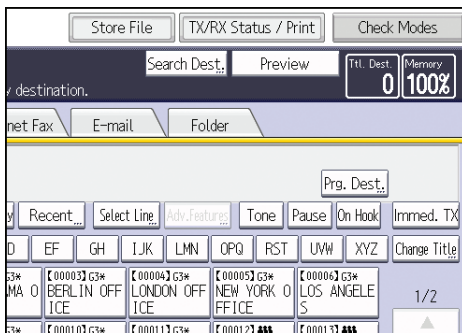
Prints only the results of communications specified by file number.

Print per User

Prints the results of communications by individual senders.

4

1. Press [TX/RX Status / Print].



2. Press [Print Journal].

3. Select the printing method.

4. If you selected [Print per File No.] in Step 3, enter a 4-digit file number using the number keys.

5. If you selected [Print per User] in Step 3, select a user from the list, and then press [OK].

6. Press the [Start] key.

7. Press [Exit] twice.

5. Print

This chapter describes frequently used printer functions and operations. For the information not included in this chapter, see Print on the supplied CD-ROM.

Quick Install

You can install the printer drivers easily from the CD-ROM provided with this machine.

Using Quick Install, the PCL 6 printer driver is installed under network environment, and the Standard TCP/IP port will be set.

★ Important

- **Manage Printers permission is required to install the drivers. Log on as an Administrators group member.**

1. Quit all applications. (Do not close this manual.)

2. Insert the provided CD-ROM into the computer's CD-ROM drive.

If the [AutoPlay] dialog box appears, click [Run SETUP.EXE].

If you are using a computer that is running Windows 8 or Windows Server 2012, click the drive and CD-ROM names when these appear in the upper right corner of the screen, and then click [Run SETUP.EXE].

3. Select an interface language, and then click [OK].

4. Click [Quick Install].

5. The software license agreement appears in the [License Agreement] dialog box. After reading the agreement, click [I accept the agreement.], and then click [Next].

6. Click [Next].

7. Select the machine model you want to use in the [Select Printer] dialog box.

8. Click [Install].

9. Configure the user code, default printer, and shared printer as necessary.

10. Click [Continue].

The installation starts.

If the [User Account Control] dialog box appears, and then click [Yes] or [Continue].

11. Click [Finish].

When you are prompted to restart your computer, restart it by following the instructions that appear.

12. Click [Exit] in the first window of the installer, and then take out the CD-ROM.

Displaying the Printer Driver Properties

This section explains how to open the printer driver properties from [Devices and Printers].

★ Important

- **Manage Printers permission is required to change the printer settings. Log on as an Administrators group member.**
 - **You cannot change the machine default settings for individual users. Settings made in the printer properties dialog box are applied to all users.**
1. On the [Start] menu, click [Devices and Printers].
 2. Right-click the icon of the printer you want to use.
 3. Click [Printer properties].

Standard Printing

★ Important

- The default setting is 2 sided printing. If you want to print on only one side, select [Off] for the 2 sided printing setting.
- If you send a print job via USB 2.0 while the machine is in Low Power mode or Sleep mode, an error message might appear when the print job is complete. In this case, check if the document was printed.

When Using the PCL 6 Printer Driver

1. Click the WordPad menu button in the upper left corner of the window, and then click [Print].
2. In the [Select Printer] list, select the printer you want to use.
3. Click [Preferences].
4. In the "Job Type:" list, select [Normal Print].
5. In the "Document Size:" list, select the size of the original to be printed.
6. In the "Orientation:" list, select [Portrait] or [Landscape] as the orientation of the original.
7. In the "Input Tray:" list, select the paper tray that contains the paper you want to print onto.

If you select [Auto Tray Select] in the "Input Tray:" list, the source tray is automatically selected according to the paper size and type specified.

8. In the "Paper Type:" list, select the type of paper that is loaded in the paper tray.
9. Select [Color] or [Black and White] in the "Color/ Black and White:" list.
10. If you want to print multiple copies, specify a number of sets in the "Copies:" box.
11. Click [OK].
12. Start printing from the application's [Print] dialog box.

Printing on Both Sides of Sheets

This section explains how to print on both sides of each page using the printer driver.

★ Important

- The types of paper that can be printed on both sides are as follows:
 - Plain (60 to 81 g/m²), Recycled, Special 1, Special 2, Special 3, Middle Thick (82 to 105 g/m²), Thick 1 (106 to 169 g/m²), Thick 2 (170 to 220 g/m²), Thick 3 (221 to 256 g/m²), Thin (52 to 59 g/m²), Color, Letterhead, Preprinted, Bond, Cardstock





When Using the PCL 6 Printer Driver

5

1. Click the WordPad menu button in the upper left corner of the window, and then click [Print].
2. In the [Select Printer] list, select the printer you want to use.
3. Click [Preferences].
4. Click the [Detailed Settings] tab.
5. In the "Menu:" box, click the [Edit] icon.
6. Select the method for binding the output pages in the "2 sided:" list.
7. Change any other print settings if necessary.
8. Click [OK].
9. Start printing from the application's [Print] dialog box.

Types of 2 sided Printing

You can select which way the bound pages open by specifying which edge to bind.

Orientation	Open to Left	Open to Top
Portrait		
Landscape		

Combining Multiple Pages into Single Page

This section explains how to print multiple pages onto a single sheet. The combine printing function allows you to economize on paper by printing multiple sheets at reduced size onto a single sheet.

When Using the PCL 6 Printer Driver

1. Click the WordPad menu button in the upper left corner of the window, and then click [Print].
2. In the [Select Printer] list, select the printer you want to use.
3. Click [Preferences].
4. Click the [Detailed Settings] tab.
5. In the "Menu:" box, click the [Edit] icon.
6. Select the combination pattern in the "Layout:" list, and then specify the method for combining pages in the "Page Order:" list.

To draw a border line around each page, select [Draw Frame Border].

7. Change any other print settings if necessary.
8. Click [OK].
9. Start printing from the application's [Print] dialog box.

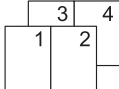
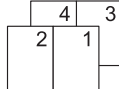
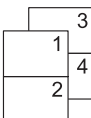
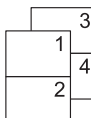
5

Types of Combine Printing

This function allows you to print 2, 4, 6, 9, or 16 pages at reduced size onto a single sheet and to specify a page ordering pattern for the combination. When combining 4 or more pages onto a single sheet of paper, four patterns are available.

The following illustrations show example page ordering patterns for 2- and 4-page combinations.

2 Pages per Sheet

Orientation	From Left to Right/Top to Bottom	From Right to Left/Top to Bottom
Portrait		
Landscape		

4 Pages per Sheet

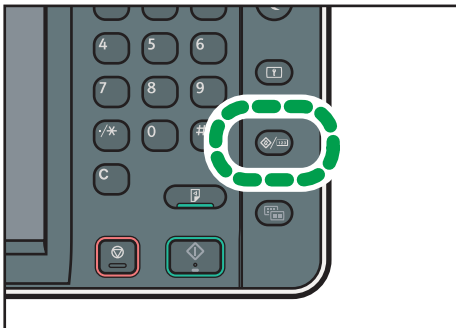
Right, then Down	Down, then Right	Left, then Down	Down, then Left																
<table border="1"><tr><td>1</td><td>2</td></tr><tr><td>3</td><td>4</td></tr></table>	1	2	3	4	<table border="1"><tr><td>1</td><td>3</td></tr><tr><td>2</td><td>4</td></tr></table>	1	3	2	4	<table border="1"><tr><td>2</td><td>1</td></tr><tr><td>4</td><td>3</td></tr></table>	2	1	4	3	<table border="1"><tr><td>3</td><td>1</td></tr><tr><td>4</td><td>2</td></tr></table>	3	1	4	2
1	2																		
3	4																		
1	3																		
2	4																		
2	1																		
4	3																		
3	1																		
4	2																		

Printing on Envelopes

Configure the paper settings appropriately using both the printer driver and the control panel.

Configuring Envelope Settings Using the Control Panel

1. Load envelopes in the paper tray.
2. Display the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.



CXX005

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.
3. Press [Tray Paper Settings].
 4. Select the paper size setting of the paper tray in which the envelopes are loaded.
 5. Select the envelope size, and then press [OK].
 6. Press [▼Next].
 7. Select the paper type setting of the paper tray in which the envelopes are loaded.
 8. Press [Envelope] in the "Paper Type" area, and then select the appropriate item in the "Paper Thickness" area.
 9. Press [OK].
 10. Close the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.
 - When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Printing on Envelopes Using the Printer Driver

When using the PCL 6 printer driver

1. Click the WordPad menu button in the upper left corner of the window, and then click [Print].
2. In the [Select Printer] list, select the printer you want to use.
3. Click [Preferences].
4. In the "Document Size:" list, select the envelope size.
5. In the "Input Tray:" list, select the paper tray where the envelopes are loaded.
6. In the "Paper Type:" list, select [Envelope].
7. Change any other print settings if necessary.
8. Click [OK].
9. Start printing from the application's [Print] dialog box.

Saving and Printing Using the Document Server

The Document Server enables you to store documents on the machine's hard disk, and allows you to edit and print them as necessary.

★ Important

- Applications with their own drivers, such as PageMaker, do not support this function.
- Do not cancel the file transfer process while the data is being sent to the Document Server. The process may not be canceled properly. If you accidentally cancel a print job, use the control panel of the machine to delete the transferred data. For details about how to delete documents that are stored in the Document Server, see "Deleting Stored Documents", Copy/ Document Server, or Web Image Monitor Help.
- Up to 3,000 files can be stored in the Document Server. New files cannot be stored when 3,000 files have already been stored. Even if less than 3,000 files are stored, new files cannot be stored when
 - The number of pages in a document exceeds 2,000.
 - The total number of stored pages in the machine and the sent data has reached 9,000 (It may be fewer depending on the print data).
 - The hard disk is full.

You can send data created on a client computer to the Document Server.

Storing Documents in Document Server

★ Important

- If the machine is not used as the Document Server, the maximum number of the documents that can be stored in the server may be less than the number described in the specification.
1. Click the WordPad menu button in the upper left corner of the window, and then click [Print].
 2. In the "Select Printer" list, select the printer you want to use.
 3. Click [Preferences].
 4. In the "Job Type:" list, click [Document Server].
 5. Click [Details...].
 6. Enter a user ID, file name, password, and user name as required.
 7. Specify the folder number to store the document in the "Folder Number" box.

When "0" is specified in the "Folder Number:" box, documents will be saved in the Shared folder.

8. If the folder is protected by a password, enter the password in the "Folder Password:" box.
9. Click [OK].
10. Change any other print settings if necessary.
11. Click [OK].
12. Start printing from the application's [Print] dialog box.

 **Note**

- You can print the documents stored in the Document Server using the control panel. For details, see page 139 "Printing Stored Documents".

Managing Documents Stored in Document Server

5

If this machine is configured as a network printer using TCP/IP, you can view or delete the documents stored in the machine's Document Server using Web Image Monitor from a client computer connected to the network. You can print and operate this machine remotely without operating the control panel.

6. Scan

This chapter describes frequently used scanner functions and operations. For the information not included in this chapter, see Scan on the supplied CD-ROM.

Basic Procedure When Using Scan to Folder

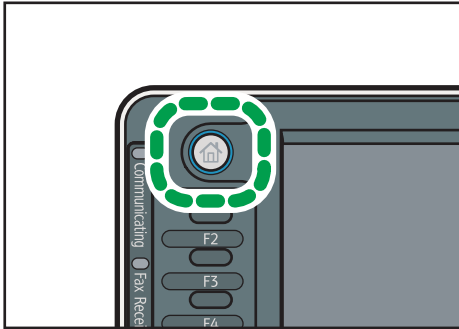
★ Important

- Before performing this procedure, see "Preparation for Sending by Scan to Folder", Scan and confirm the details of the destination computer. See also "Registering Folders", Connecting the Machine/ System Settings, and register the address of the destination computer to the address book.

1. Display the initial scanner screen.

- When using the standard operation panel

Press the [Home] key on the top left of the control panel, and press the [Scanner] icon on the [Home] screen.



CXX002

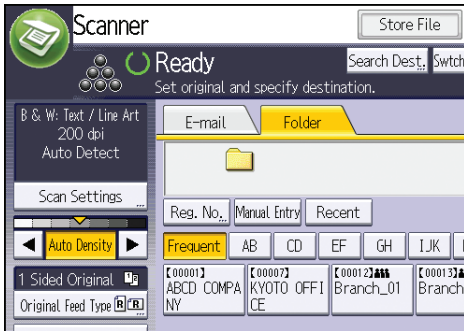
- When using the Smart Operation Panel

Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Scanner] icon on the Home screen 4.

2. Make sure that no previous settings remain.

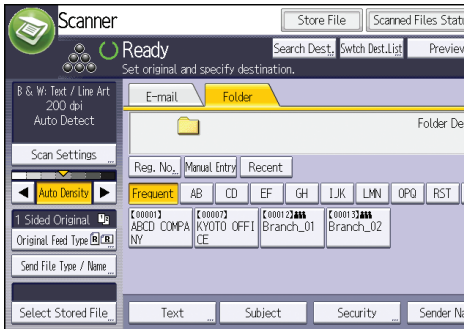
If a previous setting remains, press the [Reset] key.

3. Press the [Folder] tab.



4. Place originals.

5. If necessary, specify the scan settings according to the original to be scanned.



Example: Scanning the document in color/duplex mode, and saving as a PDF file.

- Press [Scan Settings], and then press [Full Color: Text / Photo] in the [Original Type] tab.
- Press [Original Feed Type], and then press [2 Sided Original].
- Press [PDF] under [Send File Type / Name].

6. Specify the destination.

You can specify multiple destinations.

7. Press the [Start] key.

Creating a Shared Folder on a Computer Running Windows/Confirming a Computer's Information

The following procedures explain how to create a shared folder on a computer running Windows, and how to confirm the computer's information. In these examples, Windows 7 Ultimate is the operating system, and the computer is a member in a network domain. Write down the confirmed information.

Step 1: Confirming the user name and computer name

Confirm the user name and the name of the computer you will send scanned documents to.

1. On the [Start] menu, point to [All Programs], then [Accessories], and then click on [Command Prompt].
2. Enter the command "ipconfig/all", and then press the [Enter] key.
3. Confirm the name of the computer.

The computer's name is displayed under [Host Name].

You can also confirm the IPv4 address. The address displayed under [IPv4 Address] is the IPv4 address of the computer.

4. Next, enter the command "set user", and then press the [Enter] key. (Be sure to put a space between "set" and "user".)
5. Confirm the user name.

The user name is displayed under [USERNAME].

Step 2: Creating a shared folder on a computer running Microsoft Windows

6

Create a shared destination folder in Windows and enable sharing. In the following procedure, a computer which is running under Windows 7 Ultimate and participating in a domain is used as an example.

★ Important

- You must log in as an Administrators group member to create a shared folder.
- If "Everyone" is left selected in step 6, the created shared folder will be accessible by all users. This is a security risk, so we recommend that you give access rights only to specific users. Use the following procedure to remove "Everyone" and specify user access rights.

1. Create a folder, just as you would create a normal folder, in a location of your choice on the computer.
2. Right-click the folder, and then click [Properties].
When using Windows XP, right-click the folder, and then click [Sharing and Security].
3. On the [Sharing] tab, select [Advanced Sharing...].
When using Windows XP, on the [Sharing] tab, select [Share this folder].
Proceed to step 5.
4. Select the [Share this folder] check box.
5. Click [Permissions].
6. In the [Group or user names:] list, select "Everyone", and then click [Remove].
7. Click [Add...].


8. In the [Select Users or Groups] window, click [Advanced...].
9. Specify one or more object types, select a location, and then click [Find Now].
10. From the list of results, select the groups and users you want to grant access to, and then click [OK].
11. In the [Select Users or Groups] window, click [OK].
12. In the [Groups or user names:] list, select a group or user, and then, in the [Allow] column of the permissions list, select either the [Full Control] or [Change] check box.
Configure the access permissions for each group and user.
13. Click [OK].

Step 3: Specifying access privileges for the created shared folder

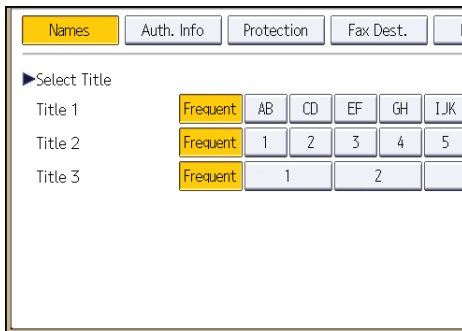
If you want to specify access privileges for the created folder to allow other users or groups to access the folder, configure the folder as follows:

1. Right-click the folder created in step 2, and then click [Properties].
2. On the [Security] tab, click [Edit...].
3. Click [Add...].
4. In the [Select Users or Groups] window, click [Advanced...].
5. Specify one or more object types, select a location, and then click [Find Now].
6. From the list of results, select the groups and users you want to grant access to, and then click [OK].
7. In the [Select Users or Groups] window, click [OK].
8. In the [Groups or user names:] list, select a group or user, and then, in the [Allow] column of the permissions list, select either the [Full Control] or [Change] check box.
9. Click [OK].

Registering an SMB Folder

1. Display the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.
 - When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon () on the Home screen 4.
2. Press [Address Book Mangmnt].

3. Check that [Program / Change] is selected.
4. Press [New Program].
5. Press [Change] under "Name".
The name entry display appears.
6. Enter the name, and then press [OK].
7. Press [▼Next].
8. Press the key for the classification you want to use under "Select Title".

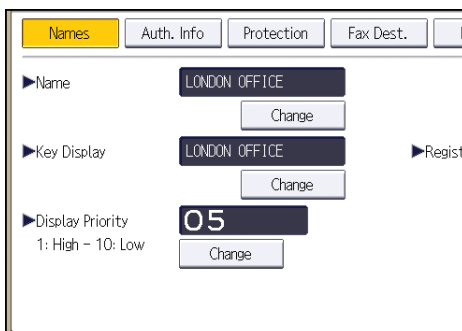


The keys you can select are as follows:

- [Frequent]: Added to the page that is displayed first.
- [AB], [CD], [EF], [GH], [IJK], [LMN], [OPQ], [RST], [UVW], [XYZ], [1] to [10]: Added to the list of items in the selected title.

You can select [Frequent] and one more key for each title.

9. Press [Auth. Info], and then press [▼Next].

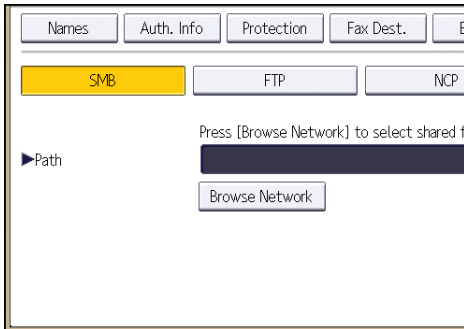


10. Press [Specify Other Auth. Info] on the right side of "Folder Authentication".

When [Do not Specify] is selected, the SMB User Name and SMB Password that you have specified in "Default User Name / Password (Send)" of File Transfer settings are applied.

11. Press [Change] under "Login User Name".
12. Enter the login user name of the destination computer, and then press [OK].

13. Press [Change] under "Login Password".
14. Enter the password of the destination computer, and then press [OK].
15. Enter the password again to confirm, and then press [OK].
16. Press [Folder].
17. Check that [SMB] is selected.



18. Press [Change] or [Browse Network], and then specify the folder.

To specify a folder, you can either enter the path manually or locate the folder by browsing the network.

19. Press [Connection Test] to check the path is set correctly.
20. Press [Exit].

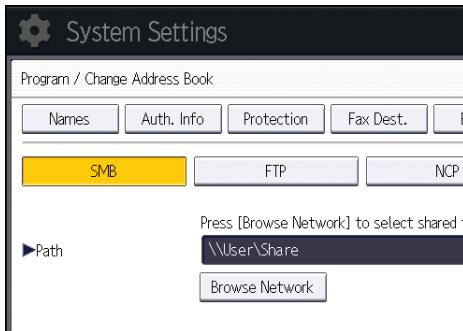
If the connection test fails, check the settings, and then try again.

21. Press [OK].
22. Press [Exit].
23. Close the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.
 - When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Locating the SMB folder manually

1. Press [Change] under "Path".
2. Enter the path where the folder is located.

For example: if the name of the destination computer is "User", and the folder name is "Share", the path will be \\User\Share.



If the network does not allow automatic obtaining of IP addresses, include the destination computer's IP address in the path. For example: if the IP address of the destination computer is "192.168.0.191", and the folder name is "Share", the path will be "\\192.168.0.191\Share".

3. Press [OK].

If the format of the entered path is not correct, a message appears. Press [Exit], and then enter the path again.

Locating the SMB folder using Browse Network

6

1. Press [Browse Network].

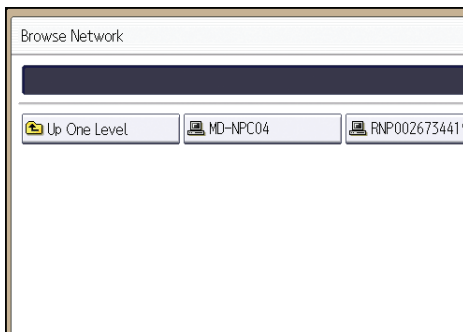
The client computers sharing the same network as the machine appear.

Network display only lists client computers you are authorized to access.

2. Select the group that contains the destination computer.

3. Select the computer name of the destination computer.

Shared folders under it appear.




You can press [Up One Level] to switch between levels.

4. Select the folder you want to register.

5. Press [OK].

Deleting an SMB Registered Folder

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon () on the Home screen 4.

2. Press [Address Book Mangmnt].

3. Check that [Program / Change] is selected.

4. Select the name whose folder you want to delete.

Press the name key, or enter the registered number using the number keys.

You can search by the registered name, user code, fax number, folder name, e-mail address, or IP-Fax destination.

5. Press [Folder].

6. Press the protocol which is not currently selected.


A confirmation message appears.

7. Press [Yes].

8. Press [OK].

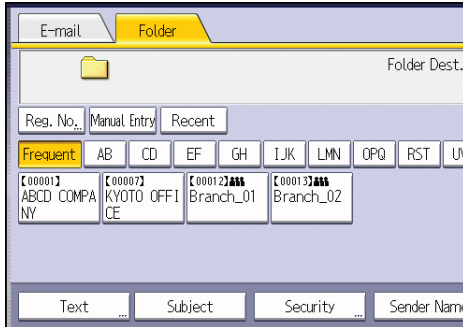
9. Press [Exit].

10. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

Entering the Path to the Destination Manually

1. Press [Manual Entry].



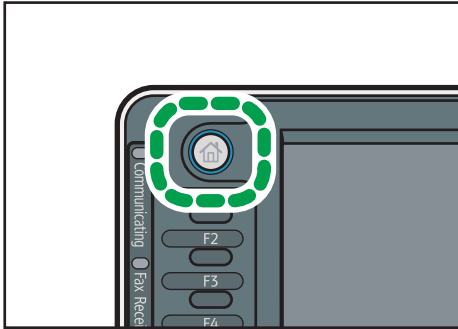
2. Press [SMB].
3. Press [Manual Entry] on the right side of the path field.
4. Enter the path for the folder.
 In the following example path, the shared folder name is "user" and the computer name is "desk01":
`\\desk01\user`
5. Press [OK].
6. Depending on the destination setting, enter the user name for logging in to the computer.
 Press [Manual Entry] to the right of the user name field to display the soft keyboard.
7. Depending on the destination setting, enter the password for logging in to the computer.
 Press [Manual Entry] for the password to display the soft keyboard.
8. Press [Connection Test].
 A connection test is performed to check whether the specified shared folder exists.
9. Check the connection test result, and then press [Exit].
10. Press [OK].

Basic Procedure for Sending Scan Files by E-mail

1. Display the initial scanner screen.

- When using the standard operation panel

Press the [Home] key on the top left of the control panel, and press the [Scanner] icon on the [Home] screen.



CXX002

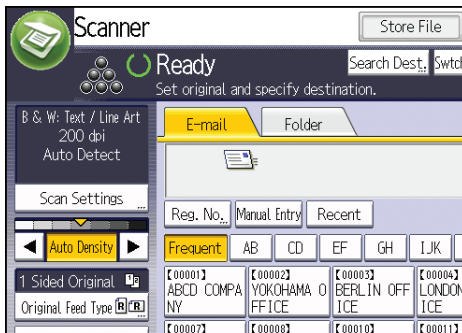
- When using the Smart Operation Panel

Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Scanner] icon on the Home screen 4.

2. Make sure that no previous settings remain.

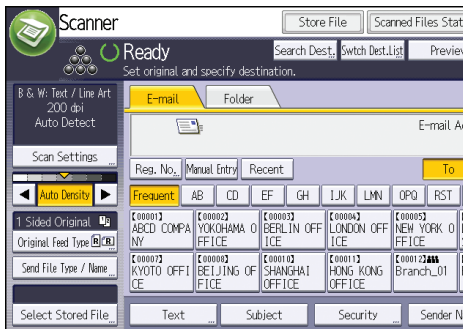
If a previous setting remains, press the [Reset] key.

3. Press the [E-mail] tab.



4. Place originals.

5. If necessary, specify the scan settings according to the original to be scanned.



Example: Scanning the document in color/duplex mode, and saving as a PDF file.

- Press [Scan Settings], and then press [Full Color: Text / Photo] in the [Original Type] tab.
- Press [Original Feed Type], and then press [2 Sided Original].
- Press [PDF] under [Send File Type / Name].

6. Specify the destination.

You can specify multiple destinations.

7. To specify the e-mail sender, press [Sender Name], and then press [OK].

8. To use Message Disposition Notification, press [Recept. Notice].

If you select [Recept. Notice], the selected e-mail sender will receive e-mail notification when the e-mail recipient has opened the e-mail.

9. Press the [Start] key.

Registering an E-mail Destination

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press [Address Book Mangmnt].

3. Check that [Program / Change] is selected.

4. Press [New Program].

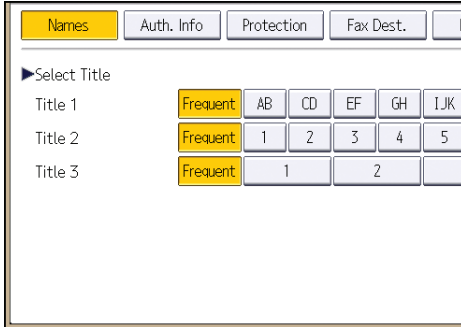
5. Press [Change] under "Name".

The name entry display appears.

6. Enter the name, and then press [OK].

7. Press [▼Next].

8. Press the key for the classification you want to use under "Select Title".



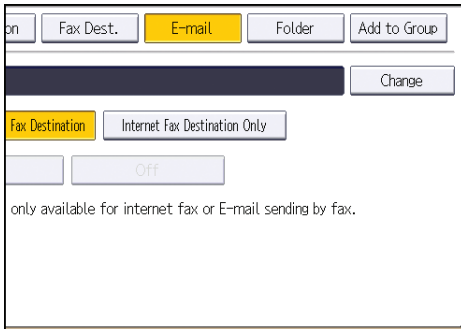
The keys you can select are as follows:

- [Frequent]: Added to the page that is displayed first.
- [AB], [CD], [EF], [GH], [IJK], [LMN], [OPQ], [RST], [UVW], [XYZ], [1] to [10]: Added to the list of items in the selected title.

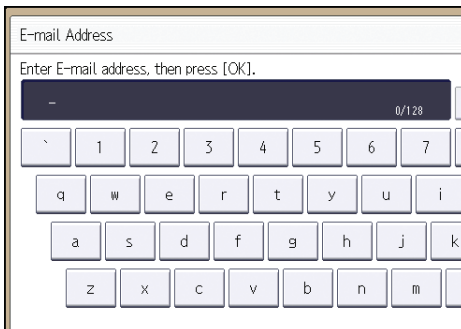
You can select [Frequent] and one more key for each title.

9. Press [E-mail].

10. Press [Change] under "E-mail Address".



11. Enter the e-mail address.



12. Press [OK].

13. Select [E-mail / Internet Fax Destination] or [Internet Fax Destination Only].

If [E-mail / Internet Fax Destination] is specified, registered e-mail addresses appear in both Internet fax address display and E-mail address display on the fax function screen, and in the address display on the scanner function screen.


If [Internet Fax Destination Only] is specified, registered e-mail addresses only appear in Internet fax display on the fax function screen.

14. If you want to use Internet fax, specify whether or not to use "Send via SMTP Server".

15. Press [OK].


16. Press [Exit].

17. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

Deleting an E-mail Destination

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon () on the Home screen 4.

2. Press [Address Book Mangmnt].

3. Check that [Program / Change] is selected.

4. Select the name whose e-mail address you want to delete.

Press the name key, or enter the registered number using the number keys. You can search by the registered name, user code, fax number, folder name, e-mail address, or IP-Fax destination.

5. Press [E-mail].


6. Press [Change] under "E-mail Address".

7. Press [Delete All], and then press [OK].

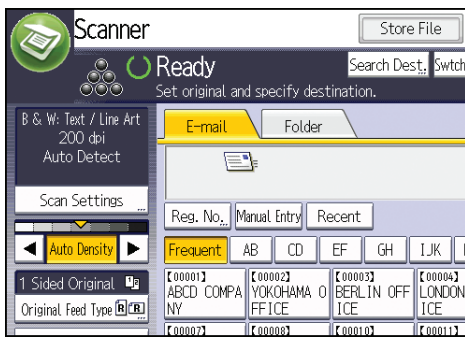
8. Press [OK].

9. Press [Exit].

10. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

Entering an E-mail Address Manually

1. Press [Manual Entry].**2. Enter the e-mail address.****3. Press [OK].**

Basic Procedure for Storing Scan Files

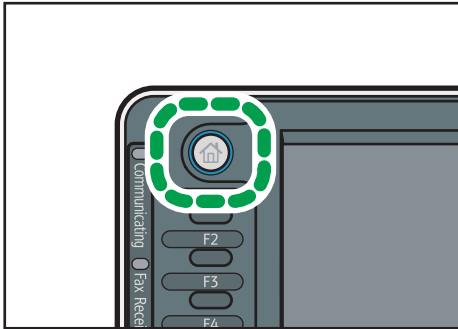
★ Important

- You can specify a password for each stored file. We recommend that you protect stored files from unauthorized access by specifying passwords.
- Scan file stored in the machine may be lost if some kind of failure occurs. We advise against using the hard disk to store important files. The supplier shall not be responsible for any damage that may result from the loss of files.

1. Display the initial scanner screen.

- When using the standard operation panel

Press the [Home] key on the top left of the control panel, and press the [Scanner] icon on the [Home] screen.



CXX002

- When using the Smart Operation Panel

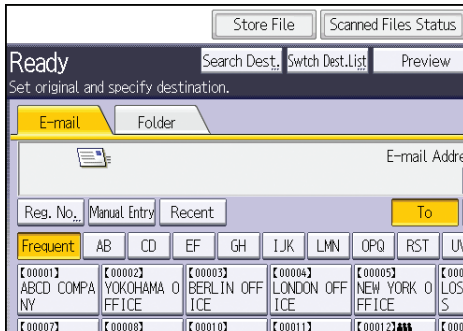
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Scanner] icon on the Home screen 4.

2. Make sure that no previous settings remain.

If a previous setting remains, press the [Reset] key.

3. Place originals.

4. Press [Store File].



5. Press [Store to HDD].

6. If necessary, specify the stored file's information, such as [User Name], [File Name], [Password], and [Select Folder].

- User Name
Press [User Name], and then select a user name. To specify an unregistered user name, press [Manual Entry], and then enter the name. After specifying a user name, press [OK].
- File Name
Press [File Name], enter a file name, and then press [OK].
- Password
Press [Password], enter a password, and then press [OK]. Re-enter the password for confirmation, and then press [OK].
- Select Folder
Specify the folder in which to save the stored files.

7. Press [OK].

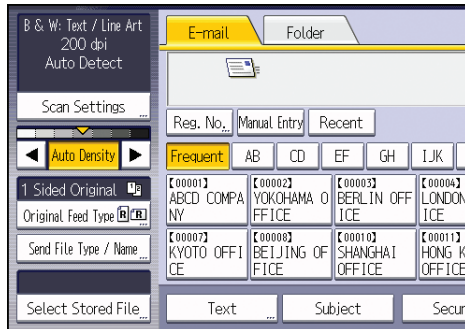
8. If necessary, press [Scan Settings] to specify scanner settings such as resolution and scan size.

9. Press the [Start] key.

Checking a Stored File Selected from the List

This section explains how to preview a file selected from the list of stored files.

1. Press [Select Stored File].



2. Specify the folder in which to save the stored files.
3. From the list of stored files, select the file you want to check.
You can select more than one file.
4. Press [Preview].

Specifying the File Type

This section explains the procedure for specifying the file type of a file you want to send.

File types can be specified when sending files by e-mail or Scan to Folder, sending stored files by e-mail or Scan to Folder, and saving files on a memory storage device.

You can select one of the following file types:

- Single Page: [TIFF / JPEG], [PDF]

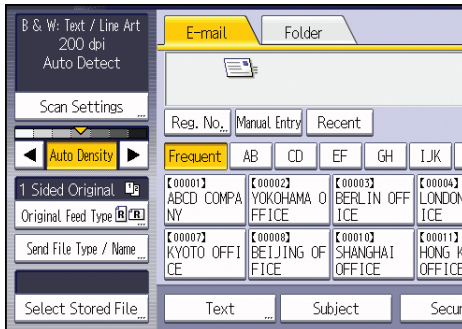
If you select a single-page file type when scanning multiple originals, one file is created for each single page and the number of files sent is the same as the number of pages scanned.

- Multi-page: [TIFF], [PDF]

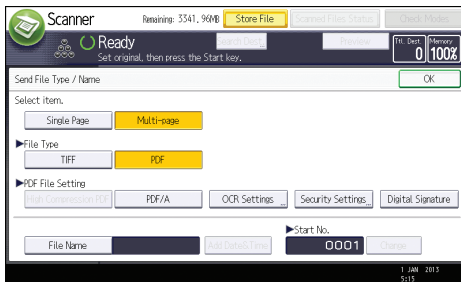
If you select a multi-page file type when scan multiple originals, scanned pages are combined and sent as a single file.

Selectable file types differ depending on the scan settings and other conditions. For details about file types, see "Notes About and Limitations of File Types", Scan.

1. Press [Send File Type / Name].



2. Select a file type.

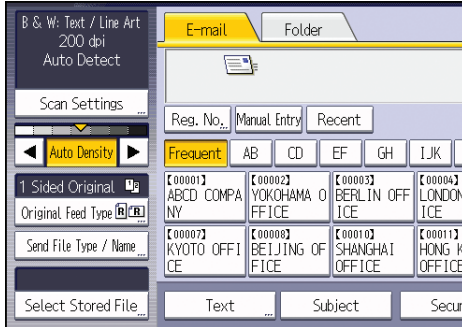


If the File Type is set to [PDF], configure PDF File Setting as required.

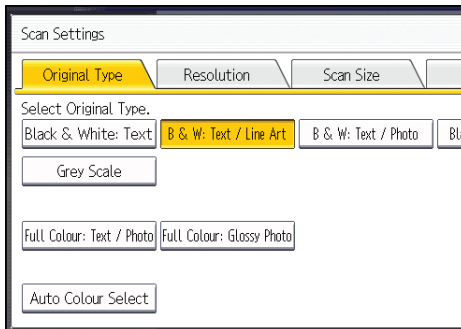
3. Press [OK].

Specifying Scan Settings

1. Press [Scan Settings].



2. Specify resolution, scan size, and other settings, as required.



3. Press [OK].

7. Document Server

This chapter describes frequently used Document Server functions and operations. For the information not included in this chapter, see Copy/ Document Server on the supplied CD-ROM.

Storing Data

This section describes the procedure for storing documents on the Document Server.

Important

- A document accessed with a correct password remains selected even after operations are complete, and it can be accessed by other users. After the operation, be sure to press the [Reset] key to cancel the document selection.
- The user name registered to a stored document in the Document Server is to identify the document creator and type. It is not to protect confidential documents from others.
- When turning on the fax transmission or scanning by the scanner, make sure that all other operations are ended.

File Name

A file name such as "COPY0001" and "COPY0002" is automatically attached to the scanned document. You can change the file name.

User Name

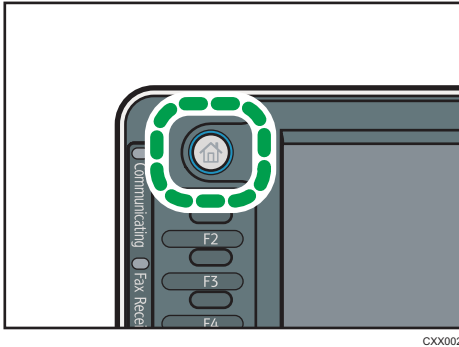
You can register a user name to identify the user or user group that stored the documents. To assign it, select the user name registered in the Address Book, or enter the name directly. Depending on the security setting, [Access Privileges] may appear instead of [User Name].

For details about the Address Book, see "Registering Addresses and Users for Facsimile/Scanner Functions", Connecting the Machine/ System Settings.

Password

To prevent unauthorized printing, you can specify a password for any stored document. A protected document can only be accessed if its password is entered. If a password is specified for the documents, the lock icon appears on the left side of the file name.

1. Press the [Home] key on the top left of the control panel, and press the [Document Server] icon on the screen.



CXX002

2. Press [To Scanning Screen].
3. Press [Target Fldr. to Store].
4. Specify a folder in which to store the document, and then press [OK].
5. Press [User Name].
6. Specify a user name, and then press [OK].

The user names shown are names that were registered in the Address Book. To specify a name not shown in the screen, press [Manual Entry], and then enter a user name.

7. Press [File Name].
8. Enter a file name, and then press [OK].
9. Press [Password].
10. Enter a password with the number keys, and then press [OK].

You can use four to eight digits for the password.

11. For double-check, enter the password again, and then press [OK].
12. Place the original.
13. Specify the original scanning conditions.
14. Press the [Start] key.

The original is scanned. The document is saved in the Document Server.

After scanning, a list of folders will be displayed. If the list does not appear, press [Finish Scanning].

Printing Stored Documents

Prints stored documents on the Document Server.

The items you can specify on the printing screen are as follows:

- Paper tray
- The number of prints
- [Finishing] ([Sort], [Rotate Sort], [Stack], [Staple], [Punch])
- [Cover/Slip Sheet] ([Front Cover], [Front/Back Cover], [Designate/Chapter], [Slip Sheet])
- [Edit / Stamp] ([Margin Adj.], [Stamp])
- [2 Sided Copy Top to Top], [2 Sided Copy Top to Bottom], [Booklet], [Magazine]

For details about each function, see Copy/ Document Server.

1. Select a folder.

No.	Folder Name	Created Date/Time	Sel.	File
	Shared Folder			
001	User001	28 Feb. 11:03		
002	User002	28 Feb. 11:03		
003	User003	28 Feb. 11:04		
004	User004	28 Feb. 11:04		
005	User005	28 Feb. 11:04		

2. Select a document to be printed.

3. When printing two or more documents at a time, repeat Step 2.

Up to 30 documents can be printed.

4. When specifying printing conditions, press [To Printing Screen], and then configure print settings.

5. Enter the number of print copies with the number keys.

The maximum quantity that can be entered is 999.

6. Press the [Start] key.

8. Web Image Monitor

This chapter describes frequently used Web Image Monitor functions and operations. For the information not included in this chapter, see Connecting the Machine/ System Settings on the supplied CD-ROM or Web Image Monitor Help.

Displaying Top Page

This section explains the Top Page and how to display Web Image Monitor.

★ Important

- When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10".

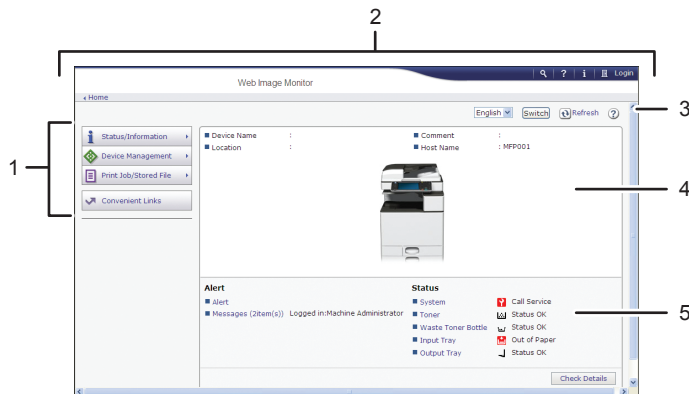
1. Start your Web browser.
2. Enter "http://(machine's IP address or host name)/" in your Web browser's URL bar.

Top Page of Web Image Monitor appears.

If the machine's host name has been registered on the DNS or WINS server, you can enter it.

When setting SSL, a protocol for encrypted communication, under environment which server authentication is issued, enter "https://(machine's IP address or host name)/".

Web Image Monitor is divided into the following areas:



CVD004

1. Menu area



If you select a menu item, its content will be shown.


2. Header area

The dialog box for switching to the user mode and administrator mode appears, and each mode's menu will be displayed.

The link to Help and dialog box for keyword search appears.

3. Refresh/Help

 (Refresh): Click  at the upper right in the work area to update the machine information. Click the Web browser's [Refresh] button to refresh the entire browser screen.

 (Help): Use Help to view or download Help file contents.

4. Basic Information area

Displays the basic information of the machine.

5. Work area

Displays the contents of the item selected in the menu area.

9. Adding Paper and Toner

This chapter describes how to load paper into the paper tray and recommended paper sizes and types.

Precautions for Loading Paper

CAUTION

- When loading paper, take care not to trap or injure your fingers.

Important

- Do not stack paper over the limit mark.

Note

- To prevent multiple sheets from being fed at once, fan the paper before loading it.
- If you load paper when only a few sheets of paper remain in the tray, multiple sheet feeding may occur. Remove any remaining paper, stack them with the new sheets of paper, and then fan the entire stack before loading it into the tray.
- Straighten curled or warped paper before loading.
- For details about the paper sizes and types that can be used, see page 155 "Recommended Paper Sizes and Types".
- You might at times hear a rustling noise from paper moving through the machine. This noise does not indicate a malfunction.

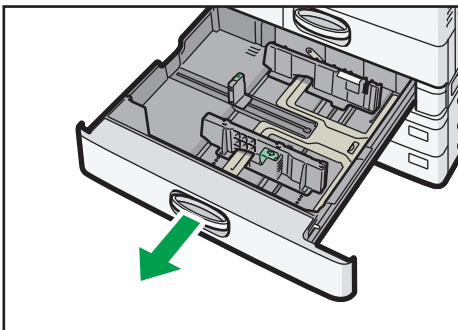
Loading Paper into Paper Trays

Every paper tray is loaded in the same way.

In the following example procedure, paper is loaded into Tray 2.

★ Important

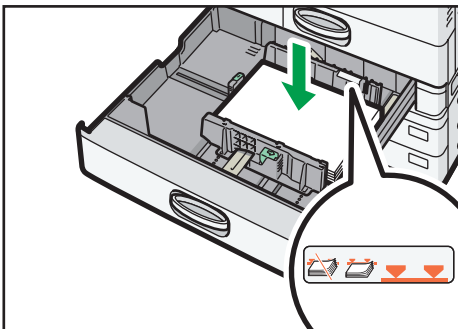
- **Region A** (mainly Europe and Asia)
Tray 1 can hold A4 paper only. If you want to print on A5, B5 JIS, or 8 1/2 × 11 from Tray 1, contact your service representative.
 - **Region B** (mainly North America)
Tray 1 can hold 8 1/2 × 11 paper only. If you want to print on A4, A5, or B5 JIS from Tray 1, contact your service representative.
 - Check the paper edges are aligned at the right side.
 - 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.
1. Check that paper in the paper tray is not being used, and then pull the tray carefully out until it stops.



CVA010

2. Square the paper and load it print side up.

Do not stack paper over the limit mark.



CVA011

3. Carefully push the paper tray fully in.

Note

- Various sizes of paper can be loaded in Trays 2–4 by adjusting the positions of side fences and end fence. For details, see "Changing the Paper Size in Trays 2–4", Paper Specifications and Adding Paper.
- You can load envelopes in Trays 2–4. When loading envelopes, place them in the correct orientation. For details, see page 163 "Envelopes".

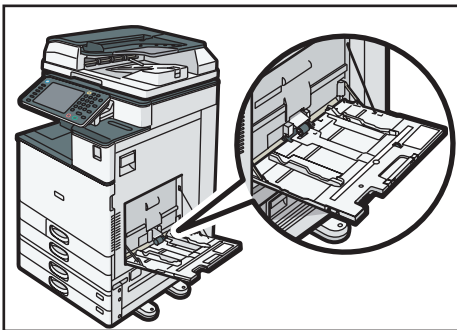
Loading Paper into the Bypass Tray

Use the bypass tray to use OHP transparencies, adhesive labels, translucent paper, and paper that cannot be loaded in the paper trays.

★ Important

- The maximum number of sheets you can load at the same time depends on paper type. Do not stack paper over the limit mark. For the maximum number of sheets you can load, see page 155 "Recommended Paper Sizes and Types".

1. Open the bypass tray.

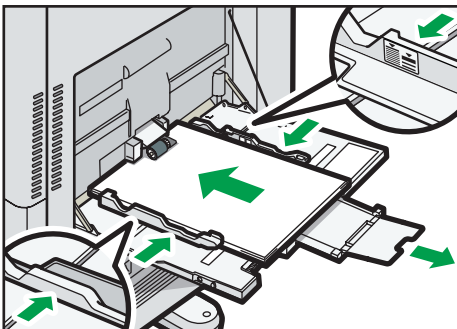


DAV001

2. Load the paper face down until you hear the beep.




3. Align the paper guides to the paper size.

If the guides are not flush against the paper, images might be skewed or paper misfeeds might occur.



DAV002

↓ Note

- When you use the bypass tray, it is recommended to load the paper in  orientation.
- Certain types of paper might not be detected properly when placed on the bypass tray. If this happens, remove the paper and place it on the bypass tray again.
- Pull the extender out when loading sheets larger than A4 , 8 1/2 × 11  in the bypass tray.

- When loading thick paper, thin paper, or OHP transparencies, specify the paper size and the paper type.
- Letterhead paper must be loaded in a specific orientation. For details, see page 152 "Loading Orientation-fixed Paper or Two-sided Paper".
- You can load envelopes into the bypass tray. Envelopes must be loaded in a specific orientation. For details, see page 163 "Envelopes".
- Specify the sizes of paper that are not automatically detected. For details about the sizes that can be detected automatically, see page 155 "Recommended Paper Sizes and Types". For details about how to specify sizes, see page 147 "Printing from the Bypass Tray Using the Printer Function" or "Copying from the Bypass Tray", Copy/ Document Server.
- When copying from the bypass tray, see "Copying from the Bypass Tray", Copy/ Document Server. When printing from a computer, see page 147 "Printing from the Bypass Tray Using the Printer Function".
- When the [Panel Key Sound] is turned off, it does not sound if you load paper into the bypass tray. For details about [Panel Key Sound], see "General Features", Connecting the Machine/ System Settings.

Printing from the Bypass Tray Using the Printer Function

★ Important

- If you select [Machine Setting(s)] in [Bypass Tray] under [Tray Setting Priority] in [System] of the Printer Features menu, the settings made using the control panel have priority over the printer driver settings. For details, see "System", Print.
- The default of [Bypass Tray] is [Machine Setting(s): Any Type].

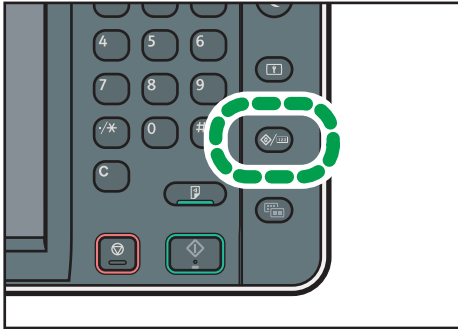
↓ Note

- Settings remain valid until they are changed.
- For details about setting printer drivers, see "Printing Documents", Print.
- The default setting for [Printer Bypass Paper Size] in [Tray Paper Settings] is [Auto Detect].

Specifying regular sizes using the control panel

1. Display the initial settings screen.

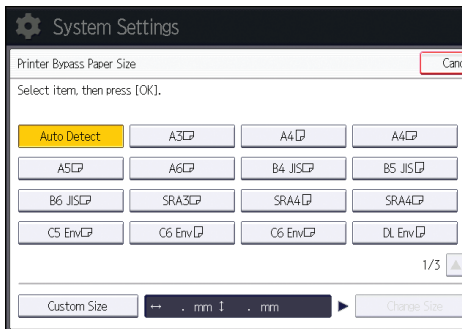
- When using the standard operation panel
Press the [User Tools/Counter] key.



CXX005

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

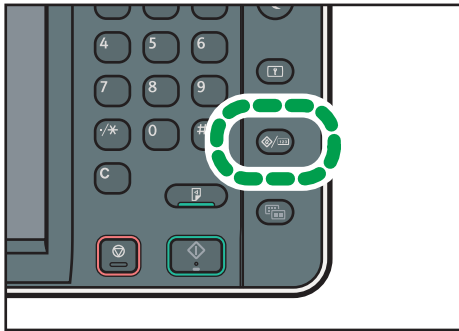
2. Press [Tray Paper Settings].
3. Press [Printer Bypass Paper Size].
4. Select the paper size.



5. Press [OK].
6. Close the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.
 - When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Specifying a custom size paper using the control panel

1. Display the initial settings screen.
 - When using the standard operation panel
Press the [User Tools/Counter] key.



CXX005

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press [Tray Paper Settings].

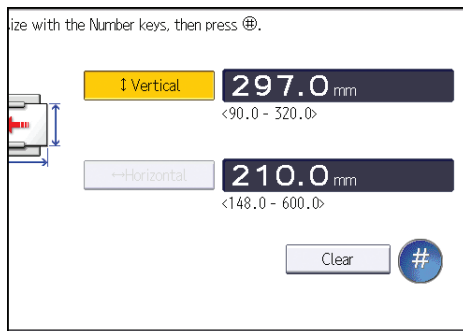
3. Press [Printer Bypass Paper Size].

4. Press [Custom Size].

If a custom size is already specified, press [Change Size].

5. Press [Vertical].

6. Enter the vertical size using the number keys, and then press [#].



7. Press [Horizontal].

8. Enter the horizontal size using the number keys, and then press [#].

9. Press [OK] twice.

10. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

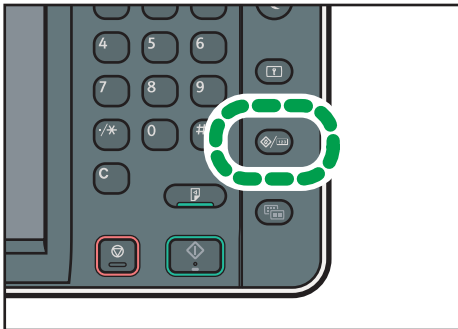
Specifying thick paper, thin paper, or OHP transparencies for paper type using the control panel

★ Important

- Use A4 or 8 1/2 × 11 size OHP transparencies, and specify their size.
- Usually only one side of OHP transparencies can be used for printing. Be sure to load them with the print side down.
- When printing onto OHP transparencies, remove printed sheets one by one.

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.



CXX005

- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press [Tray Paper Settings].

3. Press [Printer Bypass Paper Size], and then specify the paper size.

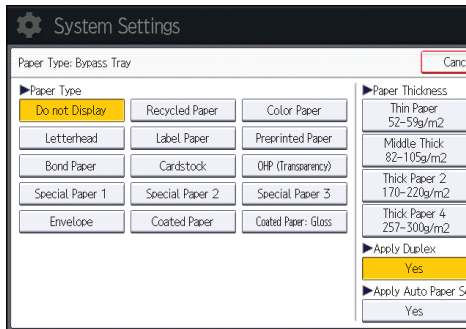
4. Press [OK].

5. Press [▼Next].

6. Press [Paper Type: Bypass Tray].


7. Select the proper items, according to the paper type you want to specify.

- Press [OHP (Transparency)] on the [Paper Type] area when loading OHP transparencies.
- To load thin or thick paper, press [Do not Display] on the [Paper Type] area, and then select the appropriate paper thickness in the [Paper Thickness] area.



8. Press [OK].

9. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

Note

- We recommend that you use specified OHP transparencies.
- For details about paper thickness, see "Tray Paper Settings", Connecting the Machine/ System Settings.

Loading Orientation-fixed Paper or Two-sided Paper

Orientation-fixed (top to bottom) or two-sided paper (for example, letterhead paper, punched paper, or copied paper) might not be printed correctly, depending on how the originals and paper are placed.





Settings for the User Tools

- Copier mode
Specify [Yes] for [Letterhead Setting] in [Input / Output] under the Copier / Document Server Features menu, and then place the original and paper as shown below.
- Printer mode
Specify [Auto Detect] or [On (Always)] for [Letterhead Setting] in [System] under the Printer Features menu, and then place the paper as shown below.



For details about the letterhead settings, see "Input / Output", Copy/ Document Server, or "System", Print.




Original orientation and paper orientation

The meanings of the icons are as follows:











Icon	Meaning
 	Place or load paper scanned or printed side face up.
 	Place or load paper scanned or printed side face down.

- Original orientation











Original orientation	Exposure glass	ADF
Readable orientation		

Original orientation	Exposure glass	ADF
Unreadable orientation	<ul style="list-style-type: none"> • Copy  <ul style="list-style-type: none"> • Scanner 	

- Paper orientation
 - Copier mode

Copy side	Tray 1	Trays 2-4	Bypass tray
One-sided		 	 
Two-sided		 	 

- Printer mode

Print side	Tray 1	Trays 2-4	Bypass tray
One-sided		 	 
Two-sided		 	 

 **Note**

- In copier mode:
 - For details about how to make two-sided copies, see page 75 "Duplex Copying".
- In printer mode:
 - To print on letterhead paper when [Auto Detect] is specified for [Letterhead Setting], you must specify [Letterhead] as the paper type in the printer driver's settings.
 - 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.
 - For details about how to make two-sided prints, see page 110 "Printing on Both Sides of Sheets".













Recommended Paper Sizes and Types

This section describes recommended paper sizes and types.

★ Important





- If you use paper that curls, either because it is too dry or too damp, a staple clogging or paper jam may occur.
- Do not use paper designed for inkjet printers, as these may stick to the fusing unit and cause a misfeed.
- When you load OHP transparencies, check the front and back of the sheets, and place them correctly, or a misfeed might occur.










Tray 1

Paper type and weight	Paper size	Paper capacity
60–300 g/m ² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4	 Region A A4   Region B 8 1/2 × 11 	550 sheets
60–300 g/m ² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4	*1  Region A A5  , B5 JIS  , 8 1/2 × 11   Region B A4  , A5  , B5 JIS 	550 sheets

*1 To load paper any of the sizes specified above, contact your service representative.


















Tray 2





Paper type and weight	Paper size	Paper capacity
<p>60–300 g/m² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4</p>	<p>Paper sizes that can be detected automatically:</p> <p> Region A</p> <p>A3, A4, A5, B4 JIS, B5 JIS, 8 1/2 × 11, SRA3</p> <p> Region B</p> <p>A4, A5, B5 JIS, 11 × 17, 8 1/2 × 14, 8 1/2 × 11, 7 1/4 × 10 1/2, 12 × 18</p>	<p>550 sheets</p>
<p>60–300 g/m² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4</p>	<p>Select the paper size using the Tray Paper Settings menu:</p> <p> Region A</p> <p>A5, A6, B6 JIS, 11 × 17, 8 1/2 × 14, 8 1/2 × 13, 8 1/2 × 11, 8 1/4 × 14, 8 1/4 × 13, 8 × 13, 8 × 10, 7 1/4 × 10 1/2, 5 1/2 × 8 1/2, 8K, 16K, 12 × 18, 11 × 15, 10 × 14</p> <p> Region B</p> <p>A3, A4, A5, A6, B4 JIS, B5 JIS, B6 JIS, 8 1/2 × 13, 8 1/4 × 14, 8 1/4 × 13, 8 × 13, 8 × 10, 7 1/4 × 10 1/2, 5 1/2 × 8 1/2, 8K, 16K, 11 × 15, 10 × 14, SRA3</p>	<p>550 sheets</p>

Paper type and weight	Paper size	Paper capacity
60–300 g/m ² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4	Custom size ^{*1} :  Region A Vertical: 90.0–320.0 mm Horizontal: 148.0–457.2 mm  Region B Vertical: 3.55–12.59 inches Horizontal: 5.83–18.00 inches	550 sheets
Envelopes	Select the paper size using the Tray Paper Settings menu: 4 ¹ / ₈ × 9 ¹ / ₂  , 3 ⁷ / ₈ × 7 ¹ / ₂  , C5 Env  , C6 Env  , DL Env 	<ul style="list-style-type: none"> : 50 sheets : Double flap: 15 sheets Single flap: 25 sheets

*1 When loading paper with a vertical length of more than 304.8 mm (12.00 inches) in Trays 2–4, use paper that has a horizontal width of 450.0 mm (17.71 inches) or less.





Trays 3 and 4
















Paper type and weight	Paper size	Paper capacity
60–300 g/m ² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4	Paper sizes that can be detected automatically:  Region A A3  , A4  , A5  , B4 JIS  , B5 JIS  , 8 ¹ / ₂ × 11  , SRA3   Region B A4  , A5  , B5 JIS  , 11 × 17  , 8 ¹ / ₂ × 14  , 8 ¹ / ₂ × 11  , 7 ¹ / ₄ × 10 ¹ / ₂  , 12 × 18 	550 sheets

Paper type and weight	Paper size	Paper capacity
60–300 g/m ² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4	Select the paper size using the Tray Paper Settings menu:  Region A 11 × 17□, 8 ¹ / ₂ × 14□, 8 ¹ / ₂ × 13□, 8 ¹ / ₂ × 11□, 8 ¹ / ₄ × 14□, 8 ¹ / ₄ × 13□, 8 × 13□, 8 × 10□, 7 ¹ / ₄ × 10 ¹ / ₂ □□, 8K□, 16K□□, 12 × 18□, 11 × 15□, 10 × 14□  Region B A3□, A4□, B4 JIS□, B5 JIS□, 8 ¹ / ₂ × 13□, 8 ¹ / ₄ × 14□, 8 ¹ / ₄ × 13□, 8 × 13□, 8 × 10□, 7 ¹ / ₄ × 10 ¹ / ₂ □□, 8K□, 16K□□, 11 × 15□, 10 × 14□, SRA3□	550 sheets
60–300 g/m ² (16 lb. Bond–110 lb. Cover) Plain Paper–Thick Paper 4	Custom size ^{*1} :  Region A Vertical: 182.0–320.0 mm Horizontal: 148.0–457.2 mm  Region B Vertical: 7.17–12.59 inches Horizontal: 5.83–18.00 inches	550 sheets
Envelopes	Select the paper size using the Tray Paper Settings menu: 4 ¹ / ₈ × 9 ¹ / ₂ □, C5 Env□	50 sheets

* 1 When loading paper with a vertical length of more than 304.8 mm (12.00 inches) in Trays 2–4, use paper that has a horizontal width of 450.0 mm (17.71 inches) or less.

Bypass tray

Paper type and weight	Paper size	Paper capacity
52–300 g/m ² (14 lb. Bond–110 lb. Cover) Thin Paper–Thick Paper 4	<p>Paper sizes that can be detected automatically:</p> <p> Region A</p> <p>A3□, A4□□, A5□□, A6□, B4 JIS□, B5 JIS□□, B6 JIS□, SRA3□</p> <p> Region B</p> <p>11 × 17□, 8¹/₂ × 11□□, 5¹/₂ × 8¹/₂□, 12 × 18□, SRA3□</p>	<ul style="list-style-type: none"> • 100 sheets (up to 10 mm in height) • Thick Paper 1: 40 sheets • Thick Paper 2–Thick Paper 3: 20 sheets • Thick Paper 4: 16 sheets
52–300 g/m ² (14 lb. Bond–110 lb. Cover) Thin Paper–Thick Paper 4	<p>*1</p> <p> Region A</p> <p>11 × 17□, 8¹/₂ × 14□, 8¹/₂ × 13□, 8¹/₂ × 11□□, 8¹/₄ × 14□, 8¹/₄ × 13□, 8 × 13□, 8 × 10□,</p> <p>7¹/₄ × 10¹/₂□□, 5¹/₂ × 8¹/₂□, 8K□, 16K□□, 12 × 18□, 11 × 15□, 10 × 14□, SRA4□□</p> <p> Region B</p> <p>A3□, A4□□, A5□□, A6□, B4 JIS□, B5 JIS□□, B6 JIS□, 8¹/₂ × 14□, 8¹/₂ × 13□, 8¹/₄ × 14□, 8¹/₄ × 13□, 8 × 13□, 8 × 10□,</p> <p>7¹/₄ × 10¹/₂□□, 8K□, 16K□□, 11 × 15□, 10 × 14□, SRA4□□</p>	<ul style="list-style-type: none"> • 100 sheets (up to 10 mm in height) • Thick Paper 1: 40 sheets • Thick Paper 2–Thick Paper 3: 20 sheets • Thick Paper 4: 16 sheets

Paper type and weight	Paper size	Paper capacity
52–300 g/m ² (14 lb. Bond–110 lb. Cover) Thin Paper–Thick Paper 4	Custom size ^{*2} :  Region A Vertical: 90.0–320.0 mm Horizontal: 148.0–457.2 mm ^{*3, *4}  Region B Vertical: 3.55–12.59 inches Horizontal: 5.83–18.00 inches ^{*3, *4}	<ul style="list-style-type: none"> • 100 sheets (up to 10 mm in height) • Thick Paper 1: 40 sheets • Thick Paper 2–Thick Paper 3: 20 sheets • Thick Paper 4: 16 sheets
OHP transparencies	A4  , 8 1/2 × 11 	50 sheets
Translucent paper	A3  , A4  , B4 JIS  , B5 JIS 	1 sheet
Label paper (adhesive labels)	B4 JIS  , A4 	30 sheets
Envelopes	^{*1} 4 1/8 × 9 1/2  , 3 7/8 × 7 1/2  , C5 Env  , C6 Env  , DL Env 	10 sheets

- *1 Select the paper size. For copier mode, see "Copying onto Regular Size Paper from the Bypass Tray", Copy/ Document Server. For printer mode, see page 147 "Specifying regular sizes using the control panel".
- *2 Enter the paper size. For copier mode, see "Copying onto Custom Size Paper from the Bypass Tray", Copy/ Document Server. For printer mode, see page 148 "Specifying a custom size paper using the control panel".
- *3 In printer or facsimile mode, the maximum horizontal length of the custom size is 600.0 mm (23.62 inches).
- *4 Paper that has a horizontal length of 432 mm (17.1 inches) or more is prone to creasing, feed failures, and jamming.

Paper Thickness

Paper Thickness ^{*1}	Paper weight
Thin Paper ^{*2}	52–59 g/m ² (14–15 lb. Bond)
Plain Paper 1	60–74 g/m ² (16–20 lb. Bond)



Paper Thickness ^{*1}	Paper weight
Plain Paper 2	75–81 g/m ² (20 lb. Bond)
Middle Thick	82–105 g/m ² (20–28 lb. Bond)
Thick Paper 1	106–169 g/m ² (28 lb. Bond–90 lb. Index)
Thick Paper 2	170–220 g/m ² (65–80 lb. Cover)
Thick Paper 3	221–256 g/m ² (80 lb. Cover–140 lb. Index)
Thick Paper 4	257–300 g/m ² (140 lb. Index–110 lb. Cover)

*1 Print quality will decrease if the paper you are using is close to the minimum or maximum weight. Change the paper weight setting to thinner or thicker.

*2 Depending on the type of thin paper, the edges may crease or the paper may be misfed.

Note

- Certain types of paper, such as translucent paper or OHP transparencies, may produce noise when delivered. This noise does not indicate a problem and print quality is unaffected.
- The paper capacity described in the tables above is an example. Actual paper capacity might be lower, depending on the paper type.
- When loading paper, make sure the stack height does not exceed the limit mark of the paper tray.
- If multiple sheet feeding occurs, fan sheets thoroughly or load sheets one by one from the bypass tray.
- Flatten out curled sheets before loading them.
- Depending on the paper sizes and types, the copy/print speed may be slower than usual.
- When loading thick paper of 106–300 g/m² (28 lb. Bond–110 lb. Cover), see page 162 "Thick Paper".
- When loading envelopes, see page 163 "Envelopes".
- When copying or printing onto letterhead paper, the paper placing orientation is different depending on which function you are using. For details, see page 152 "Loading Orientation-fixed Paper or Two-sided Paper"
- If you load paper of the same size and same type in two or more trays, the machine automatically feeds from one of the trays in which [Yes] is selected for [Apply Auto Paper Select] when the first tray in use runs out of paper. This function is called Auto Tray Switching. This saves interrupting a copy run to replenish paper when making a large number of copies. You can specify the paper type of the paper trays under [Paper Type]. For details, see "Tray Paper Settings", Connecting the Machine/ System Settings. For the setting procedure of the Auto Tray Switching function, see "General Features", Copy/ Document Server.
- When loading label paper:

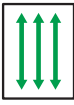
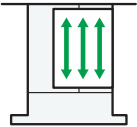
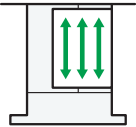
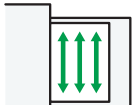

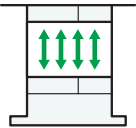
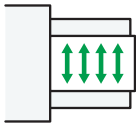
- We recommend that you use specified label paper.
- It is recommended to place one sheet at a time.
- Press [Bypass], and then select the appropriate paper thickness for [Paper Type].
- When loading OHP transparencies:
 - It is recommended to place one sheet at a time.
 - When copying onto OHP transparencies, see "Copying onto OHP Transparencies", Copy/Document Server.
 - When printing on OHP transparencies from the computer, see page 150 "Specifying thick paper, thin paper, or OHP transparencies for paper type using the control panel".
 - Fan OHP transparencies thoroughly whenever you use them. This prevents OHP transparencies from sticking together, and from feeding incorrectly.
 - Remove copied or printed sheets one by one.
- When loading translucent paper:
 - When loading translucent paper, always use long grain paper, and set the paper direction according to the grain.
 - Translucent paper easily absorbs humidity and becomes curled. Remove curl in the translucent paper before loading.
 - Remove copied or printed sheets one by one.
- When loading coated paper:
 - To print on coated paper: press the [User Tools/Counter] key, press [Tray Paper Settings], and then, for each tray's [Paper Type] be sure to specify [Paper Type] to [Coated Paper], and [Paper Thickness] to the appropriate paper thickness.
 - To print on high-gloss coated paper: press the [User Tools/Counter] key, press [Tray Paper Settings], and then, for each tray's [Paper Type], be sure to set [Paper Type] to [Coated Paper: Gloss].
 - When loading coated paper or glossy paper, always fan the paper before using it.
 - If a paper jam occurs or if the machine makes a strange noise when feeding stacks of coated paper, feed the coated paper from the bypass tray one sheet at a time.
- After continuous printing of A5 , A6 , envelopes or other smaller custom paper sizes, printing on different sized paper may require a wait of up to 1 minute for adjustments.

Thick Paper

This section gives you various details about and recommendations concerning thick paper.

When loading thick paper of 106–300 g/m² (28 lb. Bond–110 lb. Cover), follow the recommendations below to prevent misfeeds and loss of image quality.

- Store all your paper in the same environment - a room where the temperature is 20–25°C (68–77°F) and the humidity is 30–65%.
- When loading paper in Trays 1–4, be sure to load at least 20 sheets. Also, be sure to position the side fences flush against the paper stack.
- Jams and misfeeds can occur when printing on thick smooth paper. To prevent such problems, be sure to fan smooth paper thoroughly before loading them. If paper continues to become jammed or feed in together even after they are fanned, load them one by one from the bypass tray.
- When loading thick paper, set the paper direction according to its grain, as shown in the following diagram:

Direction of paper grain	Tray 1	Trays 2–4	Bypass tray
			
	Not recommended		


↓ Note


- Select [Thick Paper 1], [Thick Paper 2], [Thick Paper 3], or [Thick Paper 4] as the paper thickness in [Tray Paper Settings].
- Even if thick paper is loaded as described above, normal operations and print quality might still not be possible, depending on the paper type.
- Prints might have prominent vertical creases.
- Prints might be noticeably curled. Flatten out prints if they are creased or curled.

Envelopes

This section gives you various details about and recommendations concerning envelopes.

★ Important



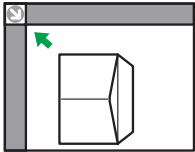
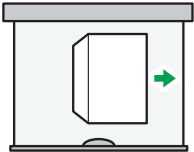
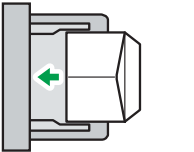


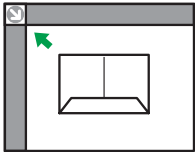
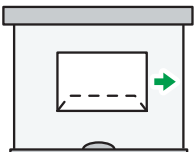
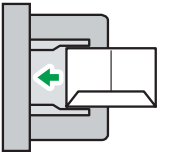
- Do not use window envelopes.
- Misfeeds might occur depending on the length and shape of the flaps.
- Only envelopes that are at least 148 mm (5.9 inches) wide and whose flaps are open can be loaded in the  orientation.

- When loading envelopes in the  orientation, load them with flaps fully open. Otherwise, they might not feed into the machine.
- Before loading envelopes, press down on them to remove any air from inside, 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.

In copier mode

The way to load envelopes varies depending on the orientation of the envelopes. When copying onto envelopes, load them according to the applicable orientation shown below:

How to load envelopes

Orientation of envelopes	Exposure glass	Trays 2–4	Bypass tray
Side-opening envelopes  	 <ul style="list-style-type: none"> • Flaps: open • Bottom side of envelopes: toward the left of the machine • Side to be scanned: face down 	 <ul style="list-style-type: none"> • Flaps: open • Bottom side of envelopes: toward the right of the machine • Side to be printed: face up 	 <ul style="list-style-type: none"> • Flaps: open • Bottom side of envelopes: toward the left of the machine • Side to be printed: face down
Side-opening envelopes  	 <ul style="list-style-type: none"> • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be scanned: face down 	* 1  <ul style="list-style-type: none"> • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be printed: face up 	 <ul style="list-style-type: none"> • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be printed: face down


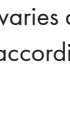
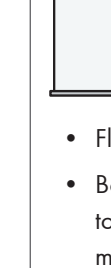
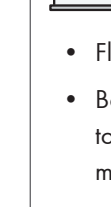

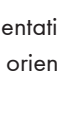
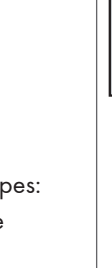
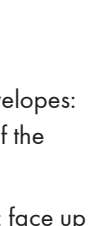
*1 You cannot load side-opening envelopes in the  orientation in Trays 3 and 4.

When loading envelopes, specify the envelope size and thickness. For details, see page 85 "Copying onto Envelopes".

In printer mode

The way to load envelopes varies depending on the orientation of the envelopes. When printing onto envelopes, load them according to the applicable orientation shown below:

How to load envelopes

Types of envelopes	Trays 2-4	Bypass tray
Side-opening envelopes  	 <ul style="list-style-type: none"> • Flaps: open • Bottom side of envelopes: toward the right of the machine • Side to be printed: face up 	 <ul style="list-style-type: none"> • Flaps: open • Bottom side of envelopes: toward the left of the machine • Side to be printed: face down
Side-opening envelopes  	*1  <ul style="list-style-type: none"> • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be printed: face up 	 <ul style="list-style-type: none"> • Flaps: closed • Bottom side of envelopes: toward the back of the machine • Side to be printed: face down

*1 You cannot load side-opening envelopes in the  orientation in Trays 3 and 4.

When loading envelopes, select "Envelope" as the paper types using both [Tray Paper Settings] and printer driver and specify the thickness of envelopes. For details, see page 113 "Printing on Envelopes".

To print on envelopes that are loaded with their short edges against the machine body, rotate the print image by 180 degrees using the printer driver.

Recommended envelopes

For information about recommended envelopes, contact your local dealer.

For details about the sizes of envelopes you can load, see page 155 "Recommended Paper Sizes and Types".

Note

- Load only one size and type of envelope at a time.
- The Duplex function cannot be used with envelopes.
- To get better output quality, it is recommended that you set the right, left, top, and bottom print margin, to at least 15 mm (0.6 inches) each.
- Output quality on envelopes may be uneven if parts of an envelope have differing thicknesses. Print one or two envelopes to check print quality.
- Copied or printed sheets are delivered to the internal tray even if you specified a different tray.
- Flatten out prints if they are creased or curled.
- Check the envelopes are not damp.
- High temperature and high humidity conditions can reduce print quality and cause envelopes to become creased.
- Depending on the environment, copying or printing on envelopes may wrinkle them even if they are recommended.
- Certain types of envelopes might come out creased, dirtied, or misprinted. If you are printing a solid color on an envelope, lines may appear where the overlapped edges of the envelope make it thicker.

Adding Toner

This section explains precautions when adding toner, how to send faxes or scanned documents when the toner has run out, and how to dispose of used toner.

WARNING

- Do not incinerate toner (new or used) or toner containers. Doing so risks burns. Toner will ignite on contact with naked flame.

WARNING

- Do not store toner (new or used) or toner containers anywhere near naked flames. Doing so risks fire and burns. Toner will ignite on contact with naked flame.

WARNING

- Do not use a vacuum cleaner to remove spilled toner (including used toner). Absorbed toner may cause a fire or explosion due to electrical contact flickering inside the vacuum cleaner. However, it is possible to use a vacuum cleaner that is explosion-proof and dust ignition-proof. If toner is spilled on the floor, remove the spilled toner slowly using a wet cloth, so that the toner is not scattered.

CAUTION

- Do not crush or squeeze toner containers. Doing so can cause toner spillage, possibly resulting in dirtying of skin, clothing, and floor, and accidental ingestion.

CAUTION

- Store toner (new or used), toner containers, and components that have been in contact with toner out of reach of children.

CAUTION

- If toner or used toner is inhaled, gargle with plenty of water and move into a fresh air environment. Consult a doctor if necessary.

CAUTION

- If toner or used toner gets into your eyes, flush immediately with large amounts of water. Consult a doctor if necessary.

CAUTION

- If toner or used toner is swallowed, dilute by drinking a large amount of water. Consult a doctor if necessary.

CAUTION

- When removing jammed paper or replacing toner, avoid getting toner (new or used) on your clothing. If toner comes into contact with your clothing, wash the stained area with cold water. Hot water will set the toner into the fabric and make removing the stain impossible.

CAUTION

- When removing jammed paper or replacing toner, avoid getting toner (new or used) on your skin. If toner comes into contact with your skin, wash the affected area thoroughly with soap and water.

CAUTION



- When replacing a toner or waste toner container or consumables with toner, make sure that the toner does not splatter. Put the waste consumables in a bag after they are removed. For consumables with a lid, make sure that the lid is shut.

Important

- Always replace the toner cartridge when a notification appears on the machine.
- Fault may occur if you use toner other than the recommended type.
- When adding toner, do not turn off the main power. If you do, settings will be lost.
- Store toner where it will not be exposed to direct sunlight, temperatures above 35°C (95°F), or high humidity.
- Store toner horizontally.
- Do not shake the toner cartridge with its mouth down after removing it. Residual toner may scatter.
- Do not repeatedly install and remove toner cartridges. This will result in toner leakage.

Follow the instruction on the screen regarding how to replace a toner cartridge.

Note

- If "Toner Cartridge is almost empty." appears, the toner has almost run out. Have a replacement toner cartridge at hand.
- If  appears when there is a lot of toner, follow the toner replacement instructions that appear on the screen. Pull out the cartridge, and then reinstall it.
- You can check the name of the required toner and the replacement procedure using the [Add Toner] screen.

- For details about how to check contact number where you can order supplies, see "Inquiry", Maintenance and Specifications.

Sending Faxes or Scanned Documents When Toner Has Run Out

When the machine has run out of toner, the indicator on the display lights. Note that even if there is no toner left, you can still send faxes or scanned documents.

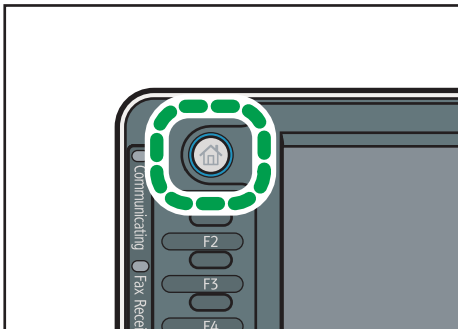
★ Important

- If number of communications executed after the toner has run out and not listed in the automatically output Journal exceeds 200, communication is not possible.

1. Display the initial facsimile or scanner screen.

- When using the standard operation panel

Press the [Home] key on the top left of the control panel, and press the [Facsimile] icon or the [Scanner] icon on the [Home] screen.



CXX002

- When using the Smart Operation Panel

Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [Fax] icon or the [Scanner] icon on the Home screen 4.

2. Press [Exit], and then perform transmission operation.

The error message disappears.

↓ Note

- Any reports are not printed.

Disposing of Used Toner

This section describes what to do with used toner.

Toner cannot be re-used.

Pack used toner containers in the container's box or a bag to prevent the toner from leaking out of the container when you dispose of it.

 **Region A** (mainly Europe and Asia)

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.

10. Troubleshooting

This chapter describes basic troubleshooting procedures.

When a Status Icon Is Displayed

This section describes the status icons displayed when the machine requires the user to remove misfed paper, to add paper, or to perform other procedures.

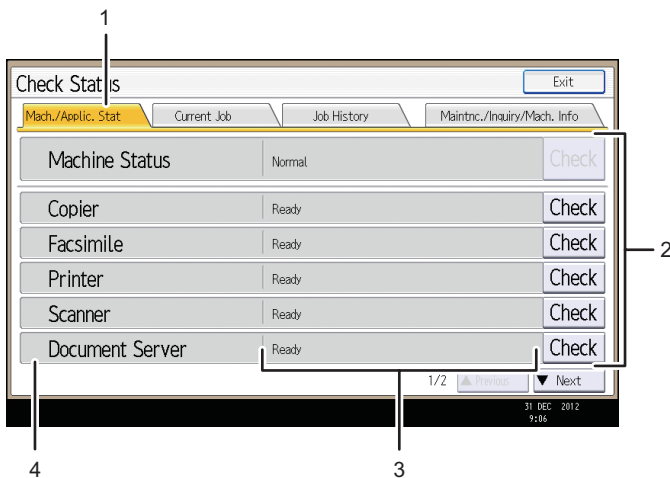
Status Icons	Status
 : Paper Misfeed icon	Appears when a paper misfeed occurs. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting.
 : Original Misfeed icon	Appears when an original misfeed occurs. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting.
 : Load Paper icon	Appears when paper runs out. For details about loading paper, see "Loading Paper", Paper Specifications and Adding Paper.
 : Add Toner icon	Appears when toner runs out. For details about adding toner, see "Adding Toner", Maintenance and Specifications.
 : Add Staple icon	Appears when staples run out. For details about adding staples, see "Adding Staples", Maintenance and Specifications.
 : Waste Toner Full icon	Appears when the waste toner bottle is full. For details about replacing the waste toner bottle, see "Replacing the Waste Toner Bottle", Maintenance and Specifications.
 : Hole Punch Receptacle Full icon	Appears when the hole punch receptacle is full. For details about removing punch waste, see "Removing Staple Waste", Troubleshooting.
 : Service Call icon	Appears when the machine is malfunctioning or requires maintenance.

Status Icons	Status
☐* : Open Cover icon	Appears when one or more covers of the machine are open.

When the Indicator Lamp for the [Check Status] Key Is Lit or Flashing

If the indicator lamp for the [Check Status] key lights up or flashes, press the [Check Status] key to display the [Check Status] screen. Check the status of each function in the [Check Status] screen.

[Check Status] screen



CUR012

1. [Mach./Applic. Stat] tab

Indicates the status of the machine and each function.

2. [Check]

If an error occurs in the machine or a function, press [Check] to view details.


Pressing [Check] displays an error message or the corresponding function screen. Check the error message displayed on the function screen and take the appropriate action. For details about how to resolve the problems described in error messages, see "When Messages Appear", Troubleshooting.

3. Messages


Displays a message that indicates the status of the machine and each function.

4. Status icons

The status icons that can be displayed are described below:

: The function is performing a job.

: An error has occurred on the machine.

: The function cannot be used because an error has occurred in the function or machine. This icon may also appear if the toner is running low.

The following table explains problems that cause the indicator lamp for the [Check Status] key to light or flash.

Problems	Causes	Solutions
Documents and reports do not print out.	The paper output tray is full.	Remove the prints from the tray.
Documents and reports do not print out.	There is no paper left.	Load paper. For details about loading paper, see "Loading Paper", Paper Specifications and Adding Paper.
An error has occurred.	A function which has the status "Error Occurred" in the [Check Status] screen is defective.	Press [Check] in the function which the error has occurred. Then check the displayed message, and take appropriate action. For details about error messages and their solutions, see "When Messages Appear", Troubleshooting. You can use other functions normally.
The machine is unable to connect to the network.	A network error has occurred.	<ul style="list-style-type: none"> • Check that the machine is correctly connected to the network, and that the machine is correctly set. For details about how to connect the network, see "Interface Settings", Connecting the Machine/ System Settings. • For details about connecting to the network, contact your administrator. • If the indicator lamp is still lit even after trying to solve the problem as described here, contact your service representative.

When the Machine Makes a Beeping Sound

The following table describes the meaning of the various beep patterns that the machine produces to alert users about left originals and other machine conditions.

Beep patterns	Meanings	Causes
Single short beep	Panel/screen input accepted.	A control panel or screen key was pressed.
Short, then long beep	Panel/screen input rejected.	An invalid key was pressed on the control panel or screen, or the entered password was incorrect.
Single long beep	Job completed successfully.	A Copier/Document Server Features job has finished.
Two long beeps	Machine has warmed up.	When the power is turned on or the machine exits Sleep mode, the machine has fully warmed up and is ready for use.
Five long beeps	Soft alert	An auto reset was performed through the simple screen of the Copier/Document Server function, the Facsimile function, or the Scanner function.
Five long beeps repeated four times.	Soft alert	An original has been left on the exposure glass or paper tray is empty.
Five short beeps repeated five times.	Strong alert	The machine requires user attention because paper has jammed, the toner needs replenishing, or other problems have occurred.

↓ Note

- Users cannot mute the machine's beep alerts. When the machine beeps to alert users of a paper jam or toner request, if the machine's covers are opened and closed repeatedly within a short space of time, the beep alert might continue, even after normal status has resumed.
- You can select to enable or disable beep alerts. For details about Panel Key Sound, see "General Features", Connecting the Machine/ System Settings.

When You Have Problems Operating the Machine

Problems	Causes	Solutions
When the machine is turned on, the only icon that appears on the home screen is the [Copier] icon. (When using the standard operation panel)	Functions other than the copier function are not yet ready.	Wait a little longer.
The machine has just been turned on and the User Tools screen is displayed, but the User Tools menu has items missing.	Functions other than the copier function are not yet ready. Time required varies by function. Functions appear in the User Tools menu when they become ready for use.	Wait a little longer.
The indicator lamp remains lit and the machine does not enter Sleep mode even though the [Energy Saver] key was pressed.	In some cases, the machine does not enter Sleep mode when the [Energy Saver] key is pressed.	Before you press the [Energy Saver] key, check that the status of the machine does not prevent it from entering Sleep mode. For details about statuses that inhibit Sleep mode, see "Saving Energy", Getting Started.
The display is turned off.	The machine is in Sleep mode.	<p>When using the standard operation panel</p> <p>Press the [Energy Saver] key or the [Check Status] key to clear Sleep mode.</p> <p>When using the Smart Operation Panel</p> <p>Press the [Check Status] key to clear Sleep mode.</p>
Nothing happens when the [Check Status] key or the [Energy Saver] key is pressed.	The power is turned off.	Make sure the main power indicator is off, and then turn on the power.

Problems	Causes	Solutions
The power turns off automatically.	The Weekly Timer setting is set to [Main Power Off].	Change the Weekly Timer setting. For details about the Weekly Timer setting, see "Timer Settings", Connecting the Machine/ System Settings.
The user code entry screen is displayed.	Users are restricted by User Code Authentication.	For details about how to log in when User Code Authentication is enabled, see "When the Authentication Screen is Displayed", Getting Started.
The Authentication screen appears.	Basic Authentication, Windows Authentication, LDAP Authentication or Integration Server Authentication is set.	Enter your login user name and user password. For details about the Authentication screen, see "When the Authentication Screen is Displayed", Getting Started.
An error message remains, even if misfed paper is removed.	Paper is still jammed in the tray.	Remove the jammed paper by following the procedures displayed on the control panel. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting.
An error message remains displayed even if the indicated cover is closed.	One or more covers that are not indicated are still open.	Close all the covers of the machine.
Original images are printed on the reverse side of the paper.	You may have loaded the paper incorrectly.	Load the paper correctly. For details about loading paper, see "Loading Paper", Paper Specifications and Adding Paper.

Problems	Causes	Solutions
Misfeeds occur frequently.	Using curled paper often causes misfeeds, soiled paper edges, or slipped positions while performing staple or stack printing.	<ul style="list-style-type: none"> • Take the stiffness out of the paper with your hands to straighten out the curl. • Load the paper up side down so that the curled edges face downward. For details about recommended paper, see "Recommended Paper", Paper Specifications and Adding Paper. • Lay cut paper on a flat surface to prevent paper from curling, and do not lean it against the wall. For details about the proper way to store paper, see "Paper Storage", Paper Specifications and Adding Paper.
Misfeeds occur frequently.	The tray's side or end fences may not be set properly.	<ul style="list-style-type: none"> • Remove the misfed paper. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting. • Check that the side or end fences are set properly. For details about setting the side and end fences, see "Changing the Paper Size", Paper Specifications and Adding Paper.

Problems	Causes	Solutions
Misfeeds occur frequently.	Paper of undetectable size has been loaded.	<ul style="list-style-type: none"> Remove the misfed paper. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting. If you load a paper size that is not selected automatically, you need to specify the paper size with the control panel. For details about specifying paper size with the control panel, see "Changing to a Size That Is Not Automatically Detected", Paper Specifications and Adding Paper.
Misfeeds occur frequently.	There is a foreign object on the finisher tray.	<ul style="list-style-type: none"> Remove the misfed paper. For details about removing jammed paper, see "Removing Jammed Paper", Troubleshooting. Do not place anything on the finisher tray.
Cannot print in duplex mode.	You have selected a paper tray that is not set for duplex printing.	Change the setting for "Apply Duplex" in [System Settings] to enable duplex printing for the paper tray. For details about setting "Apply Duplex", see "Tray Paper Settings", Connecting the Machine/ System Settings.
Cannot print in duplex mode.	You have selected a paper type that cannot be used for duplex printing.	In [System Settings], select a paper type that can be used for duplex printing. For details about setting "Paper Type", see "Tray Paper Settings", Connecting the Machine/ System Settings.
Paper does not align neatly when it is output from the internal shift tray.	The paper press attached to the paper output slot of the internal shift tray is pointed towards the back or front of the tray.	Adjust the paper press so that it points in the same direction as the paper that is output.

Problems	Causes	Solutions
An error has occurred when the Address Book is changed from the display panel or Web Image Monitor.	The Address Book cannot be changed while deleting the multiple stored documents.	Wait a while, and then retry the operation.
The Address Book cannot be changed from the display panel.	The Address Book cannot be changed while it is being backed up from Web Image Monitor or other tools running on the computer.	<ul style="list-style-type: none"> • Wait until the Address Book backup is complete, and then try to change the Address Book again. • If an SC997 error occurs, press [Exit].
Cannot use Web Image Monitor to print documents stored in Document Server.	When print volume limits are specified, users cannot print beyond their print volume limit. Print jobs selected by users who have reached their print volume limits will be canceled.	<ul style="list-style-type: none"> • For details about specifying print volume limits, see Security Guide. • To view the status of a print job, see [Print Job History]. In Web Image Monitor, click [Job] on the [Status/Information] menu. And then click [Print Job History] in "Document Server".
The function does not run or cannot be used.	If you are not able to carry out your job, it may be that the machine is being used by another function.	<p>Wait until the current job is completed before trying again.</p> <p>For details about Function Compatibility, see "When Multiple Functions Cannot Be Executed Simultaneously", Troubleshooting.</p>
The function does not run or cannot be used.	The function cannot be performed while the Address Book is being backed up from Web Image Monitor or other tools running on the computer.	Wait a while. When the Address Book backup is complete, the function will be performed.
Paper is bent.	Paper may be bent when it is ejected from the finisher upper tray.	Change the output tray to the finisher shift tray.

Note

- If you cannot make copies as you want because of paper type, paper size, or paper capacity problems, use the recommended paper. For details about recommended paper, see page 155 "Recommended Paper Sizes and Types".

When Multiple Functions Cannot Be Executed Simultaneously

If you are not able to carry out your job, it may be that the machine is being used by another function. Wait until the current job is completed before trying again. In certain cases, you can carry out another job using a different function while the current job is being performed.

For details about Function Compatibility, see "Function Compatibility", Troubleshooting.

Messages Displayed When Using the Copy/Document Server Function

★ Important

- If you cannot make copies as you want because of the paper type, paper size or paper capacity problems, use recommended paper. For details about recommended paper, see page 155 "Recommended Paper Sizes and Types".

Messages	Causes	Solutions
"Cannot delete the folder because it contains locked files. Please contact the file administrator."	The folder cannot be deleted because it contains a locked original.	Unlock the locked original to delete it. For details about locked files, see Security Guide.
"Cannot detect original size."	The original placed on the exposure glass is a non-standard size.	<ul style="list-style-type: none"> • Place the original on the exposure glass again. Face the original down. • If the machine cannot detect the size of the original, specify the size manually - do not use Auto Paper Select mode or the Auto Reduce/Enlarge function. For details about specifying the settings, see "Sizes Detectable with Auto Paper Select", Paper Specifications and Adding Paper.
"Cannot detect original size."	Original is not placed, or the original placed on the exposure glass is a non-standard size.	<ul style="list-style-type: none"> • Place the original correctly. • Specify the paper size. • When placing an original directly on the exposure glass, the lifting/lowering action of the exposure glass cover or the Auto Document Feeder (ADF) triggers the automatic original size detection process. Lift the exposure glass cover or the ADF 30 degrees or more.

Messages	Causes	Solutions
"Cannot display preview of this page."	The image data may have been corrupted.	Press [Exit] to display the preview screen without a thumbnail. If the selected document contains several pages, press [Switch] on the "Display Page" area to change the page, and then a preview of the next page will appear.
"Cannot punch this paper size."	The Punch function cannot be used with paper size selected.	For details about paper sizes, see "Specifications for Punch Unit (Internal Finisher SR3130)", Maintenance and Specifications.
"Cannot staple paper of this size."	The Staple function cannot be used with paper size selected.	Select an appropriate paper size. For details about paper sizes, see "Specifications for Internal Finisher SR3130" and "Specifications for Finisher SR3180", Maintenance and Specifications.
"Check paper size."	An irregular paper size is set.	If you press the [Start] key, the copy will start using the selected paper.
"Duplex is not available with this paper size."	A paper size not available in Duplex mode has been selected.	Select an appropriate paper size. For details about paper sizes, see "Specifications for the Main Unit", Maintenance and Specifications.
"Exceeded the maximum number of sheets that can be used. Copying will be stopped."	The number of pages the user is permitted to copy has been exceeded.	For details about how to check the number of copies available per user, see Security Guide.
"File being stored exceeded max. number of pages per file. Copying will be stopped."	The scanned originals have too many pages to store as one document.	Press [Exit], and then store again with an appropriate number of pages.

Messages	Causes	Solutions
"Magazine or Booklet mode is not available due to mixed image mode."	You selected the "Magazine" or "Booklet" function for originals scanned using different functions, such as copy and printer.	Make sure originals for the "Magazine" or "Booklet" function are scanned using the same function.
"Maximum number of sets is n." (A figure is placed at n.)	The number of copies exceeds the maximum copy quantity.	You can change the maximum copy quantity from [Max. Copy Quantity] in [General Features] under [Copier / Document Server Features]. For details about Max. Copy Quantity, see "General Features", Copy/ Document Server.
"Memory is full. nn originals have been scanned. Press [Print] to copy scanned originals. Do not remove remaining originals." ("n" in the message represents a changeable number.)	The scanned originals exceed the number of pages that can be stored in memory.	Press [Print] to copy scanned originals and cancel the scanning data. Press [Clear Memory] to cancel the scanning data and not copy.
"Press [Continue] to scan and copy remaining originals."	The machine checked if the remaining originals should be copied, after the scanned originals were printed.	Remove all copies, and then press [Continue] to continue copying. Press [Stop] to stop copying.
"Rotate Sort is not available with this paper size."	A size of paper for which Rotate Sort is not available is selected.	Select an appropriate paper size. For details about paper sizes, see "Sort", Copy/ Document Server.
"Stapling capacity exceeded."	The number of sheets per set is over the staple capacity.	Check the number of sheets to be stapled. For details about the stapler capacity, see "Specifications for Internal Finisher SR3130" and "Specifications for Internal Finisher SR3180", Maintenance and Specifications.

Messages	Causes	Solutions
"The selected folder is locked. Please contact the file administrator."	An attempt was made to edit or use a locked folder.	For details about locked folders, see Security Guide.

Note

- If you set [Memory Full Auto Scan Restart] in [Input / Output] of User Tools to [On], even if the memory becomes full, the memory overflow message will not be displayed. The machine will make copies of the scanned originals first, and then automatically proceed to scan and to copy the remaining originals. In this case, the resulting sorted pages will not be sequential. For details about Memory Full Auto Scan Restart, see "Input / Output", Copy/ Document Server.

Messages Displayed When Using the Facsimile Function

Messages	Causes	Solutions
"Cannot find the specified path. Please check the settings."	The name of the computer or folder entered as the destination is wrong.	Check that the computer name and the folder name for the destination are correct.
"Error occurred, and transmission was cancelled."	<ul style="list-style-type: none"> • Original jammed during Immediate Transmission. • A problem occurred in the machine, or noise occurred on the telephone line. 	Press [Exit], and then send the documents again.
"Functional problem occurred. Stopped processing."	The power was turned off while the machine was receiving a document by Internet Fax.	Even if you turn on the power immediately, depending on the mail server, the machine might not be able to resume reception of the Internet Fax if the timeout period has not expired. Wait until the mail server's timeout period has expired, and then resume reception of the Internet Fax. For details about reception of the Internet Fax, contact your administrator.
"Functional problems with facsimile. Data will be initialized."	There is a problem with the fax.	Record the code number shown on the screen, and then contact your service representative. Other functions can be used.
"Memory is full. Cannot scan more. Transmission will be stopped."	The memory is full.	<p>If you press [Exit], the machine returns to standby mode and starts transmitting the stored pages.</p> <p>Check the pages that have not been sent using the Communication Result Report, and then resend those pages.</p>
"Put original back, check it and press the Start key."	Original jammed during Memory Transmission.	Press [Exit], and then send the documents again.

Messages	Causes	Solutions
"Some page(s) are near blank."	The first page of the document is almost blank.	The original's blank side might have been scanned. Be sure to place your originals correctly. For details about determining the cause of blank pages, see "Detecting Blank Pages", Fax.

↓ Note

- Settings that can be confirmed in System Settings or Facsimile Features on the control panel can also be confirmed from Web Image Monitor. For details about how to confirm the settings from Web Image Monitor, see Web Image Monitor Help.
- If the paper tray runs out of paper, "There is no paper. Load paper." appears on the screen, asking you to add paper. If there is paper left in the other trays, you can receive documents as usual, even if the message appears on the screen. You can turn this function on or off with "Parameter Settings". For details about how to do this, see "Parameter Settings", Fax.

When There Is a Problem Specifying the Network Settings

Messages	Causes	Solutions
"Check whether there are any network problems." [13-10]	The alias telephone number you entered is already registered on the gatekeeper by another device.	<ul style="list-style-type: none"> • Check that the correct alias phone number is listed in [H.323 Settings] of [Facsimile Features]. For details about H.323 Settings, see "Initial Settings", Fax. • For details about network problems, contact your administrator.
"Check whether there are any network problems." [13-11]	Cannot access gatekeeper.	<ul style="list-style-type: none"> • Check that the correct gatekeeper address is listed in [H.323 Settings] of [Facsimile Features]. For details about H.323 Settings, see "Initial Settings", Fax. • For details about network problems, contact your administrator.

Messages	Causes	Solutions
"Check whether there are any network problems." [13-17]	Registering of user name is rejected by SIP server.	<ul style="list-style-type: none"> • Correct that the correct SIP Server IP Address and SIP User Name are listed in [SIP Settings] of [Facsimile Features]. For details about SIP Settings, see "Initial Settings", Fax. • For details about network problems, contact your administrator.
"Check whether there are any network problems." [13-18]	Cannot access SIP server.	<ul style="list-style-type: none"> • Check that the correct SIP Server IP Address is listed in [SIP Settings] of [Facsimile Features]. For details about SIP Settings, see "Initial Settings", Fax. • For details about network problems, contact your administrator.
"Check whether there are any network problems." [13-24]	The password registered for the SIP server is not the same as the password registered for this machine.	For details about network problems, contact your administrator.
"Check whether there are any network problems." [13-25]	In [Effective Protocol], the IP address is not enabled, or an incorrect IP address has been registered.	<ul style="list-style-type: none"> • Check that IPv4 in [Effective Protocol] is set to "Active" in [System Settings]. For details about effective protocol, see "Interface Settings", Connecting the Machine/ System Settings. • Check that the correct IPv4 address is specified for the machine in [System Settings]. For details about IPv4 address, see "Interface Settings", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.

Messages	Causes	Solutions
<p>"Check whether there are any network problems." [13-26]</p>	<p>The "Effective Protocol" and "SIP Server IP Address" settings are different, or an incorrect IP address has been registered.</p>	<ul style="list-style-type: none"> • Check that the correct IP address is specified for the machine in [System Settings]. For details about IP address, see "Interface Settings", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.
<p>"Check whether there are any network problems." [14-01]</p>	<p>The DNS server, SMTP server, or folder specified for transfer to was not found, or the destination for Internet Fax around (not through) the SMTP server could not be found.</p>	<ul style="list-style-type: none"> • Check that the following settings in [System Settings] are listed correctly. <ul style="list-style-type: none"> • DNS server • Server name and IP address for the SMTP Server <p>For details about these settings, see "Interface Settings" or "File Transfer", Connecting the Machine/ System Settings.</p> • Check that the folder for transfer is correctly specified. • Check that the computer in which the folder for transfer is specified is correctly operated. • Check that the LAN cable is correctly connected to the machine. • For details about the network connection of the destination, contact the administrator at the destination. • For details about network problems, contact your administrator.

Messages	Causes	Solutions
<p>"Check whether there are any network problems." [14-09]</p>	<p>E-mail transmission was refused by SMTP authentication, POP before SMTP authentication, or login authentication of the computer in which the folder for transfer is specified.</p>	<ul style="list-style-type: none"> • Check that User Name and Password for the following settings in [System Settings] are listed correctly. <ul style="list-style-type: none"> • SMTP Authentication • POP before SMTP • Fax E-mail Account <p>For details about these settings, see "File Transfer", Connecting the Machine/ System Settings.</p> <ul style="list-style-type: none"> • Check that the user ID and password for the computer with the folder for forwarding are correctly specified. • Check that the folder for forwarding is correctly specified. • Confirm that the computer with the folder for forwarding is properly working. • For details about network problems, contact your administrator.
<p>"Check whether there are any network problems." [14-33]</p>	<p>E-mail addresses for the machine and the administrator are not registered.</p>	<ul style="list-style-type: none"> • Check that the correct E-mail Address is listed in [Fax E-mail Account] of [System Settings]. For details about Fax E-mail Account, see "File Transfer", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.

Messages	Causes	Solutions
"Check whether there are any network problems." [15-01]	No POP3/IMAP4 server address is registered.	<ul style="list-style-type: none"> • Check that the correct Server Name or Server Address is listed in [POP3 / IMAP4 Settings] of [System Settings]. For details about POP3 / IMAP4 Settings, see "File Transfer", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.
"Check whether there are any network problems." [15-02]	Cannot log in to the POP3/IMAP4 server.	<ul style="list-style-type: none"> • Check that the correct User Name and Password are listed in [Fax E-mail Account] of [System Settings]. For details about Fax E-mail Account, see "File Transfer", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.
"Check whether there are any network problems." [15-03]	No machine e-mail address is programmed.	<ul style="list-style-type: none"> • Check that the correct machine e-mail address is specified in [System Settings]. For details about settings of e-mail address, see "File Transfer", Connecting the Machine/ System Settings. • For details about network problems, contact your administrator.

Messages	Causes	Solutions
<p>"Check whether there are any network problems." [15-11]</p>	<p>Cannot find the DNS server or POP3/IMAP4 server.</p>	<ul style="list-style-type: none"> • Check that the following settings in [System Settings] are listed correctly. <ul style="list-style-type: none"> • IP address of the DNS Server • the server name or IP address of the POP3/IMAP4 server • the port number of the POP3/IMAP4 server • Reception Protocol <p>For details about these settings, see "Interface Settings" or "File Transfer", Connecting the Machine/ System Settings.</p> • Check that the LAN cable is correctly connected to the machine. • For details about network problems, contact your administrator.
<p>"Check whether there are any network problems." [15-12]</p>	<p>Cannot log in to the POP3/IMAP4 server.</p>	<ul style="list-style-type: none"> • Check that the following settings in [System Settings] are listed correctly. <ul style="list-style-type: none"> • the user name and password for [Fax E-mail Account] • the user name and password for POP before SMTP authentication <p>For details about these settings, see "File Transfer", Connecting the Machine/ System Settings.</p> • For details about network problems, contact your administrator.

↓ Note

- Settings that can be confirmed in System Settings or Facsimile Features on the control panel can also be confirmed from Web Image Monitor. For details about how to confirm the settings from Web Image Monitor, see Web Image Monitor Help.
- If the paper tray runs out of paper, "There is no paper. Load paper." appears on the screen, asking you to add paper. If there is paper left in the other trays, you can receive documents as usual, even if the message appears on the screen. You can turn this function on or off with "Parameter Settings". For details about how to do this, see "Parameter Settings", Fax.
- If "Check whether there are any network problems." appears, the machine is not correctly connected to the network or the settings of the machine are not correct. If you do not need to connect to a network, you can specify the setting so this message is not displayed, and then the [Check Status] key no longer lights. For details about how to do this, see "Parameter Settings", Fax. If you reconnect the machine to the network, be sure to set "Display" by configuring the appropriate User Parameter.

When the Remote Fax Function Cannot Be Used

Messages	Causes	Solutions
"Authentication with remote machine failed. Check remote machine's auth. settings."	User authentication on the main machine has failed.	For details about user authentication, see Security Guide.
"Authentication with remote machine failed. Check remote machine's auth. settings."	User Code Authentication is set on the device connected via the remote fax function.	The remote fax function does not support User Code Authentication. Disable the User Code Authentication on the main machine.
"Authentication with remote machine failed. Check remote machine's auth. settings."	The user does not have permission to use the function on the main machine.	For details about how to set permissions, see Security Guide.

Messages	Causes	Solutions
"Check whether there are any network problems." [16-00]	<ul style="list-style-type: none"> • An IP address has not been registered for the main machine. • A network is not connected properly. 	<ul style="list-style-type: none"> • Check that the correct IP address is specified for the machine in [System Settings]. For details about the IP address of the main machine, contact your administrator. • For details about network problems, contact your administrator.
"Connection with the remote machine has failed. Check the remote machine status."	A network error occurred while using the remote fax function.	<ul style="list-style-type: none"> • Check that the main machine supports the remote fax function. • Check that the main machine is working normally. • Check that the correct IP address or host name is set for the main machine in [System Settings]. For details about these settings, contact your administrator. • Check that the LAN cable is correctly connected to the machine. • For details about network problems, contact your administrator.
"Connection with the remote machine has failed. Check the remote machine status."	The main machine's power is off.	Turn on the main machine's power.
"Connection with the remote machine has failed. Check the remote machine status."	A timeout error occurred while an attempt was made to connect the device via remote fax function.	<ul style="list-style-type: none"> • Check that the LAN cable is correctly connected to the machine. • Check that the main machine is working correctly. • For details about connection with main machine, see "Sending/Receiving Documents Using a Remote Machine (Remote Fax)", Fax.

Messages	Causes	Solutions
"Connection with the remote machine has failed. There is a problem with the remote machine structure. Contact the administrator."	The settings or machine configuration for using the remote fax function to connect to the main machine are incorrect.	For details about the settings and machine configuration for using the remote fax function to connect to a main machine, contact your administrator.
"Transfer error has occurred. Check the status of the remote machine."	A network error occurred during transfer.	<ul style="list-style-type: none"> • Check that the correct IP address or host name is set for the main machine in [System Settings]. For details about these settings, contact your administrator. • Check that the main machine is working correctly. • Check that the LAN cable is correctly connected to the machine. • For details about transmission, contact your administrator.
"The HDD of the remote machine is full."	The hard disk became full after using the remote fax function to scan an original.	Delete unnecessary files.

Messages Displayed When Using the Printer Function

This section describes the principal messages that appear on the display panel, error logs or reports. If other messages appear, follow their instructions.

Messages Displayed on the Control Panel When Using the Printer Function

★ Important

- Before turning off the power, see page 63 "Turning On/Off the Power".

Messages	Causes	Solutions
"Hardware Problem: Ethernet"	An error has occurred in the Ethernet interface.	Turn off the power, and then back on again. If the message appears again, contact your service representative.
"Hardware Problem: HDD"	An error has occurred in the hard disk.	Turn off the power, and then back on again. If the message appears again, contact your service representative.
"Hardware Problem: USB"	An error has occurred in the USB interface.	Turn off the power, and then back on again. If the message appears again, contact your service representative.
"Hardware Problem: Wireless Card" (A "wireless LAN board" or "Bluetooth interface unit" is referred to as a "wireless card".)	The wireless LAN board can be accessed, but an error was detected.	Turn off the power, and then confirm the wireless LAN board is inserted correctly. After confirmation, turn on the power again. If the message appears again, contact your service representative.
"Hardware Problem: Wireless Card" (A "wireless LAN board" or "Bluetooth interface unit" is referred to as a "wireless card".)	<ul style="list-style-type: none"> • The Bluetooth interface unit was connected while the machine was turned on. • The Bluetooth interface unit was removed while the machine was turned on. 	Turn off the power, and then confirm the Bluetooth interface unit is inserted correctly. After confirmation, turn on the power again. If the message appears again, contact your service representative.

Messages	Causes	Solutions
"Load following paper in n. To cancel job, press [Job Reset]." (A figure is placed at n.)	The printer driver settings are incorrect or the tray does not contain paper of the size selected in the printer driver.	Check that the printer driver settings are correct, and then load paper of the size selected in the printer driver into the input tray. For details about how to change the paper size, see "Changing the Paper Size", Paper Specifications and Adding Paper.
"Paper in staple tray. Open cover and remove paper."	If printing is stopped before it is finished, paper may remain in the finisher.	Remove the paper remaining in the finisher.
"Paper size and type are mismatched. Select another tray from the following and press [Continue]. To cancel job, press [Job Reset]. Paper size and type can also be changed in User Tools."	The printer driver settings are incorrect or the tray does not contain paper of the size or type selected in the printer driver.	<ul style="list-style-type: none"> • Check that the printer driver settings are correct, and then load paper of the size selected in the printer driver into the input tray. For details about how to change the paper size, see "Changing the Paper Size", Paper Specifications and Adding Paper. • Select the tray manually to continue printing, or cancel a print job. For details about how to select the tray manually, or cancel a print job, see "If an Error Occurs with the Specified Paper Size and Type", Print.
"Paper size of n is mismatched. Select another tray from the following and press [Continue]. Paper type can also be changed in User Tools." (A tray name is placed at n.)	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.
"Parallel I/F board has a problem."	An error has occurred in the IEEE 1284 interface board.	Turn off the power, and then back on again. If the message appears again, contact your service representative.

Messages	Causes	Solutions
"Printer font error."	An error has occurred in the font settings.	Contact your service representative.
"Problems with the wireless card. Please call service." (A "wireless LAN board" or "Bluetooth unit" is referred to as a "wireless card".)	The machine has detected a Bluetooth failure, or it could not detect a Bluetooth unit. It may be incorrectly installed.	Check that the Bluetooth unit is installed properly, or contact your service representative.
"Cannot print because both the main and designation (chapter) sheets are set to the same paper tray. Press [Job Reset] to cancel the job. To print the job again specify different trays."	The tray selected for other pages is the same as the one for slip sheets.	Reset the job. Be sure the tray you select for slip sheets is not providing paper for other pages.

When using direct print from a memory storage device

Messages	Causes	Solutions
"Exceeded the limit value for total data size of the selected files. Cannot select more files."	<ul style="list-style-type: none"> The size of the selected file exceeds 1 GB. The total size of the selected files exceeds 1 GB. 	<p>Files or groups of files larger than 1 GB cannot be printed.</p> <ul style="list-style-type: none"> When the total size of the multiple files that are selected exceeds 1 GB, select files separately. When the size of the selected file exceeds 1 GB, print from a memory storage device using a function other than the Direct printing function. <p>You cannot select files of different formats at the same time.</p>

Messages	Causes	Solutions
"Unable to access the specified memory storage device."	<ul style="list-style-type: none"> An error occurred when the machine accessed the memory storage device or a file stored on the memory storage device. An error occurred when the user used the Direct printing function to print from a memory storage device. 	Save the file to a different memory storage device, and then try to print again.

Messages Printed on the Error Logs or Reports When Using the Printer Function

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

When print jobs are canceled

Messages	Causes	Solutions
"91: Error"	Printing was canceled by the auto job cancel function due to a command error.	Check that the data is valid.
"An error occurred while processing an Unauthorized Copy Prevention job. The job was cancelled."	You tried to store a file in the Document Server when the [Unauthorized Copy Prevention] was specified.	On the printer driver, select a job type other than [Document Server] in "Job Type:" or deselect [Unauthorized Copy Prevention].
"An error occurred while processing an Unauthorized Copy Prevention job. The job was cancelled."	The [Enter User Text:] field on the [Unauthorized Copy Prevention for Pattern Details] screen is blank.	On the printer driver's [Detailed Settings] tab, click [Effects] in "Menu:". Select [Unauthorized Copy Prevention], and then click [Details] to display [Unauthorized Copy Prevention for Pattern Details]. Enter text in [Enter User Text:].

Messages	Causes	Solutions
"An error occurred while processing an Unauthorized Copy Prevention job. The job was cancelled."	The resolution is set to a value less than 600 dpi when [Unauthorized Copy Prevention] is specified.	On the printer driver, set the resolution to 600 dpi or higher, or deselect [Unauthorized Copy Prevention].
"Collate has been cancelled."	Collate was canceled.	Turn off the power, and then back on again. If the message appears again, contact your service representative.
"Exceeded the maximum unit count for Print Volume Use. The job has been cancelled."	The number of pages the user is permitted to print has been exceeded.	For details about print volume use limitation, see Security Guide.
"Receiving data failed."	Data reception was aborted.	Resend the data.
"Sending data failed."	The machine received a command to stop transmission from the printer driver.	Check if the computer is working correctly.
"The selected paper size is not supported. This job has been cancelled."	Job reset is automatically performed if the specified paper size is incorrect.	Specify the correct paper size, and then print the file again.
"The selected paper type is not supported. This job has been cancelled."	Job reset is automatically performed if the specified paper type is incorrect.	Specify the correct paper type, and then print the file again.

When there is a problem with the print settings

Messages	Causes	Solutions
"Classification Code is incorrect."	The classification code has not been entered, or the classification code has been entered incorrectly.	Enter the correct classification code.

Messages	Causes	Solutions
"Classification Code is incorrect."	The classification code is not supported with the printer driver.	Select [Optional] for classification code. For details about how to specify classification code settings, see "Configuring Classification Codes", Print.
"Duplex has been cancelled."	Duplex printing was canceled.	<ul style="list-style-type: none"> • Select an appropriate paper size for the duplex function. For details about paper, see "Specifications for the Main Unit", Maintenance and Specifications. • Change the setting for "Apply Duplex" in [System Settings] to enable duplex printing for the paper tray. For details about setting "Apply Duplex", see "Tray Paper Settings", Connecting the Machine/ System Settings.
"Exceeded max. pages. Collate is incomplete."	The number of pages exceeds the maximum number of sheets that you can use Collate with.	Reduce the number of pages to print.
"Output tray has been changed."	The output tray was changed because the paper size of the specified output tray is limited.	Specify the proper output tray.
"Print overrun."	Images were discarded while printing.	<p>PCL 6</p> <p>Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help.</p> <p>PostScript 3</p> <p>Select a lower resolution on the printer driver. For details about how to change the resolution setting, see the printer driver Help.</p>

Messages	Causes	Solutions
"Punch has been cancelled."	Punch printing was canceled.	Check the paper orientation, print orientation, and then punch position. Certain settings can produce print results that might not be as expected.
"Staple has been cancelled."	Stapling printing was canceled.	Check the paper orientation, paper quantity, print orientation, and staple position. Certain settings can produce print results that might not be as expected.

When documents cannot be stored in the Document Server

Messages	Causes	Solutions
"Cannot store data of this size."	The paper size exceeded the capacity of the Document Server.	Reduce the paper size of the file that you want to send to a size that the Document Server can store. Custom size files can be sent but not stored afterward.
"Document Server is not available to use. Cannot store."	You cannot use the Document Server function.	For details about using Document Server function, contact your administrator. For details about how to set permissions, see Security Guide.
"Exceeded max. capacity of Document Server. Cannot store."	The hard disk became full after a file was stored.	Delete some of the files stored in the Document Server or reduce the size that you want to send.
"Exceeded max. number of files of Document Server. Cannot store."	The maximum file capacity of the Document Server was exceeded.	Delete some of the files stored in the Document Server.

Messages	Causes	Solutions
"Exceeded max. number of files. (Auto)"	While using the error job store function to store Normal Print jobs as Hold Print files, the maximum file capacity for file storage or Hold Print file management (automatic) was exceeded.	Delete Hold Print files (automatic) or unneeded files stored in the machine.
"Exceeded max. number of pages of Document Server. Cannot store."	The maximum page capacity of the Document Server was exceeded.	Delete some of the files stored in the Document Server or reduce the number of pages that you want to send.
"Exceeded max. number of pages. (Auto)"	While using the error job store function to store Normal Print jobs as Hold Print files, the maximum page capacity was exceeded.	Delete unneeded files stored in the machine. Reduce the number of pages to print.
"The print job has been cancelled because capture file(s) could not be stored: Exceeded max. memory."	The hard disk became full after a file was stored.	Delete the files stored in the Document Server or reduce the file size to be sent.
"The print job has been cancelled because capture file(s) could not be stored: Exceeded max. number of files."	The maximum file capacity of the Document Server was exceeded.	Delete the files stored in the Document Server.
"The print job has been cancelled because capture file(s) could not be stored: Exceeded max. number of pages per file."	The maximum page capacity of the Document Server was exceeded.	Delete some of the files stored in the Document Server or reduce the number of pages that you want to send.
"The specified folder in Document Server is locked. Cannot store."	The specified folder is locked.	Unlock the folder or specify another folder number that can be used. For details about locked folders, see Security Guide.

When there is not enough free hard disk space

Messages	Causes	Solutions
"HDD is full."	When printing with the PostScript 3 printer driver, the hard disk capacity for fonts and forms has been exceeded.	Delete unneeded forms or fonts registered in the machine.
"HDD is full."	The hard disk became full while printing a Sample Print, Locked Print, Hold Print, or Stored Print file.	Delete unneeded files stored in the machine. Alternatively, reduce the data size of the Sample Print, Locked Print, Hold Print, or Stored Print file.
"HDD is full. (Auto)"	The hard disk became full while using the error job store function to store Normal Print jobs as Hold Print files.	Delete unneeded files stored in the machine. Alternatively, reduce the data size of the Temporary Print file and/or the Stored Print file.

When there is not enough memory

Messages	Causes	Solutions
"84: Error"	There is no work area available for image processing.	Decrease the number of files sent to the machine.
"92: Error"	Printing was canceled because [Job Reset] or the [Stop] key was selected on the machine's control panel.	Perform the print operation again if necessary.

When there is a problem with a parameter

Messages	Causes	Solutions
"86: Error"	Parameters of the control code are invalid.	Check the print settings.

When the user lacks privileges to perform an operation

Messages	Causes	Solutions
"No response from the server. Authentication has failed."	A timeout occurred while connecting to the server for LDAP authentication or Windows Authentication.	Check the status of the server.
"Printing privileges have not been set for this document."	The PDF document you have tried to print has no privileges to print.	Contact the owner of the document.
"You do not have a privilege to use this function. This job has been cancelled."	The entered login user name or login password is not correct.	Check that the user name and password are correct.
"You do not have a privilege to use this function. This job has been cancelled."	The logged in user is not allowed to use the selected function.	For details about how to set permissions, see Security Guide.
"You do not have a privilege to use this function. This operation has been cancelled."	The logged in user does not have the privileges to register programs or change the paper tray settings.	For details about how to set permissions, see Security Guide.

When a user cannot be registered

Messages	Causes	Solutions
"Auto-registration of user information has failed."	Automatic registration of information for LDAP Authentication or Windows Authentication failed because the Address Book is full.	For details about automatic registration of user information, see Security Guide.

Messages	Causes	Solutions
"Information for user authentication is already registered for another user."	The user name for LDAP or Integration Server authentication was already registered in a different server with a different ID, and a duplication of the user name occurred due to a switching of domains (servers), etc..	For details about user authentication, see Security Guide.

When other errors occur

Messages	Causes	Solutions
"85: Error"	The specified graphics library is unavailable.	Check that the data is valid.
"98: Error"	The machine could not access Hard disk correctly.	Turn off the power, and then back on again. If the message appears frequently, contact your service representative.
"99: Error"	This data cannot be printed. The specified data is either corrupt or it cannot be printed from a memory storage device using the Direct printing function.	Check that the data is valid. For details about the kinds of data that can be printed from a memory storage device using the Direct printing function, see "Direct Printing from a Memory Storage Device", Print.
"Command Error"	An RPCS command error occurred.	Check using the following procedure: <ul style="list-style-type: none"> • Check if the communication between the computer and the machine is working correctly. • Check if the correct printer driver is being used. • Check if the machine's memory size is set correctly in the printer driver. • Check that the printer driver is the most up-to-date version available.

Messages	Causes	Solutions
"Compressed Data Error."	The printer detected corrupt compressed data.	<ul style="list-style-type: none"> • Check the connection between the computer and the printer. • Check that the program you used to compress the data is functioning correctly.
"Data storage error."	You tried to print a Sample Print, Locked Print, Hold Print, or Stored Print file, or to store a file in the Document Server when the hard disk was malfunctioning.	Contact your service representative.
"Error has occurred."	A syntax error, etc., occurred.	Check that the PDF file is valid.
"Exceeded max. number of files to print for temporary / stored jobs."	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.
"Exceeded max. number of pages to print for temporary / stored jobs."	While printing a Sample Print, Locked Print, Hold Print, or Stored Print file, the maximum page capacity was exceeded.	<p>Delete unneeded files stored in the machine.</p> <p>Reduce the number of pages to print.</p>
"Failed to obtain file system."	PDF direct printing could not be performed because the file system could not be obtained.	Turn off the power, and then back on again. If the message appears again, contact your service representative.
"File system is full."	PDF file does not print out 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.

Messages	Causes	Solutions
"I/O buffer overflow."	An input buffer overflow occurred.	<ul style="list-style-type: none"> In [Printer Features], under [Host Interface], select [I/O Buffer], and then set the maximum buffer size to a larger value. Reduce the number of files being sent to the machine.
"Insufficient Memory"	A memory allocation error occurred.	<p>PCL 6</p> <p>On the printer driver's [Detailed Settings] tab, click [Print 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.</p>
"Memory Retrieval Error"	A memory allocation error occurred.	Turn off the power, and then back on again. If the message appears again, replace the RAM. For details about replacing the RAM, contact your service representative.

If printing does not start, contact your service representative.

Note

- The contents of errors may be printed on the Configuration Page. Check the Configuration Page in conjunction with the error log. For details about how to print the Configuration Page, see "List / Test Print", Print.

Messages Displayed When Using the Scanner Function

Messages Displayed on the Control Panel When Using the Scanner Function

This section describes likely causes of and possible solutions for the error messages that appear on the control panel. If a message not described here appears, act according to the message.

Messages	Causes	Solutions
"Cannot find the specified path. Please check the settings."	The destination computer name or folder name is invalid.	Check whether the computer name and the folder name for the destination are correct.
"Cannot find the specified path. Please check the settings."	An antivirus program or a firewall is preventing the machine connecting to your computer.	<ul style="list-style-type: none"> • Antivirus programs and firewalls can prevent client computers from establishing connection with this machine. • If you are using anti-virus software, add the program to the exclusion list in the application settings. For details about how to add programs to the exclusion list, see the anti-virus software Help. • To prevent a firewall blocking the connection, register the machine's IP address in the firewall's IP address exclusion settings. For details about the procedure for excluding an IP address, see your operating system's Help.
"Entered user code is not correct. Please re-enter."	You have entered an incorrect user code.	Check the authentication settings, and then enter a correct user code.
"Exceeded max. number of alphanumeric characters for the path."	The maximum number of specifiable alphanumeric characters in a path has been exceeded.	The maximum number of characters which can be entered for the path is 256. Check the number of characters you entered, and then enter the path again.

Messages	Causes	Solutions
"Exceeded max. number of alphanumeric characters."	The maximum enterable number of alphanumeric characters has been exceeded.	Check the maximum number of characters which can be entered, and then enter it again. For details about the maximum enterable number of characters, see "Values of Various Set Items for Transmission/Storage/Delivery Function", Scan.
"Programmed. Cannot program the destination(s) that is not programmed in the address book."	The destinations selected while registering to the program contain a folder destination for which one of the following destinations is set: manually entered destination, delivery server destination, WSD destination, or DSM destination	WSD destinations and DSM destinations cannot be registered to the program because they cannot be registered in the address book. For manually entered and delivery server destinations, register the destinations in the address book, and then try to register them to the program again.
"Scanner journal is full. Please check Scanner Features."	[Print & Delete Scanner Journal] in [Scanner Features] is set to [Do not Print: Disable Send], and Scanner Journal is full.	Print or delete Scanner Journal. For details about Scanner Features, see "General Settings", Scan.
"The entered file name contains invalid character(s). Enter the file name again using any of the following 1 byte characters. " 0 to 9 ", " A to Z ", " a to z ", " . - _ ""	The file name contains a character that cannot be used.	Check the file name set at the time of scanning. For details about characters that can be used in file names, see "Specifying the File Name", Scan.
"The entered file name contains invalid character(s). Enter the file name again using any of the following 1 byte characters. " 0 to 9 ", " A to Z ", " a to z ", " . - _ ""	The file name contains a character that cannot be used.	Check the file name specified at the time of scanning. The file name specified in the Sending Scan Files to Folders function cannot contain the following characters: \ / : * ? " < > The file name cannot start or end with a period ".".

Messages	Causes	Solutions
"The program is recalled. Cannot recall the destination(s) for which access privileges are required."	The currently logged-in user does not have permission to view the destination that was registered in the program.	For details about how to set permissions, see Security Guide.
"The program is recalled. Cannot recall the destination(s) that is deleted from the address book."	The destination stored in the program could not be called because it was deleted from the address book.	Enter the destination directly to send data separately.
"The program is recalled. Cannot recall the folder destination(s) with protection code(s)."	The folder destinations for which the protection code was set were registered in the program.	A destination for which the protection code is set cannot be called by the program. Cancel the protection code setting or send scanned files to the destination separately.

When documents cannot be scanned properly

Messages	Causes	Solutions
"All the pages are detected as blank. No file was created."	No PDF file was created because all the pages of the scanned original were detected as blank when [On] is specified for [Delete Blank Page] in [OCR Settings].	Check whether the original is set upside down. Change [OCR Scanned PDF: Blank Page Sensitivity] in [Scanner Features] to "Sensitivity Level 1".
"Check original's orientation."	Documents may sometimes not be scanned depending on a combination of items such as the specified scaling factor and document size.	Change the orientation of the original, and then try to scan the original again.

Messages	Causes	Solutions
"Exceeded max. data capacity." "Check scanning resolution, then press Start key again."	The scanned data exceeded maximum data capacity.	Specify the scan size and resolution again. Note that it may not be possible to scan very large originals at a high resolution. For details about the settings for the scanner function, see "Relationship between Resolution and Scan Size", Scan.
"Exceeded max. data capacity." "Check the scanning resolution, then reset n original(s)." ("n" in the message represents a changeable number.)	The scanned original exceeded maximum data capacity.	Specify the scan size and resolution again. Note that it may not be possible to scan very large originals at a high resolution. For details about the settings for the scanner function, see "Relationship between Resolution and Scan Size", Scan.
"Exceeded max. data capacity." "Check the resolution and the ratio and then press the Start key again."	The data being scanned is too large for the scale ratio specified in [Specify Size].	Reduce the resolution or [Specify Size] value, and then try to scan the original again.
"Exceeded max. number of files which can be used in Document Server at the same time."	The maximum number of files that can be stored in the Document Server has been exceeded.	Check the files stored by the other functions, and then delete unneeded files. For details about how to delete files, see "Deleting Stored Documents", Copy/ Document Server.
"Not all of the image will be scanned."	If the scaling factor specified in "Specify Reproduction Ratio" is too large, part of the image may be lost.	Reduce the scaling factor in "Specify Reproduction Ratio", and then try to scan the original again. If displaying the entire image is not necessary, press the [Start] key to start scanning with the current scaling factor.

Messages	Causes	Solutions
"Not all of the image will be scanned."	Using "Specify Reproduction Ratio" to scale down a large document may cause part of the image to be lost.	Specify a large size in [Specify Size], and then try to scan the original again. If displaying the entire image is not necessary, press the [Start] key to start scanning with the current scaling factor.
"The size of the scanned data is too small." "Check the resolution and the ratio and then press the Start key again."	The data being scanned is too small for the scale ratio specified in [Specify Size].	Specify a higher resolution or a large size in [Specify Size], and then try to scan the original again.

When documents cannot be scanned because the memory is full

Messages	Causes	Solutions
"Memory is full. Cannot scan. The scanned data will be deleted."	Because of insufficient hard disk space, the first page could not be scanned.	Try one of the following measures: <ul style="list-style-type: none"> • Wait for a while, and then retry the scan operation. • Reduce the scan area or scanning resolution. For details about changing scan area and scanning resolution, see "Scan Settings" of Various Scan Settings, Scan. • Delete unneeded stored files. For details about how to delete stored files, see "Deleting a Stored File", Scan.
"Memory is full. Do you want to store scanned file?"	Because there is not enough free hard disk space in the machine for storing in the Document Server, only some of the pages could be scanned.	Specify whether to use the data or not.

Messages	Causes	Solutions
"Memory is full. Scanning has been cancelled. Press [Send] to send the scanned data, or press [Cancel] to delete."	Because there is not enough free hard disk space in the machine for delivering or sending by e-mail while storing in the Document Server, only some of the pages could be scanned.	Specify whether to use the data or not.

When data transmission fails

Messages	Causes	Solutions
"Authentication with the destination has failed. Check settings. To check the current status, press [Scanned Files Status]."	The entered user name or password was invalid.	<ul style="list-style-type: none"> • Check that the user name and password are correct. • Check that the ID and password for the destination folder are correct. • A password of 128 or more characters may not be recognized.
"Exceeded max. E-mail size. Sending E-mail has been cancelled. Check [Max. E-mail Size] in Scanner Features."	The file size per page has reached the maximum e-mail size specified in [Scanner Features].	<p>Change the scanner features settings as follows:</p> <ul style="list-style-type: none"> • Increase the e-mail size limit in [Max. E-mail Size]. • Change the [Divide & Send E-mail] setting to [Yes (per Page)] or [Yes (per Max. Size)]. For details about these settings, see "Send Settings", Scan.
"Sending the data has failed. The data will be resent later."	A network error has occurred and a file was not sent correctly.	Wait until sending is retried automatically after the preset interval. If sending fails again, contact your administrator.

Messages	Causes	Solutions
"Transmission has failed. Insufficient memory in the destination hard disk. To check the current status, press [Scanned Files Status]."	Transmission has failed. There was not enough free space on the hard disk of the SMTP server, FTP server, or client computer at the destination.	Allocate sufficient space.
"Transmission has failed. To check the current status, press [Scanned Files Status]."	While a file was being sent, a network error occurred and the file could not be sent correctly.	If the same message appears again after scanning again, the cause could be a mixed network, or else network settings were changed during WSD scanner transmission. For details about network error, contact your administrator.

When data cannot be sent because a currently used file is selected

Messages	Causes	Solutions
"Selected file is currently in use. File name cannot be changed."	You cannot change the name of a file whose status is "Waiting..."	Cancel transmission ("Waiting..." status cleared), and then change the file name.
"Selected file is currently in use. Password cannot be changed."	You cannot change the password of a file whose status is "Waiting..."	Cancel transmission ("Waiting..." status cleared), and then change the password.
"Selected file is currently in use. User name cannot be changed."	You cannot change the sender's name whose status is "Waiting..."	Cancel transmission ("Waiting..." status cleared), and then change the user name.
"Some of selected files are currently in use. They could not be deleted."	You cannot delete a file which is waiting to be transmitted ("Waiting..." status displayed).	Cancel transmission ("Waiting..." status cleared), and then delete the file.

When data cannot be sent because there are too many documents or pages

Messages	Causes	Solutions
"Exceeded max. number of pages per file. Do you want to store the scanned pages as 1 file?"	The file being stored has exceeded the maximum number of pages for one file.	Specify whether to store the data or not. Scan the pages that were not scanned, and then store them as a new file. For details about storing files, see "Storing and Saving the Scanned Documents", Scan.
"Exceeded max. number of stored files. Cannot send the scanned data as capturing files is unavailable."	Too many files are waiting to be delivered.	Try again after they have been delivered.
"Exceeded max. page capacity per file. Press [Send] to send the scanned data, or press [Cancel] to delete."	The number of scanned pages exceeded the maximum page capacity.	Select whether to send the data that has already been scanned.
"Exceeded maximum number of file to store. Delete all unnecessary files."	Too many files are waiting to be delivered.	Try again after they have been delivered.

When the WSD scanner function cannot be used

Messages	Causes	Solutions
"Cannot communicate with PC. Contact the administrator."	WSD (Device) protocol or WSD (Scanner) protocol is disabled.	For details about how to enable or disable the WSD protocol, see Security Guide.
"Cannot start scanning because communication was failed."	Scan Profile is not set on the client computer.	Set Scan Profile. For details about how to do this, see "Creating a New Scan Profile", Scan.

Messages	Causes	Solutions
"Cannot start scanning because communication was failed."	The [Take no action] setting has been selected on the client computer, forcing the client computer to remain inactive when it receives scan data.	Open scanner properties, click the [Events] tab, and then select [Start this program] as the computer's response on receipt of scan data. For details, see your operating system's Help.
"Cannot start scanning. Check the setting(s) on the PC."	The Scan Profile might be incorrectly configured.	Check the Scan Profile configuration.
"Could not send the data because the PC timed out before it was sent."	A time out occurred when using WSD Scanner. Time outs occur when too much time passes between scanning an original and sending its data. The followings are likely causes of time outs: <ul style="list-style-type: none"> • Too many originals per set. • Misfed originals. • Transmission of other jobs. 	<ul style="list-style-type: none"> • Reduce the number of originals, and then scan again. • Remove any misfed original, and then scan again. • Use Scanner Journal to check there are no jobs awaiting transmission, and then scan again.

When documents cannot be stored on a memory storage device

Messages	Causes	Solutions
"Cannot write on the memory storage device because remaining free space is insufficient."	The memory storage device is full and scan data cannot be saved. Even if the memory storage device appears to have sufficient free space, data might not be saved if the maximum number of files that can be saved is exceeded.	<ul style="list-style-type: none"> • Replace the memory storage device. • If the document is scanned as single-page or divided multiple pages, data already written to the memory storage device is saved as is. Replace the memory storage device, and then press [Retry] to save the remaining data, or press [Cancel] to redo the scan.

Messages	Causes	Solutions
"Cannot write on the memory storage device because the device is write-protected."	The memory storage device is write-protected.	Unlock the write-protection on the memory storage device.
"Cannot write on the memory storage device. Check the memory storage device and machine settings."	The memory storage device is faulty, or the file name contains a character that cannot be used.	<ul style="list-style-type: none"> • Check to see if the memory storage device is defective. • Check the memory storage device. It might be unformatted, or its format might be incompatible with this machine. • Check the file name set at the time of scanning. For details about the characters that can be used in file names, see "Specifying the File Name", Scan.
"Exceeded max. page capacity per file. Press [Write] to write the scanned data to the memory storage device, or press [Cancel] to delete."	The scan could not be completed because the maximum number of pages that can be scanned by this machine was exceeded during writing to the memory storage device.	Reduce the number of documents to be written to the memory storage device, and then try again.
"Memory is full. Press [Write] to write the current scanned data to the memory storage device, or press [Cancel] to delete."	The scan could not be completed because there was insufficient hard disk memory at the time of saving to the memory storage device.	Select whether or not to save the scanned document to the memory storage device.

Messages Displayed on the Client Computer

This section describes likely causes of and possible solutions for the main error messages displayed on the client computer when using the TWAIN driver. If a message not described here appears, act according to the message.

Messages	Causes	Solutions
"Any of Login User Name, Login Password or Driver Encryption Key is incorrect."	The entered login user name, password, or driver encryption key was invalid.	Check your login user name, login password, or driver encryption key, and then enter them correctly. For details about login user name, login password, and driver encryption key, see Security Guide.
"Authentication succeeded. However, the access privileges for scanner function has been denied."	The logged in user name does not have permission for scanner function.	For details about how to set permissions, see Security Guide.
"Cannot add any more scanning mode."	The maximum number of registerable scan modes has been exceeded.	The maximum number of modes that can be stored is 100. Delete unneeded modes.
"Cannot detect the paper size of the original. Specify the scanning size."	The set original was misaligned.	<ul style="list-style-type: none"> Place the original correctly. Specify the scan size. When placing an original directly on the exposure glass, the lifting/lowering action of the exposure glass cover or the ADF triggers the automatic original size detection process. Lift the exposure glass cover or the ADF 30 degrees or more.
"Cannot specify any more scanning area."	The maximum number of registerable scan areas has been exceeded.	The maximum number of scanning areas that can be stored is 100. Delete unneeded scanning areas.
"Clear Misfeed(s) in ADF."	A paper misfeed has occurred inside the ADF.	<ul style="list-style-type: none"> Remove the jammed originals, and then insert them again. For details about jammed paper, see "Removing Jammed Paper", Troubleshooting. When a misfeed occurs, replace the jammed originals. Check whether the originals are suitable to be scanned by the machine.

Messages	Causes	Solutions
"Error has occurred in the scanner driver."	An error has occurred in the driver.	<ul style="list-style-type: none"> • Check whether the network cable is connected correctly to the client computer. • Check whether the Ethernet board of the client computer is recognized correctly by Windows. • Check whether the client computer can use the TCP/IP protocol.
"Error has occurred in the scanner."	The application-specified scan conditions have exceeded the setting range of the machine.	Check whether the scanning settings made with the application exceed the setting range of the machine.
"Fatal error has occurred in the scanner."	An unrecoverable error has occurred on the machine.	An unrecoverable error has occurred in the machine. Contact your service representative.
"Insufficient memory. Close all other applications, then restart scanning."	Memory is insufficient.	<ul style="list-style-type: none"> • Close all the unnecessary applications running on the client computer. • Uninstall the TWAIN driver, and then reinstall it after restarting the computer.

Messages	Causes	Solutions
"Insufficient memory. Reduce the scanning area."	Scanner memory is insufficient.	<ul style="list-style-type: none"> • Reset the scan size. • Lower the resolution. • Set with no compression. For details about the settings, see TWAIN driver Help. <p>The problem may be due to the following cause:</p> <ul style="list-style-type: none"> • Scanning cannot be performed if large values are set for brightness when using halftone or high resolution. For details about the relationship between scan settings, see "Relationship between Resolution and Scan Size", Scan. • If a misfeed occurs, you might not scan an original. Remove the misfeed, and then scan the original again.
"Invalid Winsock version. Please use version 1.1 or higher."	You are using an invalid version of Winsock.	Install the operating system of the computer or copy Winsock from the operating system CD-ROM.
"No response from the scanner."	The machine or client computer is not connected to the network correctly.	<ul style="list-style-type: none"> • Check whether the machine or client computer is connected to the network correctly. • Disable the client computer's own firewall. For details about firewall, see Windows Help.
"No response from the scanner."	The network is crowded.	Wait for a while, and then try to reconnect.

Messages	Causes	Solutions
"Scanner is in use for other function. Please wait."	A function of the machine other than the Scanner function is being used such as the Copier function.	<ul style="list-style-type: none"> • Wait for a while, and then reconnect. • Cancel the job that is being processed. Press the [Stop] key. Follow the instructions in the message that appears and exit the function that is running.
"Scanner is not available on the specified device."	The TWAIN scanner function cannot be used on this machine.	Contact your service representative.
"Scanner is not ready. Check the scanner and the options."	The ADF cover is open.	Check whether the ADF cover is closed.
"The name is already in use. Check the registered names."	You tried to register a name that is already in use.	Use another name.

When there is a problem connecting to the scanner

Messages	Causes	Solutions
"Cannot connect to the scanner. Check the network Access Mask settings in User Tools."	An access mask is set.	For details about an access mask, contact your administrator.
"Cannot find "XXX" scanner used for the previous scan. "YYY" will be used instead." (("XXX" and "YYY" indicate scanner names.)	The main power of the previously used scanner is not set to "On".	Check whether the main power of the scanner used for the previous scan has been turned on.

Messages	Causes	Solutions
"Cannot find "XXX" scanner used for the previous scan. "YYY" will be used instead." ("XXX" and "YYY" indicate scanner names.)	The machine is not connected to the network correctly.	<ul style="list-style-type: none"> • Check that the previously used scanner is connected to the network correctly. • Cancel the personal firewall of the client computer. For details about firewall, see Windows Help. • Use an application such as telnet to make sure SNMPv1 or SNMPv2 is set as the machine's protocol. For details about how to check this, see "Remote Maintenance Using telnet", Connecting the Machine/ System Settings. • Select the scanner used for the previous scan.
"Communication error has occurred on the network."	A communication error has occurred on the network.	Check whether the client computer can use the TCP/IP protocol.
"Scanner is not available. Check the scanner connection status."	The machine's power is off.	Turn on the power.
"Scanner is not available. Check the scanner connection status."	The machine is not connected to the network correctly.	<ul style="list-style-type: none"> • Check whether the machine is connected to the network correctly. • Deselect the personal firewall function of the client computer. For details about firewall, see Windows Help. • Use an application such as telnet to make sure SNMPv1 or SNMPv2 is set as the machine's protocol. For details about how to check this, see "Remote Maintenance Using telnet", Connecting the Machine/ System Settings.

Messages	Causes	Solutions
"Scanner is not available. Check the scanner connection status."	Network communication is not available because the machine's IP address could not be obtained from the host name. If only "IPv6" is set to [Active], the IPv6 address might not be obtained.	<ul style="list-style-type: none">• Check whether the machine's host name is specified in the Network Connection Tool. For the WIA driver, check the [Network Connection] tab in the properties.• Use Web Image Monitor to set "LLMNR" of "IPv6" to [Active].• In Windows XP, IPv6 address cannot be obtained from the host name. Specify the machine's IPv6 address in the Network Connection Tool.

When Other Messages Appear

Messages	Causes	Solutions
<p>"Cannot connect with the wireless card. Turn the main power switch off, then check the card."</p> <p>(A "wireless LAN board" or "Bluetooth interface unit" is referred to as a "wireless card".)</p>	<ul style="list-style-type: none"> • The wireless LAN board was not inserted when the machine was turned on. • The wireless LAN board was pulled out after the machine was turned on. • The settings are not updated although the unit is detected. 	<p>Turn off the power, and then confirm the wireless LAN board is inserted correctly. After confirmation, turn on the power again. If the message appears again, contact your service representative.</p>
<p>"Cannot connect with the Bluetooth interface. Check the Bluetooth interface."</p>	<ul style="list-style-type: none"> • The Bluetooth interface unit was installed while the machine was turned on. • The Bluetooth interface unit was removed while the machine was turned on. 	<p>Turn off the power, and then confirm that the Bluetooth interface unit was installed correctly. After confirmation, turn on the power again. If the message appears again, contact your service representative.</p>
<p>"Clean the scanning glass. (Located next to the exposure glass.)"</p>	<p>The scanning glass or guide plate of the ADF is dirty.</p>	<p>Clean them. See "Maintaining Your Machine", Maintenance and Specifications.</p>
<p>"Following output tray is full. Remove paper."</p>	<p>The output tray is full.</p>	<p>Remove paper from the output tray to resume printing.</p>
<p>"Internal cooling fan is active."</p>	<p>Large print runs will cause the machine's interior to heat up, triggering the cooling fan.</p>	<p>The fan will emit noise, but this is normal and the machine will be operable while the fan is running.</p> <p>The amount of paper that can be printed and the total operation time until the fan starts running depends on the temperature of the location at which the machine is installed.</p>

Messages	Causes	Solutions
"Self checking..."	The machine is performing image adjustment operations.	The machine may perform periodic maintenance during operations. The frequency and duration of maintenance depends on the humidity, temperature, and printing factors such as number of prints, paper size, and paper type. Wait for the machine to get ready.
"XXX is not responding." (This message may appear while you are using the Smart Operation Panel. "XXX" in this message indicates the function is being used.)	The machine is busy processing data.	To continue the current job, press [Wait]. To stop the current job, press [Force close].

When There Is a Problem Scanning or Storing Originals

Messages	Causes	Solutions
"Cannot detect original size. Select scan size."	The machine failed to detect the size of the original.	<ul style="list-style-type: none"> Place the original correctly. Specify the scan size, and then place the originals again. For details about the settings for when fax function is being used, see "Scan Settings", Fax. When placing an original directly on the exposure glass, the lifting/lowering action of the exposure glass cover or the ADF triggers the automatic original size detection process. Lift the exposure glass cover or the ADF 30 degrees or more.

Messages	Causes	Solutions
"Captured file exceeded max. number of pages per file. Cannot send the scanned data."	The maximum number of pages per file has been exceeded.	Reduce the number of pages in the transmitted file, and then resend the file. For details about the maximum number of pages per file, see "Storage Function", Scan.
"Original(s) is being scanned for a different function."	Another function of the machine is being used.	Cancel the job in progress. Press [Exit], and then press the [Stop] key. Follow the instructions in the message that appears and exit the function that is running.

When the Home Screen Cannot Be Edited (When Using the Standard Operation Panel)

Messages	Causes	Solutions
"The image data size is not valid. See the manual for required data."	The image data size is not valid.	For details about file size for shortcut image, see "Displaying an Image on the [Home] Screen (When Using the Standard Operation Panel)", Convenient Functions.
"The format of the image data is not valid. See the manual for required data."	The file format of the shortcut image to be added is not supported.	The file format of shortcut images to be added must be PNG. Specify the image again.

When the Address Book Is Updated

Messages	Causes	Solutions
"Updating the destination list has failed. Try again?"	A network error has occurred.	<ul style="list-style-type: none"> • Check whether the server is connected. • Antivirus programs and firewalls can prevent client computers from establishing connection with this machine. • If you are using anti-virus software, add the program to the exclusion list in the application settings. For details about how to add programs to the exclusion list, see the anti-virus software Help. • To prevent a firewall blocking the connection, register the machine's IP address in the firewall's IP address exclusion settings. For details about the procedure for excluding an IP address, see your operating system's Help.
"Updating the destination list... Please wait. Specified destination(s) or sender's name has been cleared."	The destination list is being updated from the network using Web Image Monitor.	Wait until the message disappears. Do not turn off the power while this message is displayed. Depending on the number of destinations to be updated, there may be some delay before you can resume operation. Operation is not possible while this message is displayed.
"Updating the destination list... Please wait. Specified destination(s) or sender's name has been cleared."	A specified destination or sender's name was cleared when the destination list in the delivery server was updated.	Specify the destination or sender's name again.

When Data Cannot Be Sent Due to a Problem with the Destination

Messages	Causes	Solutions
"Some invalid destination(s) contained. Do you want to select only valid destination(s)?"	The specified group contains fax destinations, e-mail destinations, and/or folder destinations, either of which are incompatible with the specified transmission method.	In the message that appears at each transmission, press [Select].
"SMTP authentication E-mail address and Administrator E-mail address mismatch."	The SMTP authentication e-mail address and the administrator's e-mail address do not match.	For details about how to set SMTP authentication, see "File Transfer", Connecting the Machine/ System Settings.

When the Machine Cannot Be Operated Due to a Problem with the User Certificate

Messages	Causes	Solutions
"The destination cannot be selected because its encryption certificate is not currently valid."	The user certificate (destination certificate) has expired.	A new user certificate must be installed. For details about the user certificate (destination certificate), see Security Guide.
"The group destination cannot be selected because it contains a destination with a encryption certificate that is not currently valid."	The user certificate (destination certificate) has expired.	A new user certificate must be installed. For details about the user certificate (destination certificate), see Security Guide.
"Transmission cannot be performed because the encryption certificate is not currently valid."	The user certificate (destination certificate) has expired.	A new user certificate must be installed. For details about the user certificate (destination certificate), see Security Guide.

Messages	Causes	Solutions
"XXX cannot be YYY because the device certificate used for the S/MIME signature is not currently valid." (XXX and YYY indicate the user action.)	The device certificate (S/MIME) has expired.	A new device certificate (S/MIME) must be installed. For details about how to install a device certificate (S/MIME), see Security Guide.
"XXX cannot be YYY because there is a problem with the device certificate used for the S/MIME signature. Check the device certificate." (XXX and YYY indicate the user action.)	There is no device certificate (S/MIME), or the certificate is invalid.	For details about the device certificate (S/MIME), see Security Guide.
"XXX cannot be YYY because the Digital Signature's device certificate is not currently valid." (XXX and YYY indicate the user action.)	The device certificate (PDF with digital signature or PDF/A with digital signature) has expired.	A new device certificate (PDF with digital signature or PDF/A with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature or PDF/A with digital signature), see Security Guide.
"XXX cannot be YYY because there is a problem with the Digital Signature's device certificate. Check the device certificate." (XXX and YYY indicate the user action.)	There is no device certificate (PDF with digital signature or PDF/A with digital signature), or the certificate is invalid.	A new device certificate (PDF with digital signature or PDF/A with digital signature) must be installed. For details about how to install a device certificate (PDF with digital signature or PDF/A with digital signature), see Security Guide.

 **Note**

- If a fax or an e-mail cannot be sent and a message appears which states that there is a problem with the device certificate or user certificate, a new certificate must be installed. For details about how to install a new certificate, see Security Guide.

When Problems Occur While Logging In

Messages	Causes	Solutions
"Authentication has failed."	The entered login user name or login password is not correct.	For details about the correct login user name and login password, see Security Guide.
"Authentication has failed."	The machine cannot perform authentication.	For details about authentication, see Security Guide.

When the User Lacks Privileges to Perform an Operation

Messages	Causes	Solutions
"You do not have the privileges to use this function."	The logged in user name does not have permission for the selected function.	For details about how to set permissions, see Security Guide.
"The selected file(s) contained file(s) without access privileges. Only file(s) with access privileges will be deleted."	You have tried to delete files without the authority to do so.	To check your access permission for stored documents, or to delete a document you do not have permission to delete, see Security Guide.

When the LDAP Server Cannot Be Used

Messages	Causes	Solutions
"Connection with LDAP server has failed. Check the server status."	A network error has occurred and connection has failed.	Try the operation again. If the message is still shown, the network may be busy. Check the settings for LDAP server in [System Settings]. For details about settings for LDAP server, see "Programming the LDAP server", Connecting the Machine/ System Settings.

Messages	Causes	Solutions
"Exceeded time limit for LDAP server search. Check the server status."	A network error has occurred and connection has failed.	<ul style="list-style-type: none">• Try the operation again. If the message is still shown, the network may be busy.• Check that the correct settings for LDAP server are listed in [Administrator Tools] of [System Settings]. For details about LDAP server, see "Programming the LDAP server", Connecting the Machine/ System Settings.
"LDAP server authentication has failed. Check the settings."	A network error has occurred and connection has failed.	Make settings correctly for the user name and the password for LDAP server authentication.

INDEX

2 Sided Print..... 110

A

Address Book..... 11, 94, 95, 228
Address Book Management.....48
ADF..... 8, 29, 33, 38, 68
ADF's extender..... 31, 34
Authentication screen..... 64
Auto document feeder..... 8
Auto Reduce / Enlarge..... 14, 73

B

Basic procedure.. 71, 91, 109, 117, 126, 131, 137
Beeping pattern..... 175
Booklet..... 14
Browser..... 48
Bypass tray..... 31, 34, 84, 85, 146, 147

C

Canceling a transmission..... 100
Caster table for lower paper tray..... 36, 38, 39
Check Status key..... 41, 44, 173
Clear key..... 41
Combine..... 9, 14
Combine printing..... 111
Combined copying..... 79
Communicating indicator..... 41
Computer..... 218
Confidential File indicator..... 41
Control panel..... 30, 33, 41
Copier..... 47, 71
Copy orientation..... 77
Copy/Document Server..... 182
Custom size..... 84
Custom size paper..... 148

D

Data In indicator..... 41, 44
Data security for copying..... 28
Destination..... 125, 229
Display language..... 46
Display panel..... 41, 44
Distributed scan management..... 26

Document Server..... 10, 17, 48, 90, 115, 116, 137
DSM..... 26
Duplex..... 14
Duplex Copy..... 9, 75

E

E-mail address..... 130
E-mail destination..... 127, 129
E-mail transmission..... 20
Embedding text information..... 24
Energy Saver key..... 41
Enter key..... 41
Envelope..... 85, 86, 113, 114, 163
Error log..... 199
Error report..... 199
Exposure glass..... 29, 33, 67
Exposure glass cover..... 29, 36, 38
Extender..... 31, 35
External Options..... 36
External tray..... 37, 38, 40

F

Facsimile..... 47, 91, 186
Fax destination..... 94, 95
Fax indicator..... 44
Fax Received indicator..... 41
File type..... 134
Frequently-used settings..... 12
Front cover..... 30, 33
Function key..... 41

H

Handset..... 39
Hold Print..... 16
Home key..... 41, 44
Home screen..... 13, 47, 49, 52, 53, 227
Home screen image..... 47
How to Read the Manuals..... 6

I

Immediate transmission..... 97, 98
Indicator..... 173
Information screen..... 9
Initial settings..... 12

Internal Finisher SR3130.....	37, 38, 40
Internal Finisher SR3180.....	37, 38, 40
Internal shift tray.....	37, 38, 40
Internal tray 1.....	30, 33
Internal tray 2.....	37, 38, 40
Interrupt key.....	41
IP-Fax.....	20

J

Journal.....	106
--------------	-----

L

LAN-Fax.....	18
LDAP Server.....	231
Loading orientation-fixed paper.....	152
Loading paper.....	143
Loading two-sided paper.....	152
Locked Print.....	16
Logging in.....	231
Logging in to the machine.....	64
Login/Logout key.....	41
Lower paper tray.....	36, 38, 39
Lower paper trays.....	30, 34, 36, 38, 39
Lower right cover.....	32, 35

M

Magazine.....	14
Main Power.....	63
Main power indicator.....	41, 44
Main power switch.....	30, 33
Managing document.....	116
Media access lamp.....	41, 44
Media slot.....	41
Media slots.....	44
Memory transmission.....	91, 93
Menu key.....	44
Message.....	176, 182, 186, 196, 199, 200, 202, 204, 205, 206, 209, 211, 213, 214, 215, 216, 217, 218, 222, 225, 226, 227, 228, 229, 231
Model-Specific Information.....	7

N

Names of Major Features.....	8
Network settings.....	187
Number key.....	41

O

OCR unit.....	24
OHP transparency.....	150
One-Sided Combine.....	80
Options.....	36
Orientation-fixed paper.....	152
Original orientation.....	75

P

Paper capacity.....	155
Paper guides.....	31, 35
Paper size.....	147, 155
Paper thickness.....	155
Paper tray.....	30, 34, 144
Paper type.....	155
Path.....	125
PCL.....	107
Placing originals.....	67
Preventing information leakage.....	25
Printer.....	47, 109, 196, 199, 200, 202, 204, 205, 206
Printer Bypass Paper Size.....	147, 148
Printer driver.....	108
Problem.....	176, 226
Program.....	12, 57
Program key.....	41

Q

Quick Install.....	107
--------------------	-----

R

Reducing my Costs.....	9
Region A.....	7
Region B.....	7
Registering destinations.....	11
Remote Fax.....	22, 193
Reset key.....	41
Return key.....	44
Right cover.....	32, 35
Running out of toner.....	169

S

Sample Copy key.....	41
Sample Print.....	16
Scan file.....	126, 131

Scan settings.....	135
Scan to Folder.....	23, 117
Scanner....	47, 117, 209, 211, 213, 214, 215, 216, 217, 222
Sending scan files.....	10, 23
Shared folder.....	118
Shortcut.....	53
Shortcut icon.....	48, 49, 53
Shortcuts from the application list screen.....	55
Shortcuts to bookmarks.....	54
Shortcuts to programs.....	54
Simple Screen key.....	41
Smart Operation Panel.....	38, 39
SMB Folder.....	120, 122, 123, 124
Sort.....	87, 88
Standard printing.....	109
Start key.....	41
Status icon.....	171
Stop key.....	41, 44
Stored documents.....	104, 139
Stored file.....	132
Stored Print.....	16
Storing a document.....	103
Storing data.....	90
Storing document.....	115
Storing received documents.....	18
Symbols.....	6

T

Thick paper.....	150, 162
Toner.....	167, 169
Tray 1.....	30, 34
Tray 2.....	30, 34
Turning On/Off the Power.....	63
Two-Sided Combine.....	81
Two-sided paper.....	152

U

Unauthorized copy prevention.....	28
Used toner.....	169
User certificate.....	229
User code authentication.....	64
User Tools/Counter key.....	41
Using scanned files on the computer.....	10

V

Vents.....	30, 31, 32, 33, 34, 35
------------	------------------------

W

Web Image Monitor.....	27, 141
Widget.....	56
WSD scanner.....	216

MEMO



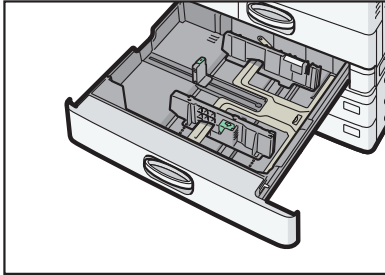
Notes for Users

Due to product improvements, the shapes of the main unit's paper trays (Trays 2, 3, 4) have been changed. In accordance with this, changes to the manual have been made as shown below.

❖ Paper trays (Shapes of Trays 2, 3, 4 before and after the improvement)

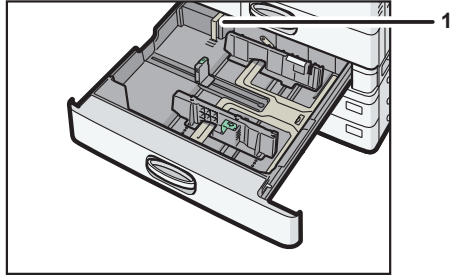
The illustration below shows Tray 2.

Before improvement:



DDU016

After improvement:



DDU010

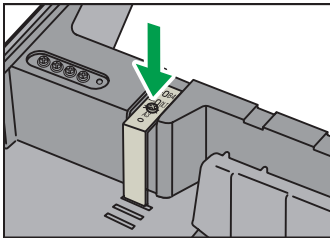
1. Supporting side fence

↓ Note

- There are no changes to the method used to load paper into the tray.
- Adjust the supporting side fence before loading into the tray sheets of paper whose size is over A3 or 11" x 17".

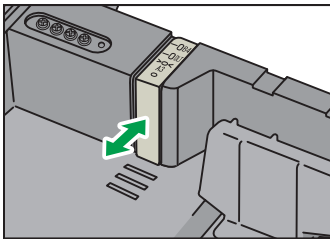
❖ Adjusting the supporting side fence

1. Loosen the fixed screw with an object such as a coin.

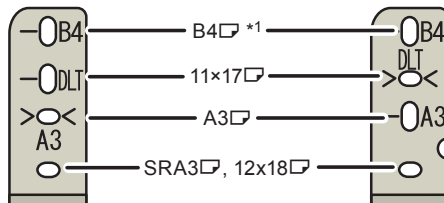


DDU011

2. Move the supporting side fence to match the size of the paper you want to load. Set the screw position to match the size of the set paper.



DDU012

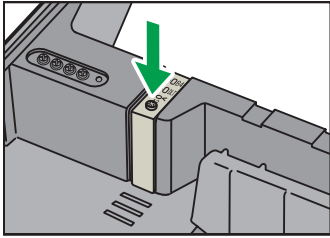


*1 Not for common use

↓ Note

- The marks on the supporting side fence may differ depending on the region.

3. Tighten the fixed screw with an object such as a coin.



❖ Recommended Paper Sizes (Trays 2, 3, 4)

The paper sizes that can be loaded in Trays 2, 3, 4 are changed as follows:

The paper sizes for postcards and envelopes are those specified in the manual.

Paper Specifications and Adding Paper > Recommended Paper > Recommended Paper Sizes and Types > Tray 2 > Plain Paper–Thick Paper 4

Paper size	
<ul style="list-style-type: none"> • Paper sizes that can be detected automatically: 	
Region A	A3, A4, A5, B4 JIS, B5 JIS, 8 ¹ / ₂ ×11, SRA3 *2
Region B	A4, A5, B5 JIS, 11×17, 8 ¹ / ₂ ×14, 8 ¹ / ₂ ×11, 7 ¹ / ₄ ×10 ¹ / ₂ , 12×18 *2
<ul style="list-style-type: none"> • Select the paper size using the Tray Paper Settings menu: 	
Region A	A5, A6, B6 JIS, 11×17, 8 ¹ / ₂ ×14, 8 ¹ / ₂ ×13, 8 ¹ / ₂ ×11, 8 ¹ / ₄ ×14, 8 ¹ / ₄ ×13, 8×13, 8×10, 7 ¹ / ₄ ×10 ¹ / ₂ , 5 ¹ / ₂ ×8 ¹ / ₂ , 8K, 16K, 12×18 *2, 11×15, 10×14
Region B	A3, A4, A5, A6, B4 JIS, B5 JIS, B6 JIS, 8 ¹ / ₂ ×13, 8 ¹ / ₄ ×14, 8 ¹ / ₄ ×13, 8×13, 8×10, 7 ¹ / ₄ ×10 ¹ / ₂ , 5 ¹ / ₂ ×8 ¹ / ₂ , 8K, 16K, 11×15, 10×14, SRA3 *2
<ul style="list-style-type: none"> • Custom size *1*3: 	
Region A	Vertical: 90.0–320.0 mm, Horizontal: 148.0–457.2 mm
Region B	Vertical: 3.55–12.59 inches, Horizontal: 5.83–18.00 inches

Paper Specifications and Adding Paper > Recommended Paper > Recommended Paper Sizes and Types > Trays 3 and 4 > Plain Paper–Thick Paper 4

Paper size	
<ul style="list-style-type: none"> • Paper sizes that can be detected automatically: 	
Region A	A3, A4, A5, B4 JIS, B5 JIS, 8 ¹ / ₂ ×11, SRA3 *2
Region B	A4, A5, B5 JIS, 11×17, 8 ¹ / ₂ ×14, 8 ¹ / ₂ ×11, 7 ¹ / ₄ ×10 ¹ / ₂ , 12×18 *2
<ul style="list-style-type: none"> • Select the paper size using the Tray Paper Settings menu: 	
Region A	11×17, 8 ¹ / ₂ ×14, 8 ¹ / ₂ ×13, 8 ¹ / ₂ ×11, 8 ¹ / ₄ ×14, 8 ¹ / ₄ ×13, 8×13, 8×10, 7 ¹ / ₄ ×10 ¹ / ₂ , 8K, 16K, 12×18 *2, 11×15, 10×14
Region B	A3, A4, B4 JIS, B5 JIS, 8 ¹ / ₂ ×13, 8 ¹ / ₄ ×14, 8 ¹ / ₄ ×13, 8×13, 8×10, 7 ¹ / ₄ ×10 ¹ / ₂ , 8K, 16K, 11×15, 10×14, SRA3 *2
<ul style="list-style-type: none"> • Custom size *1*3: 	
Region A	Vertical: 182.0–320.0 mm, Horizontal: 148.0–457.2 mm
Region B	Vertical: 7.17–12.59 inches, Horizontal: 5.83–18.00 inches

*1 When loading paper with a vertical length of more than 304.8 mm (12.0 inches) in Trays 2–4, use paper that has a horizontal width of 450 mm (17.8 inches) or less.

*2 Adjust the supporting side fence before loading SRA3 or 12×18 paper.

*3 Set the supporting side fence position to SRA3 before loading paper with a vertical length of 297 mm or longer and a horizontal length of over 335 mm.





Operating Instructions

Security Guide

TABLE OF CONTENTS

- Functions That Require Options.....9
- Main Software Names.....10
- 1. Getting Started**

- Before Configuring the Security Function Settings.....11
- Before Using This Machine.....12
- Administrators and Users.....14
- Administrators.....15
- Configuring Administrator Authentication.....16
 - Specifying Administrator Privileges.....17
 - Registering and Changing Administrators.....19
 - Using Web Image Monitor to Configure Administrator Authentication.....22
- Administrator Login Method.....23
 - Logging in Using the Control Panel.....23
 - Logging in Using Web Image Monitor.....24
- Administrator Logout Method.....25
 - Logging out Using the Control Panel.....25
 - Logging out Using Web Image Monitor.....25
- Supervisor.....26
 - Resetting the Administrator's Password.....26
 - Changing the Supervisor.....27
- 2. Configuring User Authentication**

- Users.....29
- About User Authentication.....30
- Configuring User Authentication.....31
- User Code Authentication.....34
- Basic Authentication.....37
 - Specifying Basic Authentication.....37
 - Authentication Information Stored in the Address Book.....39
 - Specifying Login User Names and Passwords.....40
 - Specifying Login Details.....41
- Windows Authentication.....43
 - Specifying Windows Authentication.....45
 - Installing Internet Information Services (IIS) and Certificate Services.....49

Creating the Server Certificate.....	51
If the Fax Number Cannot be Obtained.....	51
LDAP Authentication.....	53
Integration Server Authentication.....	58
Printer Job Authentication.....	63
Printer Job Authentication Levels.....	63
Printer Job Types.....	63
"authfree" Command.....	66
Auto Registration to the Address Book.....	67
Automatically Registered Address Book Items.....	67
Data Carry-over Setting for Address Book Auto-program.....	67
User Lockout Function.....	69
Specifying the User Lockout Function.....	70
Canceling Password Lockout.....	70
Auto Logout.....	71
Authentication Using an External Device.....	73

3. Restricting Machine Usage

Restricting Usage of the Destination List.....	75
Preventing Changes to Administrator Settings.....	77
Limiting the Settings that Can Be Changed by Each Administrator.....	77
Prohibiting Users from Making Changes to Settings.....	77
Specifying Menu Protect.....	78
Copy Function.....	78
Fax Function.....	78
Printer Function.....	78
Scanner Function.....	79
Limiting Available Functions.....	80
Restricting Media Slot Access.....	82
Managing Print Volume per User.....	83
Specifying Limitations for Print Volume.....	84
Specifying the Default Maximum Use Count.....	86
Specifying the Maximum Use Count per User.....	87
Checking Print Volume per User.....	88

Printing a List of Print Volume Use Counters.....	89
Clearing Print Volume Use Counters.....	91
Configuring the Auto-Reset Function.....	92

4. Preventing Leakage of Information from Machines

Protecting the Address Book.....	95
Specifying Address Book Access Permissions.....	95
Encrypting Data in the Address Book.....	97
Encrypting Data on the Hard Disk.....	99
Enabling the Encryption Settings.....	101
Backing Up the Encryption Key.....	103
Updating the Encryption Key.....	103
Canceling Data Encryption.....	104
Deleting Data on the Hard Disk.....	106
Conditions for Use.....	106
Instructions for Use.....	106
Auto Erase Memory.....	106
Erase All Memory.....	111

5. Enhanced Network Security

Access Control.....	115
Enabling and Disabling Protocols.....	116
Enabling and Disabling Protocols Using the Control Panel.....	123
Enabling and Disabling Protocols Using Web Image Monitor.....	123
Specifying Network Security Level.....	125
Specifying Network Security Level Using the Control Panel.....	125
Specifying Network Security Level Using Web Image Monitor.....	126
Status of Functions under Each Network Security Level.....	126
Protecting the Communication Path via a Device Certificate.....	130
Creating and Installing a Device Certificate from the Control Panel (Self-Signed Certificate).....	130
Creating and Installing a Device Certificate from Web Image Monitor (Self-Signed Certificate).....	131
Creating the Device Certificate (Issued by a Certificate Authority).....	132
Installing the Device Certificate (Issued by a Certificate Authority).....	133
Installing an Intermediate Certificate (Issued by a Certificate Authority).....	134
Configuring SSL/TLS.....	135

Enabling SSL/TLS.....	136
User Setting for SSL/TLS.....	137
Setting the SSL/TLS Encryption Mode.....	138
Enabling SSL for SMTP Connections.....	139
Configuring S/MIME.....	141
E-mail Encryption.....	141
Attaching an Electronic Signature.....	143
Specifying Checking of the Certificate Valid Period.....	145
Configuring PDFs with Electronic Signatures.....	147
Configuring IPsec.....	148
Encryption and Authentication by IPsec.....	148
Encryption Key Auto Exchange Settings.....	149
IPsec Settings.....	150
Encryption Key Auto Exchange Settings Configuration Flow.....	156
telnet Setting Commands.....	160
Configuring IEEE 802.1X Authentication.....	166
Installing a Site Certificate.....	166
Selecting the Device Certificate.....	167
Setting Items of IEEE 802.1X for Ethernet.....	167
Setting Items of IEEE 802.1X for Wireless LAN.....	169
SNMPv3 Encryption.....	171
Encrypting Transmitted Passwords.....	172
Specifying a Driver Encryption Key.....	172
Specifying an IPP Authentication Password.....	173
Kerberos Authentication Encryption Setting.....	175

6. Preventing the Leaking of Documents

Managing Folders.....	177
Deleting Folders.....	177
Changing the Password of a Folder.....	178
Unlocking Folders.....	179
Managing Stored Files.....	181
Configuring Access Permission for Each Stored File.....	182
Changing the Owner of a Document.....	185

Configuring Access Permission for Each User for Stored Files.....	185
Specifying Passwords for Stored Files.....	187
Unlocking Stored Files.....	188
Managing Locked Print Files.....	190
Deleting Locked Print Files.....	190
Changing the Password of a Locked Print File.....	192
Unlocking a Locked Print File.....	193
Unauthorized Copy Prevention / Data Security for Copying.....	195
Enabling Pattern Printing.....	196
Enabling Detect Data Security for Copying.....	197
Printing User Information on Paper.....	199
Enforced Storage of Documents to be Printed on a Printer.....	201

7. Managing the Machine

Managing Log Files.....	203
Using Web Image Monitor to Manage Log Files.....	204
Logs That Can Be Managed Using Web Image Monitor.....	204
Attributes of Logs You Can Download.....	209
Specifying Log Collect Settings.....	234
Specifying Log Encryption.....	235
Downloading Logs.....	236
Number of Logs That Can Be Kept on the Machine.....	236
Notes on Operation When the Number of Log Entries Reaches Maximum.....	238
Printer Job Logs.....	240
Deleting All Logs.....	241
Disabling Log Transfer to the Log Collection Server.....	241
Managing Logs from the Machine.....	242
Disabling Log Transfer to the Log Collection Server.....	242
Specifying Delete All Logs.....	242
Managing Logs from the Log Collection Server.....	243
Configuring the Home Screen for Individual Users.....	244
Warnings About Using User's Own Home Screens.....	244
Configuring the Browser Functions.....	246
Precautions for Using the Browser Function.....	246

Troubleshooting.....	246
Managing Device Information.....	248
Exporting Device Information.....	249
Importing Device Information.....	250
Troubleshooting.....	252
Managing Eco-friendly Counter.....	254
Configuring the Display of Eco-friendly Counters.....	254
Clearing a Machine's Eco-friendly Counter.....	255
Clearing Users' Eco-friendly Counters.....	255
Managing the Address Book.....	256
Specifying Auto Deletion of Address Book Data.....	256
Deleting All Data in the Address Book.....	256
Specifying the Extended Security Functions.....	257
Other Security Functions.....	265
Fax Function.....	265
Scanner Function.....	266
System Status.....	266
Confirming Firmware Validity.....	266
Restricting a Customer Engineer Operation.....	267
Additional Information for Enhanced Security.....	268
Settings You Can Configure Using the Control Panel.....	268
Settings You Can Configure Using Web Image Monitor.....	270
Settings You Can Configure When IPsec Is Available/Unavailable.....	272

8. Troubleshooting

If a Message is Displayed.....	275
If an Error Code is Displayed.....	277
Basic Authentication.....	277
Windows Authentication.....	278
LDAP Authentication.....	282
Integration Server Authentication.....	286
If the Machine Cannot Be Operated.....	289

9. List of Operation Privileges for Settings

How to Read.....	295
------------------	-----

System Settings.....	296
Edit Home (When Using the Standard Operation Panel).....	306
Copier / Document Server Features.....	307
Facsimile Features.....	313
Printer Functions.....	316
Printer Features.....	317
Scanner Features.....	321
Browser Features.....	323
Extended Feature Settings.....	324
Maintenance.....	325
Screen Features (When Using the Smart Operation Panel).....	326
Edit Home (When Using the Smart Operation Panel).....	328
Web Image Monitor: Display Eco-friendly Counter.....	329
Web Image Monitor: Job.....	330
Web Image Monitor: Device Settings.....	332
Web Image Monitor: Printer.....	342
Web Image Monitor: Fax.....	346
Web Image Monitor: Scanner.....	348
Web Image Monitor: Interface.....	351
Web Image Monitor: Network.....	353
Web Image Monitor: Security.....	357
Web Image Monitor: @Remote.....	358
Web Image Monitor: Webpage.....	359
Web Image Monitor: Extended Feature Settings.....	360
Web Image Monitor: Address Book.....	361
Web Image Monitor: Reset Printer Job.....	362
Web Image Monitor: Reset the Machine.....	363
Web Image Monitor: Device Home Management (When Using the Standard Operation Panel).....	364
Web Image Monitor: User's Own Customization (When Using the Smart Operation Panel).....	365
Web Image Monitor: Screen Monitoring.....	366
Web Image Monitor: Customize Screen per User.....	367
Web Image Monitor: Document Server.....	368
Web Image Monitor: Fax Received File.....	369

Web Image Monitor: Printer: Print Jobs.....	370
List of Operation Privileges for Stored Files.....	371
List of Operation Privileges for Address Books.....	373
Trademarks.....	377
INDEX	379

Functions That Require Options

The following functions require certain options and additional functions.

- Detect Data Security for Copying
Copy Data Security Unit

For details about other functions that require options, see "Functions Requiring Optional Configurations", Getting Started.

Main Software Names

Product name	Names in the text
ScanRouter EX Professional ^{*1} and ScanRouter EX Enterprise ^{*1}	the ScanRouter delivery software

*1 This product is no longer sold.

1. Getting Started

This chapter describes the precautions to take when using the machine's security features and how to configure the administrator settings.

Before Configuring the Security Function Settings

★ Important

- **If the security settings are not configured, the data in the machine is vulnerable to attack.**
- To prevent this machine being stolen or willfully damaged, etc., install it in a secure location.
- Purchasers of this machine must make sure that people who use it do so appropriately, in accordance with operations determined by the machine administrator and supervisor. If the administrator or supervisor does not make the required security settings, there is a risk of security breaches by users.
- Before setting this machine's security features and to ensure appropriate operation by users, administrators must read the Security Guide completely and thoroughly, paying particular attention to the section entitled "Before Configuring the Security Function Settings".
- 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.
- For protection of data during the communication stage, apply the machine's communication security functions and connect it to devices that support security functions such as encrypted communication.
- Administrators should routinely examine the machine's logs to check for irregular and unusual events.

Before Using This Machine

This section explains how to enable encryption of transmitted data and configure the administrator account. If you want a high level of security, make the following setting before using the machine.

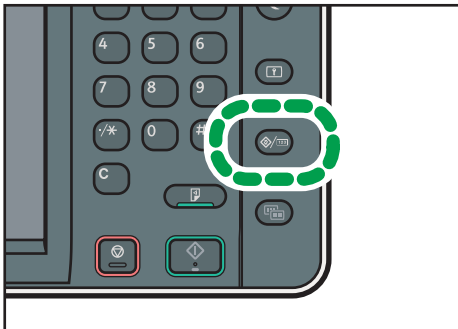
1. Turn the machine on.

For details about turning on the main power, see "Turning On/Off the Power", Getting Started.

2. Display the initial settings screen.

- When using the standard operation panel

Press the [User Tools/Counter] key.



CXX005

- When using the Smart Operation Panel

Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

3. Press [System Settings].

4. Press [Interface Settings].

5. Specify IPv4 Address.

For details on how to specify the IPv4 address, see "Interface Settings", Connecting the Machine/System Settings.

6. Press [File Transfer] in [System Settings].

7. Press [Administrator's E-mail Address], and then specify the e-mail address of the administrator of this machine.

8. Create and install the device certificate from the control panel.

For information on how to install the device certificate, see page 130 "Protecting the Communication Path via a Device Certificate".

As the e-mail address for the device certificate, enter the address specified in Step 7.

9. Change the administrator's user name and password.

For details about specifying administrators' user names and passwords, see page 19 "Registering and Changing Administrators".

10. Connect the machine to the general usage network environment.

Note

- To enable higher security, see page 268 "Additional Information for Enhanced Security".

Administrators and Users

1

This section explains the terms "administrator", "supervisor", "user", and "owner" as used in this manual.

Administrator

There are four types of administrators for the machine: user administrator, machine administrator, network administrator, and file administrator.

Their main role is to specify the settings for operating the machine. Their access privileges depend on the administrator type. Administrators cannot perform normal operations, such as copying and printing.

Supervisor

There is only one supervisor. The supervisor can specify each administrator's password. For normal operations, a supervisor is not required, because administrators specify their own passwords.

User

Users are people using the machine for normal operations, such as copying and printing.

Owner

A user who has registered files in the machine under the copier, printer, or other functions is called an owner.

Administrators

Administrators manage user access to the machine and various other important functions and settings.

When an administrator controls limited access and settings, first select the machine's administrator and enable the authentication function before using the machine. When the authentication function is enabled, the login user name and login password are required in order to use the machine. The role of administrator for this machine is divided into four categories according to their function: user administrator, machine administrator, network administrator, and file administrator. Sharing administrator tasks eases the burden on individual administrators while at the same time limiting unauthorized operations by an administrator. Multiple administrator roles can be assigned to one administrator and one role can also be shared by more than one administrator. A supervisor can also be set up, who can then change the administrators' passwords.

Administrators cannot use functions such as copying and printing. To use these functions, the administrator must be authenticated as the user.

For instructions on registering the administrator, see page 19 "Registering and Changing Administrators", and for instructions on changing the administrator's password, see page 26 "Supervisor". For details on Users, see page 29 "Users".

Important

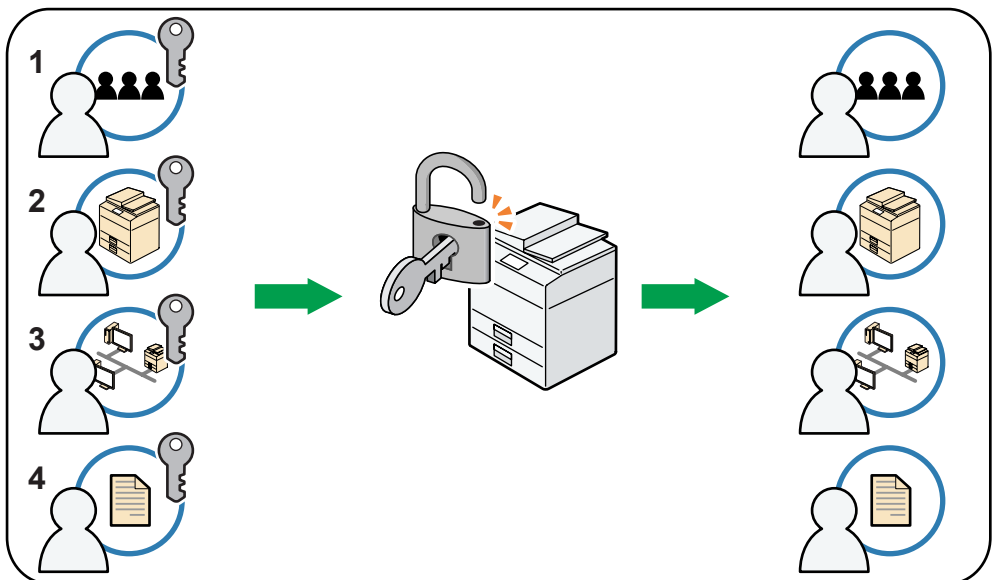
- If user authentication is not possible because of a problem with the hard disk or network, you can use the machine by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the machine urgently.

Configuring Administrator Authentication

Administrator authentication requires the login user name and password for verifying administrators attempting to specify the machine's settings or access them from a network. When registering an administrator, you cannot use a login user name already registered in the Address Book. Administrators are handled differently from the users registered in the Address Book. Windows authentication, LDAP authentication and Integration Server Authentication are not performed for an administrator, so an administrator can log in even if the server is unreachable due to a network problem. Each administrator is identified by a login user name. One person can act as more than one type of administrator if multiple administrator privileges are granted to a single login user name. For instructions on registering the administrator, see page 19 "Registering and Changing Administrators".

You can specify the login user name, login password, and encryption password for each administrator. The encryption password is used for encrypting data transmitted via SNMPv3. It is also used by applications such as SmartDeviceMonitor for Admin/Device Manager NX Lite that use SNMPv3. Administrators are limited to managing the machine's settings and controlling user access, so they cannot use functions such as copying and printing. To use these functions, the administrator must register as a user in the Address Book and then be authenticated as the user. Specify administrator authentication, and then specify user authentication. For details about specifying authentication, see page 31 "Configuring User Authentication".

Roles of each administrator



CJC009

1. User administrator

This is the administrator who manages personal information in the Address Book.

A user administrator can register/delete users in the Address Book or change users' personal information.

Users registered in the Address Book can also change and delete their own information.

If any of the users forget their password, the user administrator can delete it and create a new one, allowing the user to access the machine again.

2. Machine administrator

This is the administrator who mainly manages the machine's default settings. You can set the machine so that the default for each function can only be specified by the machine administrator. By making this setting, you can prevent unauthorized people from changing the settings and allow the machine to be used securely by its many users.

3. Network administrator

This is the administrator who manages the network settings. You can set the machine so that network settings such as the IP address and settings for sending and receiving e-mail can only be specified by the network administrator.

By making this setting, you can prevent unauthorized users from changing the settings and disabling the machine, and thus ensure correct network operation.

4. File administrator

This is the administrator who manages permission to access stored files. You can specify passwords to allow only registered users with permission to view and edit files stored in Document Server. By making this setting, you can prevent data leaks and tampering due to unauthorized users viewing and using the registered data.

↓ Note

- Administrator authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.
- You can specify User Code Authentication without specifying administrator authentication.

Specifying Administrator Privileges

To specify administrator authentication, set "Administrator Authentication Management" to [On]. If this setting is enabled, administrators will be able to configure only settings allocated to them.

To log in as an administrator, use the default login user name and login password.

When you log in as an administrator, the default login user name is "admin". The password is not configured by default.

For details about logging in and logging out with administrator authentication, see page 23 "Administrator Login Method" and page 25 "Administrator Logout Method".

★ Important

- If you have enabled "Administrator Authentication Management", make sure not to forget the administrator login user name and login password. If an administrator login user name or login password is forgotten, a new password must be specified using the supervisor's privilege. For details on supervisor privileges, see page 26 "Supervisor".

1. Display the initial settings screen.

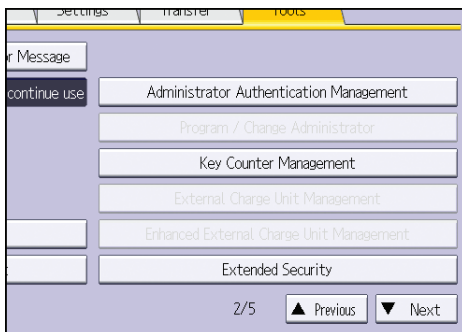
- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Press [System Settings].

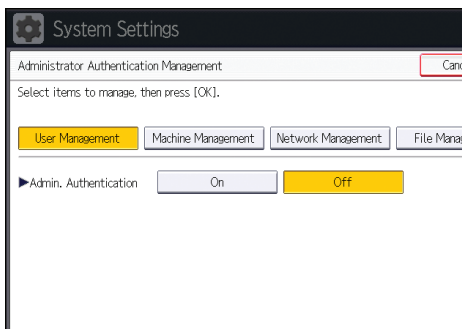
3. Press [Administrator Tools].

4. Press [▼Next].

5. Press [Administrator Authentication Management].



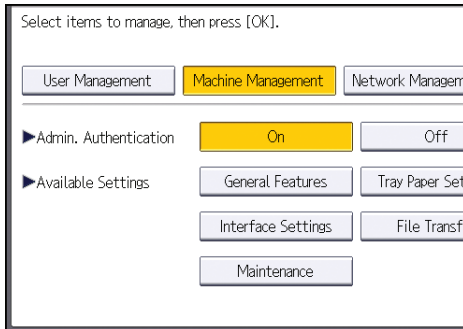
6. Press [User Management], [Machine Management], [Network Management], or [File Management] to select which settings to manage.



7. Set "Admin. Authentication" to [On].

"Available Settings" appears.

8. Select the settings to manage from "Available Settings".



The selected settings will be unavailable to users.

The available settings depend on the administrator type.

To specify administrator authentication for more than one category, repeat Steps 6 to 8.

9. Press [OK].

10. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

Registering and Changing Administrators

If administrator authentication has been specified, we recommend only one person take each administrator role.

The sharing of administrator tasks eases the burden on individual administrators while also restricting unauthorized operations by a single administrator. You can register up to four login user names (Administrators 1-4) to which you can grant administrator privileges.

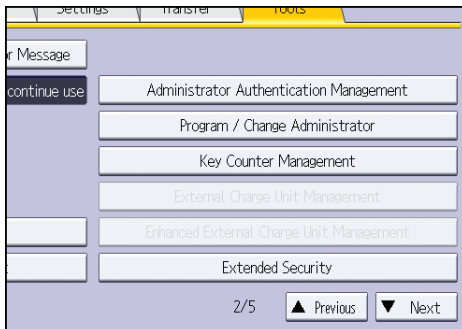
An administrator's privileges can only be changed by an administrator with the relevant privileges.

Be sure to assign all administrator privileges so that each administrator privilege is associated with at least one administrator.

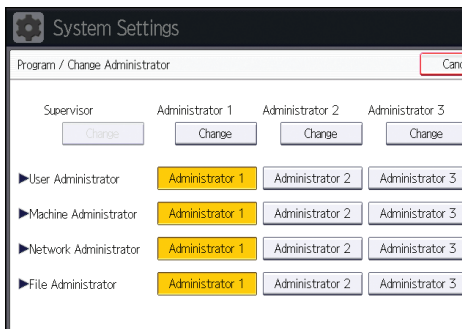
For details about logging in and logging out with administrator authentication, see page 23 "Administrator Login Method" and page 25 "Administrator Logout Method".

1. Log in as an administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].

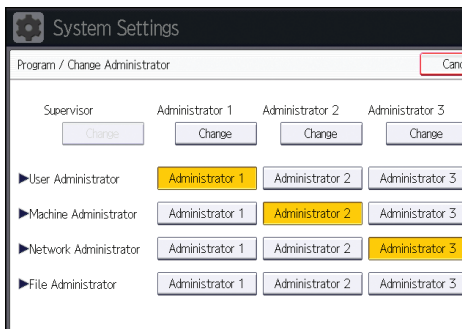
5. Press [Program / Change Administrator].



6. In the line for the administrator whose privilege you want to specify, press [Administrator 1], [Administrator 2], [Administrator 3] or [Administrator 4], and then press [Change].



When allocating administrators' privileges to one person each, select one administrator under each category as shown below.



To combine the privileges of multiple administrators, assign multiple administrators to a single administrator.

For example, to assign machine administrator privilege and user administrator privilege to [Administrator 1], press [Administrator 1] in the lines for the machine administrator and the user administrator.

7. Press [Change] for "Login User Name".

8. Enter the login user name, and then press [OK].
9. Press [Change] for "Login Password".
10. Enter the login password, and then press [OK].
Follow the password policy to strengthen the login password.
For details about the password policy and how to specify it, see page 257 "Specifying the Extended Security Functions".
11. Re-enter the login password for confirmation, and then press [OK].
12. Press [Change] for "Encryption Password".
13. Enter the encryption password, and then press [OK].
14. Re-enter the encryption password for confirmation, and then press [OK].
15. Press [OK] twice.
You will be automatically logged out.

↓ Note

- For the characters that can be used for login user names and passwords, see page 21 "Usable characters for user names and passwords".

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

- Cannot contain spaces, colons or quotation marks.
- Cannot be comprised of numbers only or cannot be left blank.
- Can be up to 32 characters long.

Login password

- The maximum password length for administrators and supervisors is 32 characters; for users it is 128 characters.
- Make passwords using a combination of capitals, small letters, numbers, and symbols. The more characters, the harder it is for others to guess.
- If the password's complexity and minimum length have been configured in [Password Policy] in [Extended Security], only passwords meeting the requirements can be specified. For details

about specifying the password policy, see "Password Policy" in page 257 "Specifying the Extended Security Functions".

Using Web Image Monitor to Configure Administrator Authentication

Using Web Image Monitor, you can log in to the machine and change the administrator settings. For details about logging in and logging out with administrator authentication, see page 23 "Administrator Login Method" and page 25 "Administrator Logout Method".

1. Log in as an administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Administrator Authentication Management] or [Program/Change Administrator] under "Device Settings".
4. Change the settings as desired.
5. Log out.

 **Note**

- For details about Web Image Monitor, see Web Image Monitor Help.

Administrator Login Method

If administrator authentication has been specified, log in using an administrator's user name and password. Supervisors log in the same way.

Logging in Using the Control Panel

1. Display the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press the [Home] key on the top left of the control panel. Flick the screen to the left, and then press the [User Tools] icon (⚙️) on the Home screen 4.

2. Display the login screen.

- When using the standard operation panel
Press the [Login/Logout] key.

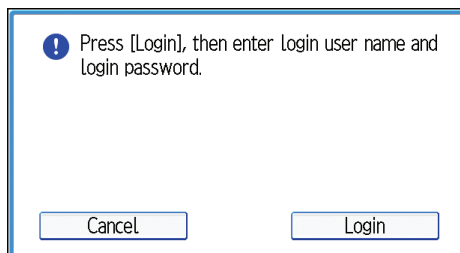


CXV044

- When using the Smart Operation Panel
Press [Login].

The login screen appears.

3. Press [Login].



4. Enter the login user name, and then press [OK].

The default login name for administrators is "admin" and "supervisor" for supervisors.

5. Enter the login password, and then press [OK].

There is no preset default password for administrators or supervisors. Therefore, leave the password field blank and press [OK].

"Authenticating... Please wait." appears, followed by the screen for specifying the default.

Note

- If user authentication has already been specified, a screen for authentication appears. To log in as an administrator, enter the administrator's login user name and login password.
- If you log in using administrator privilege, the name of the 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.
- If you try to log in from an operating screen, "You do not have the privileges to use this function. You can only change setting(s) as an administrator." appears. Press the [User Tools/Counter] key to change the default.
- When using the standard operation panel, you can display the login screen by pressing [Login] on the initial settings screen.

Logging in Using Web Image Monitor

1. Open a Web browser.**2. Enter "http://(the machine's IP address or host name)/" in the address bar.**

When entering an IPv4 address, do not begin segments with zeros. For example: If the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine.

Enter the IPv6 address with brackets before and after, like this: [2001:db8::9abc].

If you set "Permit SSL/TLS Communication" to [Ciphertext Only], enter "https://(the machine's IP address or host name)/" to access the machine.

3. Click [Login] at the top right of the window.**4. Enter the login name and password of an administrator, and then click [Login].**

The default login name for administrators is "admin" and that for supervisors is "supervisor". No login password is set up.

Note

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

Administrator Logout Method

If administrator authentication has been specified, be sure to log out after completing settings. Supervisors log out in the same way.

1

Logging out Using the Control Panel

1. Press the logout key.

- When using the standard operation panel
Press the [Login/Logout] key, and then press [Yes].
- When using the Smart Operation Panel
Press [Logout], and then press [OK].

Note

- You can log out using the following procedures also.
 - Press the [Energy Saver] key.

Logging out Using Web Image Monitor

1. Click [Logout] at the top right of the window.

Note

- Delete the cache memory in Web Image Monitor after logging out.

Supervisor

1

The supervisor can delete an administrator's password and specify a new one.

If any of the administrators forgets their password or if any of the administrators changes, the supervisor can assign a new password. If you have logged in using the supervisor's user name and password, you cannot use normal functions or specify system settings. The methods for logging in and out are the same as for administrators. See page 23 "Administrator Login Method" and page 25 "Administrator Logout Method".

★ Important

- The default login user name is "supervisor". No login password is set up. We recommend changing the login user name and login password.
- For the characters that can be used for login user names and passwords, see page 21 "Usable characters for user names and passwords".
- Be sure not to forget the supervisor login user name and login password. If you do forget them, a service representative will have to return the machine to its default state. This will result in the machine setting data, counters, logs and other data being lost; consequently, the service call may not be free of charge.

↓ Note

- You cannot specify the same login user name for the supervisor and the administrators.
- Using Web Image Monitor, you can log in as the supervisor and delete an administrator's password or specify a new one.

Resetting the Administrator's Password

1. Log in as the supervisor from the control panel.

For details on how to log in, see page 23 "Administrator Login Method".

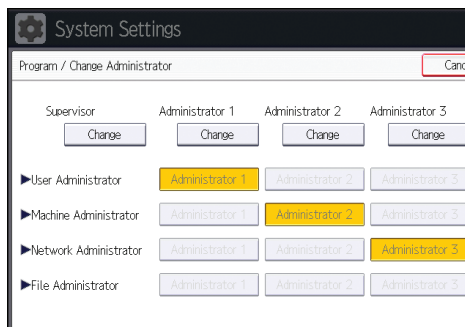
2. Press [System Settings].

3. Press [Administrator Tools].

4. Press [▼Next].

5. Press [Program / Change Administrator].

6. Press [Change] for the administrator you wish to reset.



7. Press [Change] for "Login Password".

8. Enter the login password, and then press [OK].

9. Re-enter the login password for confirmation, and then press [OK].

10. Press [OK] twice.

You will be automatically logged out.

Note

- The supervisor can change the administrators' login passwords but not their login user names.

Changing the Supervisor

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

To do this, you must enable the user administrator's privileges through the settings under "Administrator Authentication Management". For details, see page 17 "Specifying Administrator Privileges".

1. Log in as the supervisor from the control panel.

For details on how to log in, see page 23 "Administrator Login Method".

2. Press [System Settings].

3. Press [Administrator Tools].

4. Press [▼Next].

5. Press [Program / Change Administrator].

6. Under "Supervisor", press [Change].

7. Press [Change] for "Login User Name".

8. Enter the login user name, and then press [OK].

9. Press [Change] for "Login Password".

10. Enter the login password, and then press [OK].

11. Re-enter the login password for confirmation, and then press [OK].

12. Press [OK] twice.

You will be automatically logged out.

2. Configuring User Authentication

This chapter describes how to specify user authentication and explains the functions that are enabled by user authentication.

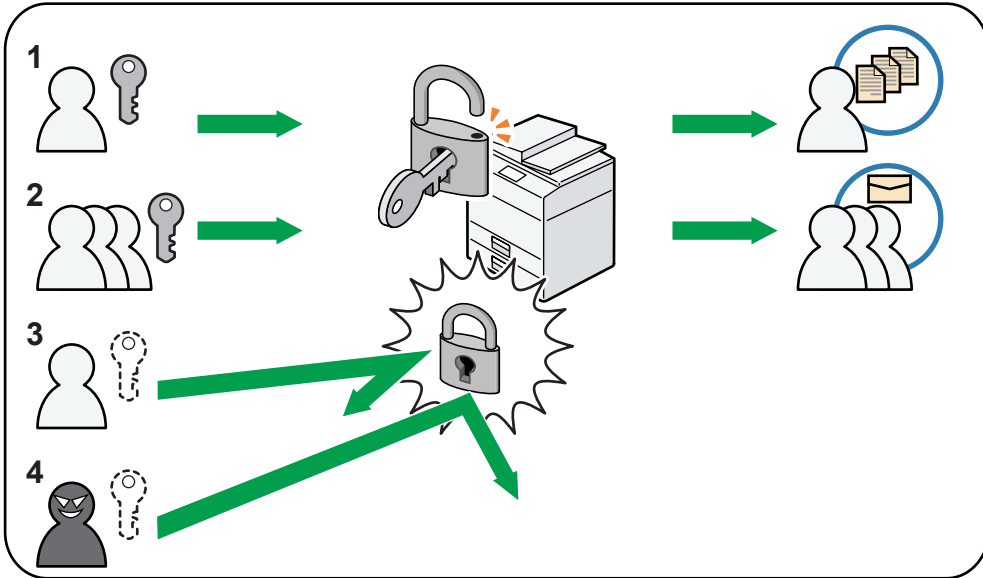
Users

A user performs normal operations on the machine, such as copying and printing. Users are managed using the information in the machine's Address Book, and can only use the functions they are permitted to access by administrators. By enabling user authentication, you can allow only people registered in the Address Book to use the machine. Users can be managed in the Address Book by the user administrator. For details about administrator, see page 15 "Administrators". For details about user registration in the Address Book, see "Registering User Information", Connecting the Machine/ System Settings or Web Image Monitor Help.

About User Authentication

User authentication is a system requiring the login user name and password for verifying users to operate the machine or access the machine over the network.

2



CJC010

1. User

A user performs normal operations on the machine, such as copying and printing.

2. Group

A group performs normal operations on the machine, such as copying and printing.

3. Unauthorized user

4. Unauthorized access

Configuring User Authentication

There are five types of user authentication methods: User Code authentication, Basic authentication, Windows authentication, LDAP authentication, and Integration Server authentication. To use user authentication, select an authentication method on the control panel, and then make the required settings for the authentication. The settings depend on the authentication method. Specify administrator authentication, and then specify user authentication.

★ Important

- If user authentication is not possible because of a problem with the hard disk or network, you can use the machine by accessing it using administrator authentication and disabling user authentication. Do this if, for instance, you need to use the machine urgently.
- You cannot use more than one authentication method at the same time.

User authentication configuration flow

Configuration procedure	Details
Configuring administrator authentication	page 17 "Specifying Administrator Privileges" page 19 "Registering and Changing Administrators"
Configuring user authentication	Specify user authentication. Five types of user authentication are available: <ul style="list-style-type: none"> • page 34 "User Code Authentication" • page 37 "Basic Authentication" • page 43 "Windows Authentication" • page 53 "LDAP Authentication" • page 58 "Integration Server Authentication"

User authentication methods

Type	Details
User Code authentication	Authentication is performed using eight-digit user codes. Authentication is applied to each user code, not to each user. It is necessary to register the user code in the machine's address book in advance.

Type	Details
Basic authentication	<p>Authentication is performed using the machine's address book.</p> <p>It is necessary to register users in the machine's address book in advance.</p> <p>Authentication can be applied to each user.</p>
Windows authentication	<p>Authentication is performed using the domain controller of the Windows server on the same network as the machine.</p> <p>Authentication can be applied to each user.</p>
LDAP authentication	<p>Authentication is performed using the LDAP server on the same network as the machine.</p> <p>Authentication can be applied to each user.</p>
Integration Server authentication	<p>Authentication is performed using an external authentication server on the same network as the machine.</p> <p>This establishes an environment in which authentication is applied collectively to users of devices (such as MFPs and computers) over the network.</p> <p>Authentication can be applied to each user.</p> <p>To create an external authentication server, software including Authentication Manager (e.g., Remote Communication Gate S) is required.</p>

A user's e-mail address obtained via Windows, LDAP, or Integration Server authentication can be used as the sender's fixed address ("From") when sending e-mails in the scanner mode or when forwarding received faxes in order to prevent ID fraud.

If the user authentication method is switched halfway

- A user code account, that has no more than eight digits and is used for User Code authentication, can be carried over and used as a login user name even after the authentication method has switched from User Code authentication to Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication. In this case, since the User Code authentication does not have a password, the login password is set as blank.
- When authentication switches to an external authentication method (Windows authentication, LDAP authentication, or Integration Server authentication), authentication will not occur, unless the external authentication device has the carried over user code account previously registered. However, the user code account will remain in the Address Book of the machine despite an authentication failure.

- From a security perspective, when switching from User Code authentication to another authentication method, we recommend that you delete accounts you are not going to use, or set up a login password. For details about deleting accounts, see "Deleting a Registered Name", Connecting the Machine/ System Settings. For details about changing passwords, see page 40 "Specifying Login User Names and Passwords".

Note

- After turning the main power on, extended features may not appear in the list of user authentication items in the User Authentication Management menu. If this happens, wait a while and then open the User Authentication Management menu again.
- User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

User Code Authentication

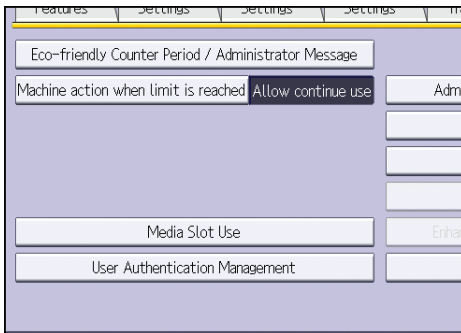
This is an authentication method for limiting access to functions according to a user code. The same user code can be used by more than one user.

For details about specifying user codes, see "Registering a User Code", Connecting the Machine/System Settings.

For details about specifying the user code on the printer driver or TWAIN driver, see the driver help.

For details about specifying the LAN-Fax driver user code, see the LAN-Fax driver Help.

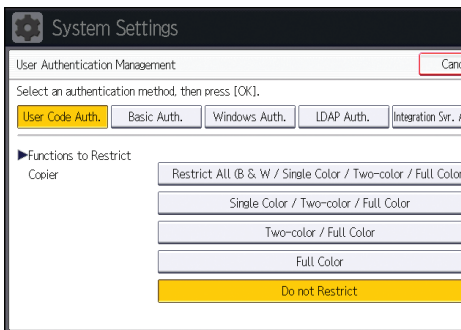
1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [User Authentication Management].



6. Select [User Code Auth.].

If you do not want to use user authentication management, select [Off].

7. In "Functions to Restrict", select the functions that you want to restrict.



If the function you want to select is not displayed, press [▼Next].

The selected functions are subject to User Code authentication. User Code authentication is not applied to the functions not selected.

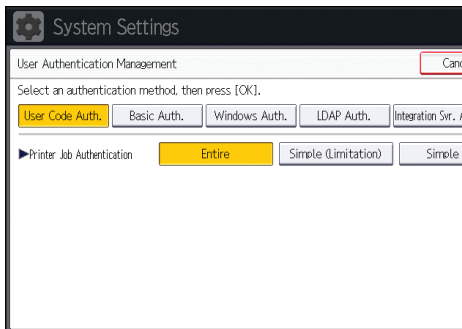
For details about limiting available functions for individuals or groups, see page 80 "Limiting Available Functions".

8. To specify printer job authentication, select an item other than [PC Control] for "Printer" under "Functions to Restrict".

If you do not want to specify printer job authentication, proceed to step 14.

9. Press [▼Next].

10. Select the "Printer Job Authentication" level.

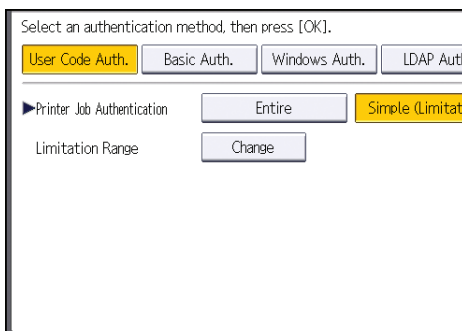


For a description of the printer job authentication levels, see page 63 "Printer Job Authentication".

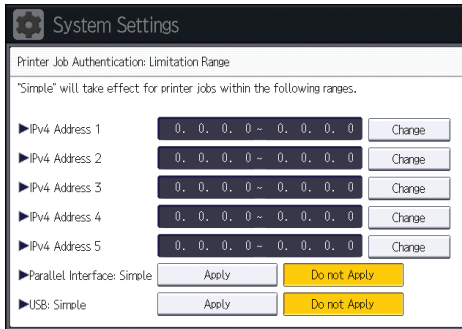
If you select [Entire] or [Simple (All)], proceed to step 14.

If you select [Simple (Limitation)], proceed to step 11.

11. Press [Change].



12. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".



You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

13. Press [Exit].

14. Press [OK].

15. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

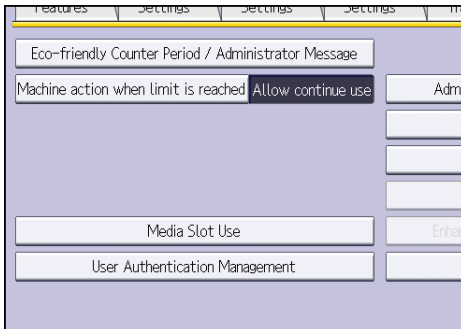
Basic Authentication

Specify this authentication method when using the machine's Address Book to authenticate each user. Using Basic authentication, you can not only manage the machine's available functions but also limit access to stored files and to the Address Book. Under Basic authentication, the administrator must specify the functions available to each user registered in the Address Book. For details about limitation of functions, see page 39 "Authentication Information Stored in the Address Book".

Specifying Basic Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

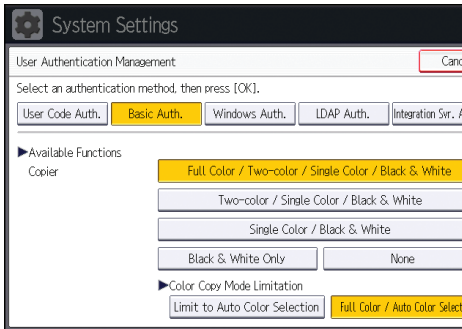
1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [User Authentication Management].



6. Select [Basic Auth.].

If you do not want to use user authentication management, select [Off].

7. In "Available Functions", select which of the machine's functions you want to permit.



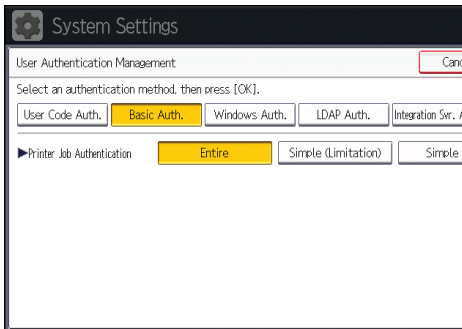
If the function you want to select is not displayed, press [▼Next].

The functions you select here become the default Basic Authentication settings that will be assigned to all new users of the Address Book.

For details about specifying available functions for individuals or groups, see page 80 "Limiting Available Functions".

8. Press [▼Next].

9. Select the "Printer Job Authentication" level.

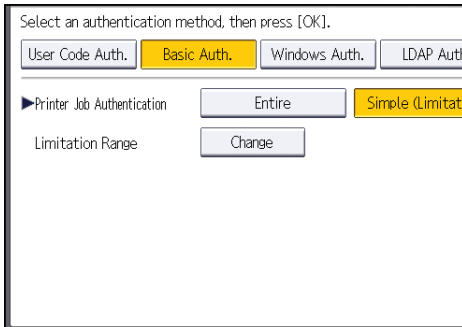


For a description of the printer job authentication levels, see page 63 "Printer Job Authentication".

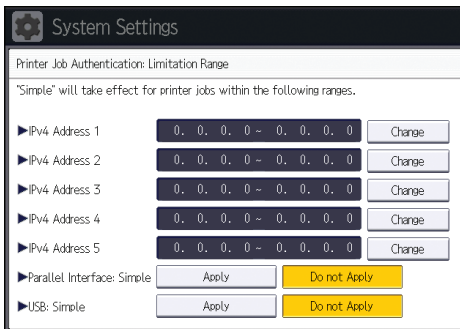
If you select [Entire] or [Simple (All)], proceed to step 13.

If you select [Simple (Limitation)], proceed to step 10.

10. Press [Change].



11. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".



You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

12. Press [Exit].

13. Press [OK].

14. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

Authentication Information Stored in the Address Book

If you have enabled user authentication, you can specify access limits and usage limits to the machine's functions for each user or group of users. Specify the necessary settings in the Address Book entry of each user. For details about limiting which functions of the machine are available, see page 80 "Limiting Available Functions".

Users must have a registered account in the Address Book in order to use the machine when user authentication is specified. For details about user registration in the Address Book, see "Registering User Information", Connecting the Machine/ System Settings.

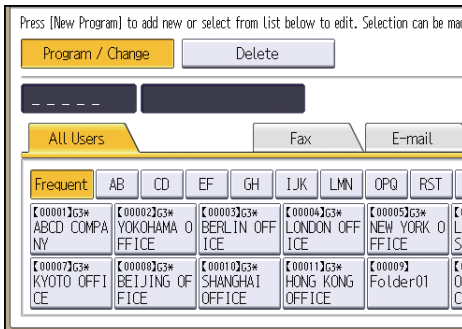
User authentication can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Specifying Login User Names and Passwords

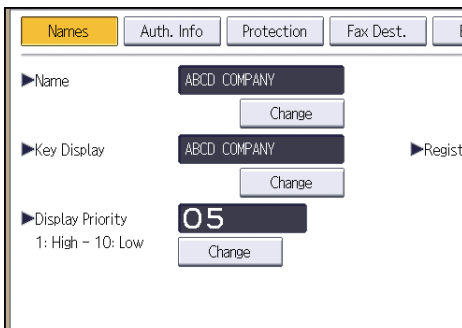
In "Address Book Management", specify the login user name and login password to be used for "User Authentication Management".

For the characters that can be used for login user names and passwords, see page 21 "Usable characters for user names and passwords".

1. Log in as the user administrator from the control panel.
2. Press [Address Book Mangmnt].
3. Select the user.



4. Press [Auth. Info].



5. Press [Change] for "Login User Name".
6. Enter a login user name, and then press [OK].
7. Press [Change] for "Login Password".

8. Enter a login password, and then press [OK].
9. Re-enter the login password for confirmation, and then press [OK].
10. Press [OK].
11. Press [Exit].
12. Log out.

↓ Note

- When using the Smart Operation Panel, you can display the Address Book screen by pressing the [Address Book Management] icon on the Home screen 4.

Specifying Login Details

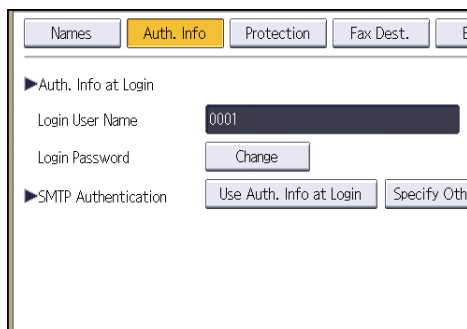
The login user name and password specified in "Address Book Management" can be used as the login information for "SMTP Authentication", "Folder Authentication", and "LDAP Authentication".

If you do not want to use the login user name and password specified in "Address Book Management" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", see "Registering Folders" and "Registering SMTP and LDAP Authentication", Connecting the Machine/ System Settings.

★ Important

- When using "Use Auth. Info at Login" for "SMTP Authentication", "Folder Authentication", or "LDAP Authentication", a user name other than "other", "admin", "supervisor" or "HIDE* **" must be specified. The symbol "* **" represents any character.

1. Log in as the user administrator from the control panel.
2. Press [Address Book Mangmnt].
3. Select the user.
4. Press [Auth. Info].
5. Select [Use Auth. Info at Login] in "SMTP Authentication".



For folder authentication, select [Use Auth. Info at Login] in "Folder Authentication".

For LDAP authentication, select [Use Auth. Info at Login] in "LDAP Authentication".

If the function you want to select is not displayed, press [▼Next].

6. Press [OK].

7. Press [Exit].

8. Log out.

↓ Note

- When using the Smart Operation Panel, you can display the Address Book screen by pressing the [Address Book Management] icon on the Home screen 4.

Windows Authentication

Specify this authentication when using the Windows domain controller to authenticate users who have their accounts on the directory server. Users cannot be authenticated if they do not have their accounts in the directory server. Under Windows authentication, you can specify the access limit for each group registered in the directory server. The Address Book stored in the directory server can be registered to the machine, enabling user authentication without first using the machine to register individual settings in the Address Book. Obtaining user information can prevent the use of false identities because the sender's address (From:) is determined by the authentication system when scanned data is sent or a received fax message is transferred via e-mail.

The first time you access the machine, you can use the functions available to your group. If you are not registered in a group, you can use the functions available under "*Default Group". To limit which functions are available to which users, first make settings in advance in the Address Book.

To automatically register user information such as fax numbers and e-mail addresses under Windows authentication, it is recommended that communication between the machine and domain controller be encrypted using SSL. To do this, you must create a server certificate for the domain controller. For details about creating a server certificate, see page 51 "Creating the Server Certificate".

Windows authentication can be performed using one of two authentication methods: NTLM or Kerberos authentication. The operational requirements for both methods are listed below.

Operational requirements for NTLM authentication

To specify NTLM authentication, the following requirements must be met:

- This machine supports NTLMv1 authentication and NTLMv2 authentication.
- A domain controller has been set up in a designated domain.
- This function is supported by the operating systems listed below. To obtain user information when running Active Directory, use LDAP. If you are using LDAP, we recommend you use SSL to encrypt communication between the machine and the LDAP server. Encryption by SSL is possible only if the LDAP server supports TLSv1 or SSLv3.
 - Windows Server 2003/2003 R2
 - Windows Server 2008/2008 R2
 - Windows Server 2012

Operational requirements for Kerberos authentication

To specify Kerberos authentication, the following requirements must be met:

- A domain controller must be set up in a designated domain.
- The operating system must support KDC (Key Distribution Center). To obtain user information when running Active Directory, use LDAP. If you are using LDAP, we recommend you use SSL to encrypt communication between the machine and the LDAP server. Encryption by SSL is possible only if the LDAP server supports TLSv1 or SSLv3. Compatible operating systems are listed below.

- Windows Server 2003/2003 R2
- Windows Server 2008/2008 R2
- Windows Server 2012

To use Kerberos authentication under Windows Server 2008, Service Pack 2 or later must be installed.

- Transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see page 175 "Kerberos Authentication Encryption Setting".

★ Important

- **During Windows Authentication, data registered in the directory server, such as the user's e-mail address, is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.**
- **Users managed in other domains are subject to user authentication, but they cannot obtain items such as e-mail addresses.**
- **If Kerberos authentication and SSL encryption are set at the same time, e-mail addresses cannot be obtained.**
- **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 to the computer and change the password.**
- **If the authenticating server only supports NTLM when Kerberos authentication is selected on the machine, the authenticating method will automatically switch to NTLM.**
- **When using Windows authentication, the login name is case sensitive. If you make a mistake, the user's login name will be added to the address book. You should delete the added user.**
- **If the "Guest" account on the Windows server is enabled, even 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".**

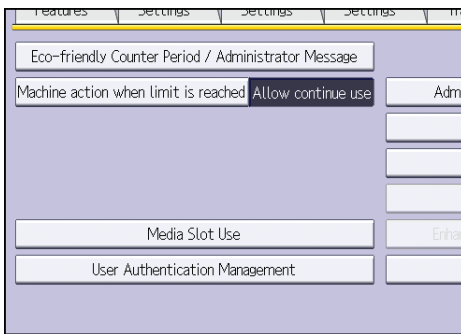
↓ Note

- For the characters that can be used for login user names and passwords, see page 21 "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.
- Users who are registered in multiple groups can use all the functions available to those groups.
- Under Windows Authentication, you do not have to create a server certificate unless you want to automatically register user information such as fax numbers and e-mail addresses using SSL.
- If you fail in obtaining fax information during authentication, see page 51 "If the Fax Number Cannot be Obtained".

Specifying Windows Authentication

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

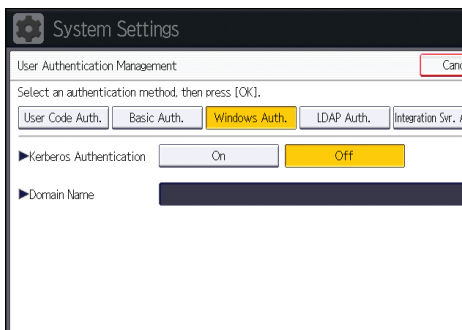
1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [User Authentication Management].



6. Select [Windows Auth.].

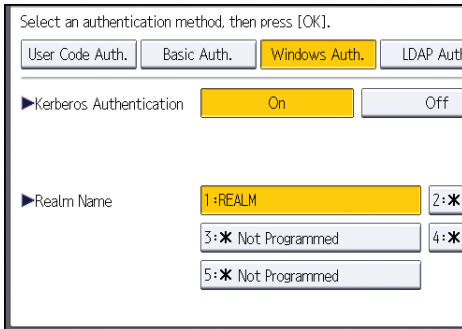
If you do not want to use user authentication management, select [Off].

7. If you want to use Kerberos authentication, press [On].



If you want to use NTLM authentication, press [Off] and proceed to step 9.

8. Select Kerberos authentication realm and proceed to step 10.



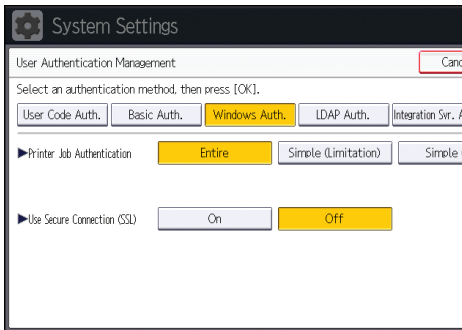
To enable Kerberos authentication, a realm must be registered beforehand. The realm name must be registered in capital letters. For details about registering a realm, see "Programming the Realm", Connecting the Machine/ System Settings.

Up to 5 realms can be registered.

9. Press [Change] for "Domain Name", enter the name of the domain controller to be authenticated, and then press [OK].

10. Press [▼Next].

11. Select the "Printer Job Authentication" level.

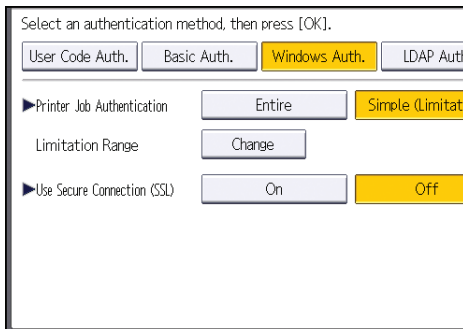


For a description of the printer job authentication levels, see page 63 "Printer Job Authentication".

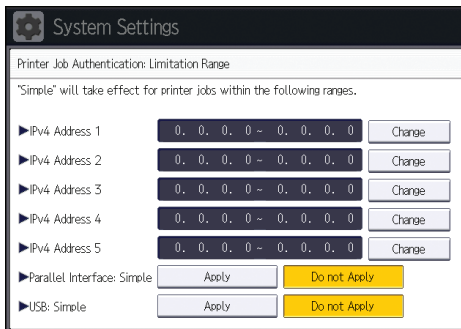
If you select [Entire] or [Simple (All)], proceed to step 15.

If you select [Simple (Limitation)], proceed to step 12.

12. Press [Change].



13. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".



You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

14. Press [Exit].

15. Press [On] for "Use Secure Connection (SSL)".

If you are not using secure sockets layer (SSL) for authentication, press [Off].

If you have not registered a global group, proceed to step 22.

If you have registered a global group, proceed to step 16.

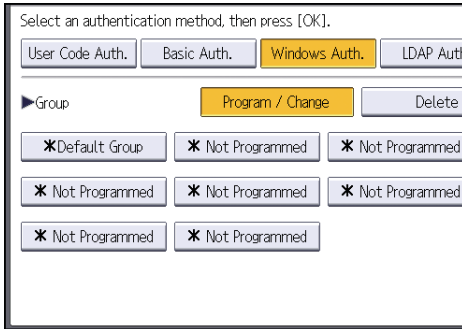
If global groups have been registered under Windows server, you can limit the use of functions for each global group.

You need to create global groups in the Windows server in advance and register in each group the users to be authenticated. You also need to register in the machine the functions available to the global group members. Create global groups in the machine by entering the names of the global groups registered in the Windows Server. (Keep in mind that group names are case sensitive.) Then specify the machine functions available to each group.

If global groups are not specified, users can use the available functions specified in [*Default Group]. If global groups are specified, users not registered in global groups can use the available functions specified in [*Default Group]. By default, all functions are available to *Default Group members. Specify the limitation on available functions according to user needs.

16. Press [▼Next].

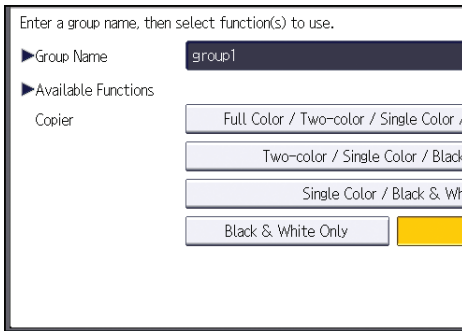
17. Under "Group", press [Program / Change], and then press [* Not Programmed].



18. Press [Change] for "Group Name", and then enter the group name.

19. Press [OK].

20. In "Available Functions", select which of the machine's functions you want to permit.



If the function you want to select is not displayed, press [▼Next].

Windows Authentication will be applied to the selected functions.

Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see page 80 "Limiting Available Functions".

21. Press [OK].

22. Press [OK].

23. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

Installing Internet Information Services (IIS) and Certificate Services

Specify this setting if you want the machine to automatically obtain e-mail addresses registered in Active Directory.

We recommend you install Internet Information Services (IIS) and Certificate services as the Windows components.

Install the components, and then create the server certificate.


If they are not installed, install them as follows:

2

Installation under Windows Server 2008 R2

1. On the [Start] menu, point to [Administrative Tools], and then click [Server Manager].
2. Click [Roles] in the left column, click [Add Roles] from the [Action] menu.
3. Click [Next>].
4. Select the "Web Server (IIS)" and "Active Directory Certificate Services" check boxes, and then click [Next>].
If a confirmation message appears, click [Add Features].
5. Read the content information, and then click [Next>].
6. Check that [Certification Authority] is checked, and then click [Next>].
7. Select [Enterprise], and then click [Next>].
8. Select [Root CA], and then click [Next>].
9. Select [Create a new private key], and then click [Next>].
10. Select a cryptographic service provider, key length, and hash algorithm to create a new private key, and then click [Next>].
11. In "Common name for this CA:", enter the Certificate Authority name, and then click [Next>].
12. Select the validity period, and then click [Next>].
13. Leave the "Certificate database location:" and the "Certificate database log location:" settings set to their defaults, and then click [Next>].
14. Read the notes, and then click [Next>].
15. Select the role service you want to use, and then click [Next>].
16. Click [Install].
17. When the installation is complete, click [Close].
18. Close [Server Manager].

Installation under Windows Server 2012

1. On the Start screen, 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.
6. Select the "Active Directory Certificate Services" and "Web Server (IIS)" check boxes, and then click [Next>].
If a confirmation message appears, click [Add Features].
7. Check the features you want to install, and then click [Next>].
8. Read the content information, and 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, and then click [Next>].
11. Check the role services you want to install under [Web Server (IIS)], and then click [Next>].
12. Click [Install].
13. After completing the installation, click the Server Manager's Notification icon , and then click [Configure Active Directory Certificate Services on the destination server].
14. Click [Next>].
15. Click [Certification Authority] in the [Role Services] area, and then click [Next>].
16. Select [Enterprise CA], and then click [Next>].
17. Select [Root CA], and then click [Next>].
18. Select [Create a new private key], and then click [Next>].
19. Select a cryptographic provider, key length, and hash algorithm to create a new private key, and then click [Next>].
20. In "Common name for this CA:", enter the Certificate Authority name, and then click [Next>].
21. Select the validity period, and then click [Next>].
22. Leave the "Certificate database location:" and the "Certificate database log location:" settings set to their defaults, and then click [Next>].
23. Click [Configure].
24. If the message "Configuration succeeded" appears, click [Close].

Creating the Server Certificate

After installing Internet Information Services (IIS) and Certificate services Windows components, create the Server Certificate as follows:

Windows Server 2008 R2 is used to illustrate the procedure.

1. On the [Start] menu, point to [Administrative Tools], and then click [Internet Information Services (IIS) Manager].

Under Windows Server 2012, click [Internet Information Services (IIS) Manager] on the Start screen.

When the confirmation message appears, click [Yes].

2. In the left column, click the server name, and then double-click [Server Certificates].
3. In the right column, click [Create Certificate Request...].
4. Enter all the information, and then 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. Close [Internet Information Services (IIS) Manager] by clicking [Finish].

If the Fax Number Cannot be Obtained

If the fax number cannot be obtained during authentication, specify the setting as follows:

Windows Server 2008 R2 is used to illustrate the procedure.

1. From the [Start] menu, point to [All Programs], click [Accessories], and then click [Command Prompt].

Under Windows Server 2012, right-click on the Start screen, click [All Apps], and then click [Command Prompt].

2. Enter "regsvr32 schmmgmt.dll", and then press the [Enter] key.
3. Click [OK], and then close the command prompt window.
4. On the [Start] menu, click [Run...].

Under Windows Server 2012, right-click on the Start page, click [All Apps], and then click [Run].

5. Enter "mmc", and then click [OK].
6. On the [File] menu, click [Add/Remove Snap-in...].
7. Select [Active Directory Scheme], and then click [Add>].
8. Click [OK].

9. Click [Active Directory Scheme] in the left column, and then open the [Attributes] folder.
10. Right-click [facsimileTelephoneNumber], and then click [Properties].
11. Select the "Replicate this attribute to the Global Catalog" check box, and then click [Apply].
12. Click [OK].
13. On the [File] menu, click [Save].
14. Specify a file name and a location in which to store the file, and then click [Save].
15. Close the console window.

LDAP Authentication

Specify this authentication method when using the LDAP server to authenticate users who have their accounts on the LDAP server. Users cannot be authenticated if they do not have their accounts on the LDAP server. The Address Book stored in the LDAP server can be registered to the machine, enabling user authentication without first using the machine to register individual settings in the Address Book. When using LDAP authentication, to prevent the password information being sent over the network unencrypted, it is recommended that communication between the machine and LDAP server be encrypted using SSL. You can specify on the LDAP server whether or not to enable SSL. To do this, you must create a server certificate for the LDAP server. For details about creating a server certificate, see page 51 "Creating the Server Certificate". The setting for using SSL can be specified in the LDAP server setting.

Using Web Image Monitor, you can enable a function that checks whether the SSL server is trustworthy when you connect to the server. For details about specifying LDAP authentication using Web Image Monitor, see Web Image Monitor Help.

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.

To enable Kerberos for LDAP authentication, a realm must be registered beforehand. The realm must be programmed in capital letters. For details about registering a realm, see "Programming the Realm", Connecting the Machine/ System Settings.

★ Important

- During LDAP authentication, the data registered in the LDAP server, such as the user's e-mail address, is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.
- Under LDAP authentication, you cannot specify access limits for groups registered in the directory 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.
- If using Active Directory in LDAP authentication when Kerberos authentication and SSL are set at the same time, e-mail addresses cannot be obtained.
- Under LDAP authentication, if "Anonymous Authentication" in the LDAP server's settings is not set to Prohibit, users who do not have an LDAP server account might still be able to gain access.
- If the LDAP server is configured using Windows Active Directory, "Anonymous Authentication" might be available. If Windows authentication is available, we recommend you use it.

Operational requirements for LDAP authentication

To specify LDAP authentication, the following requirements must be met:

- The network configuration must allow the machine to detect the presence of the LDAP server.

- When SSL is being used, TLSv1 or SSLv3 can function on the LDAP server.
- The LDAP server must be registered in the machine.
- When registering the LDAP server, the following setting must be specified.
 - Server Name
 - Search Base
 - Port Number
 - SSL communication
 - Authentication
Select either Kerberos, DIGEST, or Cleartext authentication.
 - User Name
You do not have to enter the user name if the LDAP server supports "Anonymous Authentication".
 - Password
You do not have to enter the password if the LDAP server supports "Anonymous Authentication".

For details about registering an LDAP server, see "Programming the LDAP server", Connecting the Machine/ System Settings.

 **Note**

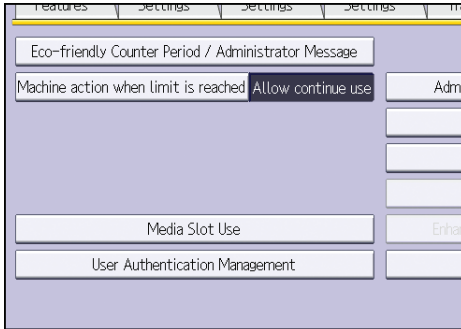
- For the characters that can be used for login user names and passwords, see page 21 "Usable characters for user names and passwords".
- In LDAP simple authentication mode, authentication will fail if the password is left blank. To allow blank passwords, contact your service representative.
- The first time an unregistered user accesses the machine after LDAP authentication has been specified, the user is registered in the machine and can use the functions available under "Available Functions" during LDAP authentication. To limit the available functions for each user, register each user and corresponding "Available Functions" setting in the Address Book, or specify "Available Functions" for each registered user. The "Available Functions" setting becomes effective when the user accesses the machine subsequently.
- Transmission between the machine and the KDC server is encrypted if Kerberos authentication is enabled. For details about specifying encrypted transmission, see page 175 "Kerberos Authentication Encryption Setting".

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**

4. Press [▼Next].

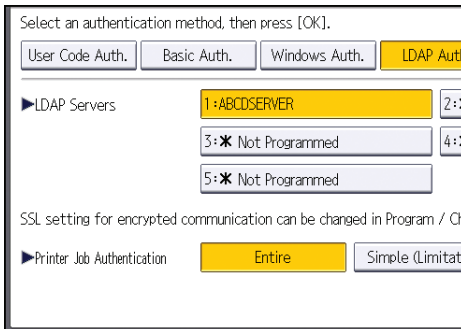
5. Press [User Authentication Management].



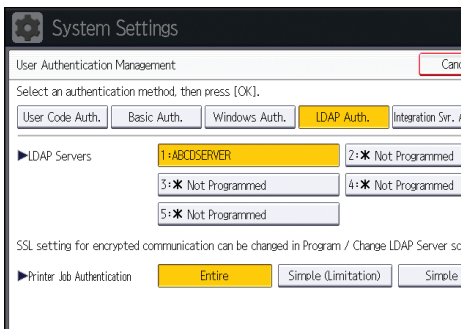
6. Select [LDAP Auth.].

If you do not want to use user authentication management, select [Off].

7. Select the LDAP server to be used for LDAP authentication.



8. Select the "Printer Job Authentication" level.

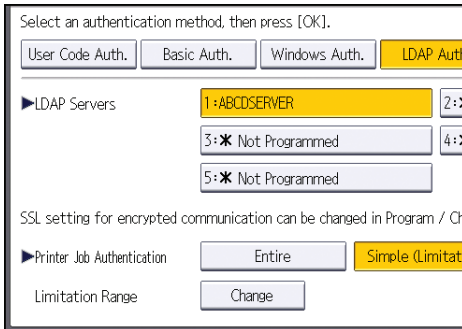


For a description of the printer job authentication levels, see page 63 "Printer Job Authentication".

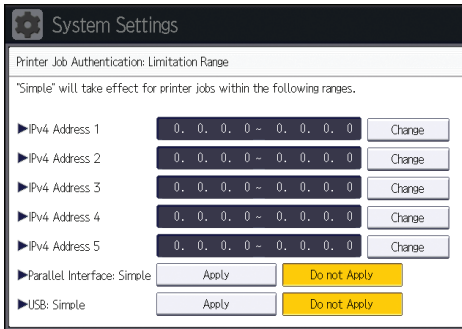
If you select [Entire] or [Simple (All)], proceed to step 12.

If you select [Simple (Limitation)], proceed to step 9.

9. Press [Change].



10. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".

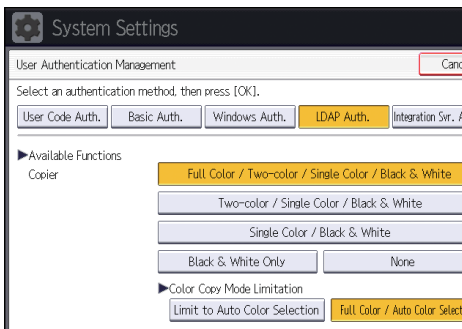


You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

11. Press [Exit].

12. Press [▼Next].

13. In "Available Functions", select which of the machine's functions you want to permit.



If the function you want to select is not displayed, press [▼Next].

LDAP authentication will be applied to the selected functions.

Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see page 80 "Limiting Available Functions".

14. Press [▼Next] to display Page 4.

15. Press [Change] for "Login Name Attribute".

16. Enter the login name attribute, and then press [OK].

Use the login name attribute as a search criterion to obtain information about an authenticated user. You can create a search filter based on the login name attribute, select a user, and then retrieve the user information from the LDAP server so it is transferred to the machine's Address Book.

To specify multiple login attributes, place a comma (,) between them. The search will return hits for either or both attributes.

Also, if you place an equals sign (=) between two login attributes (for example: cn=abcde, uid=xyz), the search will return only hits that match the attributes. This search function can also be applied when Cleartext authentication is specified.

When authenticating using the DN format, login attributes do not need to be registered.

The method for selecting the user name depends on the server environment. Check the server environment and enter the user name accordingly.

17. Press [Change] for "Unique Attribute".

18. Enter the unique attribute and then press [OK].

Specify unique attribute on the machine to match the user information in the LDAP server with that in the machine. By doing this, if the unique attribute of a user registered in the LDAP server matches that of a user registered in the machine, the two instances are treated as referring to the same user. You can enter an attribute such as "serialNumber" or "uid". Additionally, you can enter "cn" or "employeeNumber", provided it is unique. If you do not specify the unique attribute, an account with the same user information but with a different login user name will be created in the machine.

19. Press [OK].

20. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

Integration Server Authentication

For external authentication, the Integration Server authentication collectively authenticates users accessing the server over the network, providing a server-independent, centralized user authentication system that is safe and convenient.

To use the Integration Server authentication, software featuring Authentication Manager (e.g., Remote Communication Gate S) is required. For details about supported software, contact your sales representative.

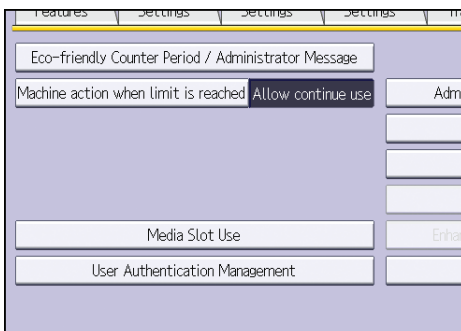
Using Web Image Monitor, you can specify that the server reliability and site certificate are checked every time you access the SSL server. For details about specifying SSL using Web Image Monitor, see Web Image Monitor Help.

★ Important

- During Integration Server Authentication, the data registered in the server, such as the user's e-mail address, is automatically registered in the machine. If user information on the server is changed, information registered in the machine may be overwritten when authentication is performed.
- The default administrator name for ScanRouter System and Remote Communication Gate S is "Admin". This is different from the default administrator name for the machine, which is "admin".

Before beginning to configure the machine, make sure that administrator authentication is properly configured under "Administrator Authentication Management".

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [User Authentication Management].



6. Select [Integration Svr. Auth.].

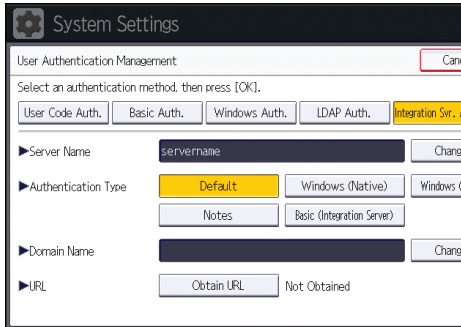
If you do not want to use user authentication management, select [Off].

7. Press [Change] for "Server Name".

Specify the name of the server for external authentication.

8. Enter the server name, and then press [OK].

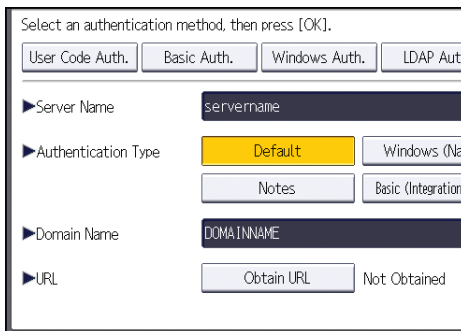
Enter the IPv4 address or host name.

9. In "Authentication Type", select the authentication system for external authentication.

Select an available authentication system. For general usage, select [Default].

10. Press [Change] for "Domain Name".**11. Enter the domain name, and then press [OK].**

You cannot specify a domain name under an authentication system that does not support domain login.

12. Press [Obtain URL].

The machine obtains the URL of the server specified in "Server Name".

If "Server Name" or the setting for enabling SSL is changed after obtaining the URL, the URL is "Not Obtained".

13. Press [Exit].

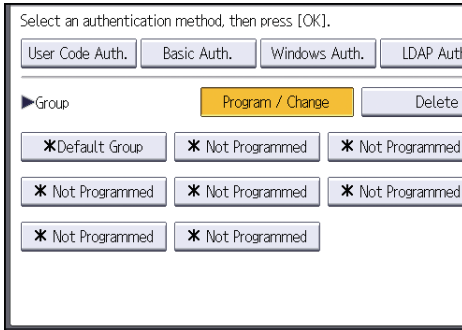
If you have not registered a group on the external authentication system being used, proceed to step 20.

If you have registered a group, proceed to step 14.

If you set "Authentication Type" to [Windows (Native)] or [Windows (NT Compatible)], you can use the global group.

If you set "Authentication Type" to [Notes], you can use the Notes group. If you set "Authentication Type" to [Basic (Integration Server)], you can use the groups created using the Authentication Manager.

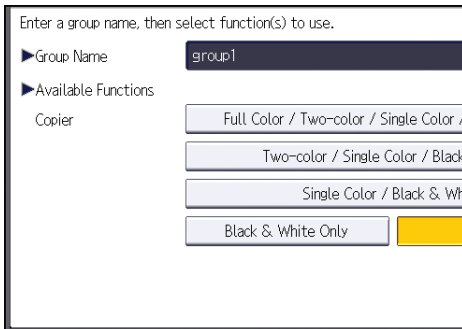
14. Press [Program / Change] for "Group", and then press [* Not Programmed].



15. Press [Change] for "Group Name", and then enter the group name.

16. Press [OK].

17. In "Available Functions", select which of the machine's functions you want to permit.



If the function you want to select is not displayed, press [▼Next].

Authentication will be applied to the selected functions.

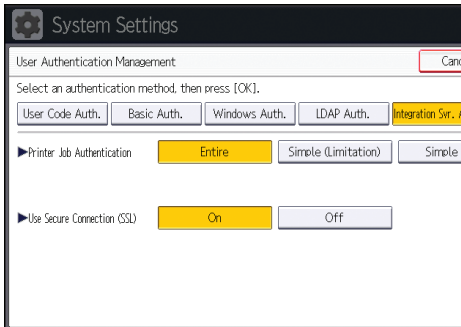
Users can use the selected functions only.

For details about specifying available functions for individuals or groups, see page 80 "Limiting Available Functions".

18. Press [OK].

19. Press [▼Next].

20. Select the "Printer Job Authentication" level.



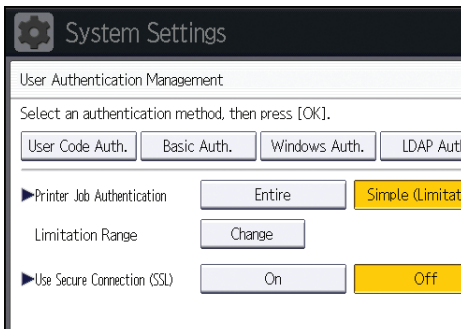
If you cannot see this item, press [▼Next] to display more settings.

For a description of the printer job authentication levels, see page 63 "Printer Job Authentication".

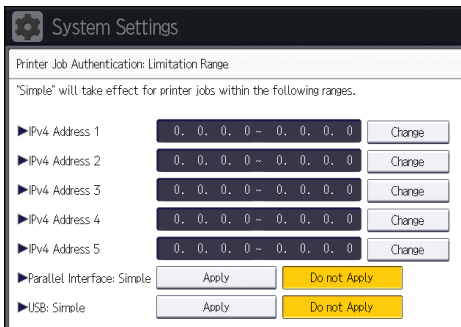
If you select [Entire] or [Simple (All)], proceed to step 25.

If you select [Simple (Limitation)], proceed to step 22.

21. Press [Change].



22. Specify the range in which [Simple (Limitation)] is applied to "Printer Job Authentication".



You can specify the IPv4 address range to which this setting is applied, and whether or not to apply the setting to the parallel and USB interfaces.

23. Press [Exit].

24. Press [On] for "Use Secure Connection (SSL)", and then press [OK].

To not use secure sockets layer (SSL) for authentication, press [Off].

25. Press [OK].

26. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

Printer Job Authentication

Printer job authentication is a function allowing user authentication to be applied to print jobs.

User authentication is supported by the PCL and PostScript3 drivers. The PostScript3 driver supports User Code authentication only.

Printer Job Authentication Levels

The security level for "Entire" is the highest, followed by "Simple (Limitation)", and at the bottom, "Simple (All)".

- Entire

Select this to authenticate all print jobs and remote configuration.

The machine authenticates all printer jobs and remote settings, and cancels jobs and settings that fail authentication.

To print in an environment that does not support authentication, select [Simple (All)] or [Simple (Limitation)].

- Simple (Limitation)

Select this to restrict the range of [Simple (All)].

The specified range can be printed regardless of the authentication. Authentication will be applied to addresses outside this range.

You can specify whether to apply [Simple (All)] to parallel connection, USB connection, and the user's IPv4 address. The range of application to IPv6 addresses can be configured from Web Image Monitor.

- Simple (All)

Select this if you want to print with a printer driver or device that cannot be identified by the machine or if authentication is not required for printing.

Printer jobs and settings without authentication information are performed without being authenticated.

The machine authenticates printer jobs and remote settings that have authentication information, and cancels the jobs and settings that fail authentication.

Unauthorized users may be able to use the machine since printing is allowed without user authentication.

Printer Job Types

Depending on the combination of printer job authentication level and printer job type, the machine may not print properly. Set an appropriate combination according to the operating environment.

When user authentication is disabled, printing is possible for all job types.

Printer job types: A printer job is specified when:

1. The [User Authentication] check box is selected in the PCL printer driver or in the PCL universal driver.
2. The [User Authentication] and [With Encryption] check boxes are selected in the PCL mini-driver*.
 - * The authentication function cannot be used with IA-64 OS.
3. The [User Authentication] check box is selected in the PCL mini-driver.
4. The [User Authentication] check box is not selected in the PCL printer driver or in the PCL mini-driver*.
 - * The authentication function cannot be used with IA-64 OS.
5. When the User Code is entered using the PostScript 3 printer driver or PS3 universal driver. This also applies to recovery/parallel printing using a PCL printer driver that does not support authentication.
6. When the User Code is not entered using the PostScript 3 printer driver or PS3 universal driver. This also applies to recovery/parallel printing using a PCL printer driver that does not support authentication.
7. A printer job or PDF file is sent from a host computer that does not have a printer driver and is printed via LPR or PictBridge. This can be also applied to Mail to Print. For details about Mail to Print, see "Receiving E-mail by Internet Fax/Mail to Print", Fax.
8. A PDF file is printed via ftp. Personal authentication is performed using the user ID and password used for logging in via ftp. However, the user ID and password are not encrypted.

Printer job authentication levels and printer job types

Printer Job Authentication	Simple (All)	Simple (All)	Simple (All)	Entire	Entire	Entire
Driver Encryption Key:Encryption Strength	Simple Encryption	DES	AES	Simple Encryption	DES	AES
Printer Job Type 1	C*1	C*1	C*1	C*1	C*1	C*1
Printer Job Type 2	C*1	C*1	X*1	C*1	C*1	X*1

Printer Job Authentication	Simple (All)	Simple (All)	Simple (All)	Entire	Entire	Entire
Driver Encryption Key:Encryption Strength	Simple Encryption	DES	AES	Simple Encryption	DES	AES
Printer Job Type 3	B	X*1	X*1	B	X*1	X*1
Printer Job Type 4	X	X	X	X	X	X
Printer Job Type 5	A	A	A	B	B	B
Printer Job Type 6	A	A	A	X	X	X
Printer Job Type 7	A	A	A	X	X	X
Printer Job Type 8	B	B	B	B	B	B

*1 Printing with User Code authentication is classified as B.

A: Printing is possible regardless of user authentication.

B: Printing is possible if user authentication is successful. If user authentication fails, the print job is reset.

C: Printing is possible if user authentication is successful and "Driver Encryption Key" for the printer driver and machine match.

X: Printing is not possible regardless of user authentication, and the print job is reset.

Note

- For details about "Driver Encryption Key:Encryption Strength", see page 257 "Specifying the Extended Security Functions".

"authfree" Command

If [Simple (Limitation)] is selected under printer job authentication, the telnet authfree command can be used to specify exceptions to the printer job authentication.

The default user name for logging into telnet is "admin". The password is not configured by default. For details about logging into and using telnet, see "Remote Maintenance Using telnet", Connecting the Machine/ System Settings.

View settings

```
msh> authfree
```

If print job authentication exclusion is not specified, authentication exclusion control is not displayed.

IPv4 address settings

```
msh> authfree "ID" range "start-address" "end-address"
```

IPv6 address settings

```
msh> authfree "ID" range6 "start-address" "end-address"
```

IPv6 address mask settings

```
msh> authfree "ID" mask6 "base-address" "masklen"
```

Parallel/USB settings

```
msh> authfree [parallel|usb] [on|off]
```

- To exclude parallel and USB connections from printer job authentication, set this to "on". The default setting is "off".
- Always specify either "parallel" or "USB".

"parallel" can be specified when an optional IEEE 1284 interface board is installed.

Authentication exclusion control initialization

```
msh> authfree flush
```

Note

- In both IPv4 and IPv6 environments, up to five access ranges can be registered and selected.

Auto Registration to the Address Book

The personal information of users logging in via Windows, LDAP or Integration Server authentication is automatically registered in the Address Book. Any other information may be specified by copying from other registered users.

2

Automatically Registered Address Book Items

- Login User Name
- Login Password
- Registration No.
- Name *¹
- Key Display *¹
- E-mail Address *²
- Protect File(s)
Permissions for Users / Groups *³

*¹ If this information cannot be obtained, the login user name is registered in this field.

*² If this information cannot be obtained, auto registration does not work.

*³ If [Data Carry-over Setting for Address Book Auto-program] is set to [Carry-over Data], it has priority.

Note

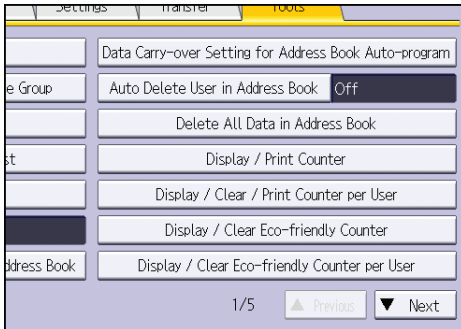
- You can automatically delete old user accounts when performing auto registration if the amount of data registered in the address book has reached the limit. For details, see page 256 "Managing the Address Book".

Data Carry-over Setting for Address Book Auto-program

Information that is not automatically registered in the Address Book can be copied from an already registered user and then registered.

1. Log in as the user administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].

4. Press [Data Carry-over Setting for Address Book Auto-program].



5. Press [Carry-over Data].

6. Use the number keys to enter the registration number of the Address Book to apply the specified setting, and then press [#].

7. Press [OK].

8. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

User Lockout Function

If an incorrect password is entered several times, the User Lockout function prevents further login attempts under the same user name. Even if the locked out user enters the correct password later, authentication will fail and the machine cannot be used until the lockout period elapses or an administrator or supervisor disables the lockout.

To use the lockout function for user authentication, the authentication method must be set to Basic authentication. Under other authentication methods, the lockout function protects supervisor and administrator accounts only, not general user accounts.

Lockout setting items

The lockout function settings can be made using Web Image Monitor.

Setting item	Description	Setting values	Default setting
Lockout	Specify whether or not to enable the lockout function.	<ul style="list-style-type: none"> Active Inactive 	<ul style="list-style-type: none"> Inactive
Number of Attempts before Lockout	Specify the number of authentication attempts to allow before applying lockout.	1-10	5
Lockout Release Timer	Specify whether or not to cancel lockout after a specified period elapses.	<ul style="list-style-type: none"> Active Inactive 	<ul style="list-style-type: none"> Inactive
Lock Out User for	Specify the number of minutes after which lockout is canceled.	1-9999 min.	60 min.

Lockout release privileges

Administrators with unlocking privileges are as follows.

Locked out user	Unlocking administrator
general user	user administrator
user administrator, network administrator, file administrator, machine administrator	supervisor

Locked out user	Unlocking administrator
supervisor	machine administrator

Specifying the User Lockout Function

2

1. Log in as the machine administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [User Lockout Policy] under "Security".
4. Set "Lockout" to [Active].
5. In the drop-down menu, select the number of login attempts to permit before applying lockout.
6. After lockout, if you want to cancel lockout after a specified time elapses, set "Lockout Release Timer" to [Active].
7. In the "Lock Out User for" field, enter the number of minutes until lockout is disabled.
8. Click [OK].
User Lockout Policy is set.
9. Log out.

Canceling Password Lockout

1. Log in as the user administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Address Book].
3. Select the locked out user's account.
4. Click [Detail Input], and then click [Change].
5. Set "Lockout" to [Inactive] under "Authentication Information".
6. Click [OK].
7. Log out.

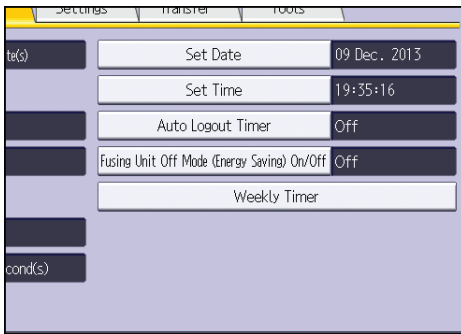
Note

- You can cancel the administrator and supervisor password lockout by turning the main power off and then turning it back on again, or by canceling the setting in [Program/Change Administrator] under [Configuration] in Web Image Monitor.

Auto Logout

After you log in, the machine automatically logs you out if you do not use the control panel within a given time. This feature is called "Auto Logout". Specify how long the machine is to wait before performing Auto Logout.

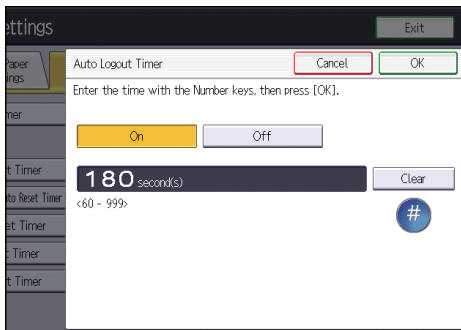
1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Timer Settings].
4. Press [Auto Logout Timer].



5. Select [On].

If you do not want to specify [Auto Logout Timer], select [Off].

6. Enter "60" to "999" (seconds) using the number keys, and then press [#].



If you make a mistake, press [Clear].

7. Press [OK].
8. Log out.

- When using the standard operation panel

Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.

- When using the Smart Operation Panel

Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

 **Note**

- If a paper jam occurs or toner runs out, the machine might not be able to perform the Auto Logout function.
- You can specify the Auto Logout setting for Web Image Monitor in [Webpage]. For details, see the Web Image Monitor Help.

Authentication Using an External Device

To authenticate using an external device, see the device manual.

For details, contact your sales representative.

3. Restricting Machine Usage

This chapter explains how to restrict use of the machine by the user.

Restricting Usage of the Destination List

The use of the destination list can be restricted separately under the scanner and fax functions.

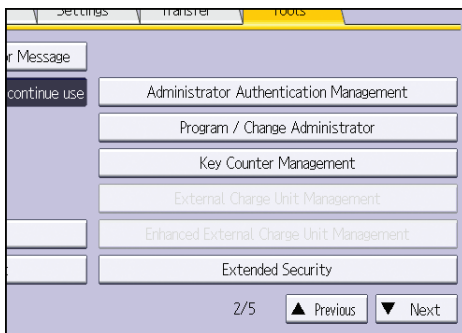
Restrict Use of Destinations (Fax), Restrict Use of Destinations (Scanner)

You can prohibit the sending of faxes and scanned documents to addresses other than those registered in the Address Book. By enabling this, you can prohibit users from manually entering the other party's fax number, e-mail address or folder destination.

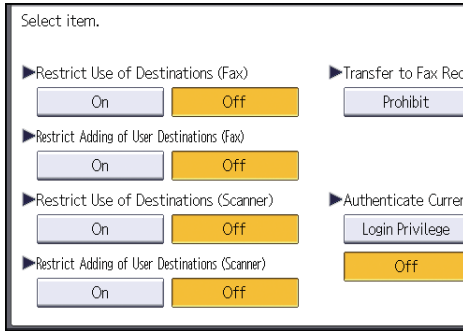
Restrict Adding of User Destinations (Fax), Restrict Adding of User Destinations (Scanner)

With regard to the addresses manually entered for sending faxes or scanned documents, you can prohibit their registration into the Address Book using [Prg. Dest.]. Also note that with this setting, only the user administrator can register new users in the Address Book and change the passwords and other information of existing registered users. Also, note that even if you set these functions to [On], the user registered as destination can change their password. Only the user administrator can change items other than the password.

1. Log in as the user administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [Extended Security].



6. Press [▼Next].
7. Set "Restrict Use of Destinations" or "Restrict Adding of User Destinations" to [On].
Specify these settings for both the fax and the scanner functions.



3

If you set "Restrict Use of Destinations (Fax)" to [On], "Restrict Adding of User Destinations (Fax)" will not appear. Similarly, if you set "Restrict Use of Destinations (Scanner)" to [On], "Restrict Adding of User Destinations (Scanner)" will not appear.

8. Press [OK].

9. Log out.

- When using the standard operation panel
Press the [Login/Logout] key. A confirmation message appears. If you press [Yes], you will be automatically logged out.
- When using the Smart Operation Panel
Press [Logout]. A confirmation message appears. If you press [OK], you will be automatically logged out.

Preventing Changes to Administrator Settings

Limiting the Settings that Can Be Changed by Each Administrator

The settings that can be made for this machine vary depending on the type of administrator, allowing the range of operations that can be made to be divided among the administrators.

The following administrators are defined for this machine.

- User administrator
- Machine administrator
- Network administrator
- File administrator

For details on the settings that can be made by each administrator, see page 295 "List of Operation Privileges for Settings".

Register the administrators before using the machine. For instructions on registering the administrator, see page 19 "Registering and Changing Administrators".

Prohibiting Users from Making Changes to Settings

Makes it possible to prohibit users from changing administrator settings.

Select the item under "Available Settings" in "Administrator Authentication Management" to prevent such changes.

For details on selections in "Available Settings", see page 16 "Configuring Administrator Authentication".

Specifying Menu Protect

Menu Protect allows you to limit user permission to access the settings in the User Tools menu except for the System Settings. This setting can be used regardless of user authentication. To change the menu protect setting, first enable administrator authentication. For details on how to set administrator authentication, see page 16 "Configuring Administrator Authentication". For a list of settings that users can specify according to the menu protect level, see page 295 "List of Operation Privileges for Settings".

3

If you want to enable "Menu Protect", specify it to [Level 1] or [Level 2]. Select [Level 2] to impose stricter restrictions on users' access permission to the machine settings.

If you want to disable "Menu Protect", specify it to [Off].

Copy Function

1. Log in as the machine administrator from the control panel.
2. Press [Copier / Document Server Features].
3. Press [Administrator Tools].
4. Press [Menu Protect].
5. Select the menu protect level, and then press [OK].
6. Log out.

Fax Function

1. Log in as the machine administrator from the control panel.
2. Press [Facsimile Features].
3. Press [Initial Settings].
4. Press [Menu Protect].
5. Select the menu protect level, and then press [OK].
6. Log out.

Printer Function

1. Log in as the machine administrator from the control panel.
2. Press [Printer Features].
3. Press [Data Management].

4. Press [Menu Protect].
5. Select the menu protect level, and then press [OK].
6. Log out.

Scanner Function

1. Log in as the machine administrator from the control panel.
2. Press [Scanner Features].
3. Press [Initial Settings].
4. Press [Menu Protect].
5. Select the menu protect level, and then press [OK].
6. Log out.

Limiting Available Functions

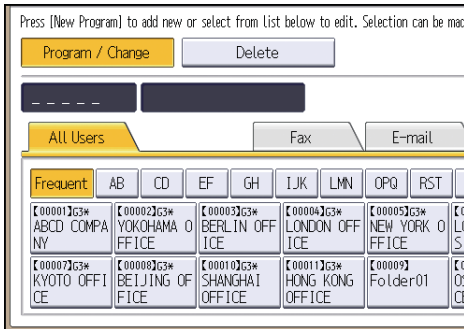
To prevent unauthorized operation, you can specify who is allowed to access each of the machine's functions.

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

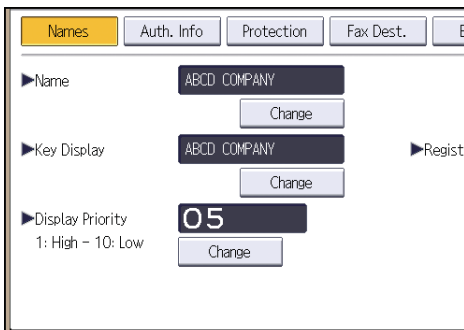
You can place limitations on the use of the copier, Document Server, fax, scanner, printer, browser functions, and extended features.

3

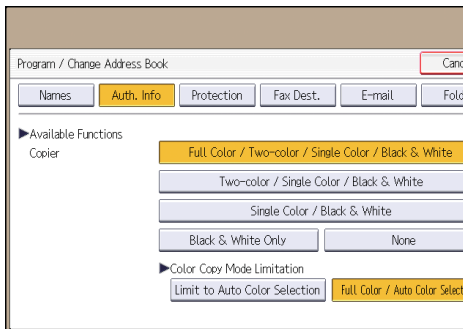
1. Log in as the user administrator from the control panel.
2. Press [Address Book Mangmnt].
3. Select the user.



4. Press [Auth. Info].



5. Press [▼Next] twice.

6. In "Available Functions", select the functions you want to specify.

If the function you want to select is not displayed, press [▼Next].

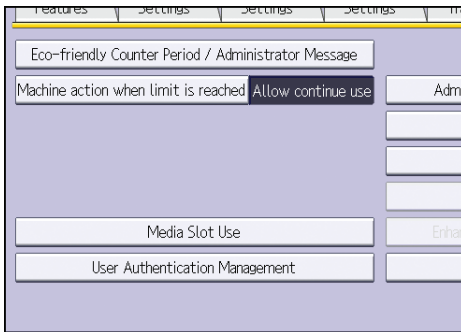
7. Press [OK].**8. Log out.****Note**

- When using the Smart Operation Panel, you can display the Address Book screen by pressing the [Address Book Management] icon on the Home screen 4.

Restricting Media Slot Access

Specify on the control panel whether or not to allow users to use the media slots. With this setting, you can restrict storing scanned files on a removable memory device, and also restrict printing of files stored on a removable memory device.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [Media Slot Use].



6. To restrict storing files on a removable memory device, press [Prohibit] under "Store to Memory Device".
7. To restrict printing of files stored on a removable memory device, press [Prohibit] under "Print from Memory Storage Device".
8. Press [OK].
9. Log out.

↓ Note

- If you select [Prohibit] under "Store to Memory Device", the [Store to Memory Device] button is not displayed on the Store File screen of the scanner function.
- If you select [Prohibit] under "Print from Memory Storage Device", the [Print from Memory Storage Device] button is not displayed on the printer function's initial screen.

Managing Print Volume per User

This function limits how much each user can print. If users reach their maximum print volume, their print jobs are canceled and/or a message indicating so is displayed.

Print volume

The print volume is calculated by multiplying the number of pages by a unit count.

The unit count can be specified according to the printing condition. For example, if one page is printed with a unit count of 10, the print volume would be 10.

The print volume is tracked for each user.

3

Setting Items

Item	Explanation	Setting
Machine action when limit is reached	<p>Specify whether to limit print volume and the method for limiting prints.</p> <ul style="list-style-type: none"> • Stop Job When the maximum print volume is reached, both the current job and waiting jobs are canceled. • Finish Job and Limit When the maximum print volume is reached, the current job is allowed to finish, but waiting jobs are canceled. • Allow Continue Use Print volume is not limited. 	<ul style="list-style-type: none"> • Stop Job • Finish Job and Limit • Allow Continue Use (Default setting)

Item	Explanation	Setting
Print Volume Use Limitation: Unit Count Setting	<p>You can specify the limits for the print volume per user under the following eight conditions.</p> <ul style="list-style-type: none"> • Copier:Color:A3/DLT • Copier:Black & White:A3/DLT • Printer:Color:A3/DLT • Printer:Black & White:A3/DLT • Copier:Color:Others • Copier:Black & White:Others • Printer:Color:Others • Printer:Black & White:Others <p>The default per-page unit count for every print condition is 1.</p> <p>The paper size "Others" refers to paper sizes other than A3 and DLT (11 × 17 in).</p>	<p>0 to 200</p> <p>(The default per-page unit count for every print condition is 1.)</p>

Things to note when limiting print volume

If the following occurs, the user will not be able to print:

- The login user name or user code registered in the Address Book is changed while the user is logged in and authenticated.

If the following occurs, print volume management will not function correctly:

- Under Windows or LDAP authentication, a user logs in to the same user account by using multiple login user names, and these multiple login names are registered in the Address Book as separate users.

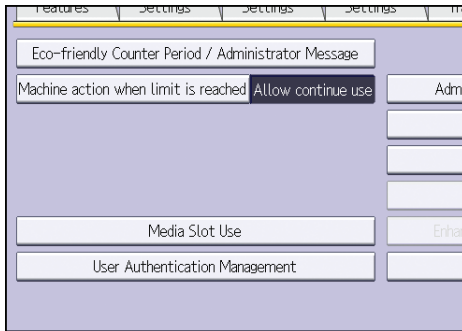
The following operations are exempt from print volume limitation:

- Printing from an operating system that does not support the current authentication method
- Printing data using the Mail to Print function, received faxes, LAN-Fax data, and files stored using the fax function

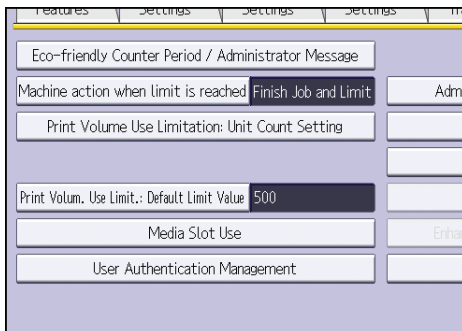
Specifying Limitations for Print Volume

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].

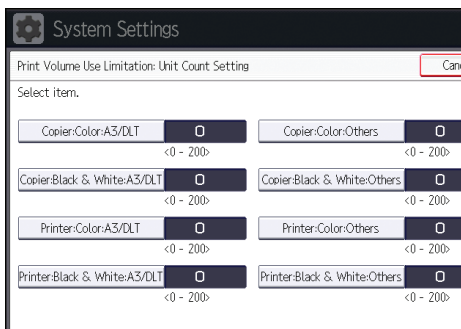
4. Press [▼Next].
5. Press [Machine action when limit is reached].



6. Select [Stop Job] or [Finish Job and Limit], and then press [OK].
If you do not want to limit print volume, select [Allow Continue Use].
7. Press [Print Volume Use Limitation: Unit Count Setting].



8. For each print condition, use the number keys to enter a per-page unit count between "0" and "200", and then press [#].



If you specify "0" for a print condition, no volume restriction is applied to jobs matching that condition.

9. Press [OK].
10. Log out.

Note

- Limitations for print volume can also be specified in [Print Volume Use Limitation] under "Configuration" in Web Image Monitor.

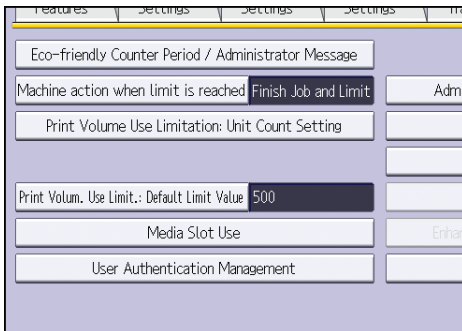
Restrictions When User Code Authentication is Enabled

When User Code authentication is enabled, the following restrictions apply to the print volume limitation settings:

- If [PC Control] is selected for the printer function, the values specified for print volume use units might not be applied to users' print counters. Do not select [PC Control] if you want to limit print volume when running User Code authentication.
- Under Basic, Windows, and LDAP authentication, figures displayed on the lower left of the control panel show users how many of the total prints allotted to them by the administrator they have used. Under User Code authentication, users cannot check the print volume they have made, using either the control panel or Web Image Monitor. Under User Code authentication, administrators can inform users of the print volume they have made.
- Log information related to print use limitations is not recorded in the Job Log or Access Log.
- Depending on the settings configured for User Code authentication, users might be able to make prints before logging in, regardless of the print volume limitation set by the administrator. Restrict all functions via "Functions to Restrict" in [User Code Auth.] in [User Authentication Management].

Specifying the Default Maximum Use Count

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [Print Volum. Use Limit.: Default Limit Value].



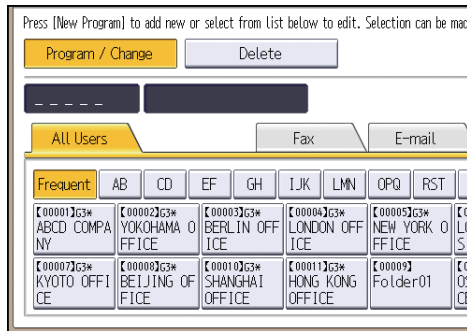
[Print Volum. Use Limit.: Default Limit Value] does not appear if you have selected [Allow Continue Use] in "Machine action when limit is reached".

6. Use the number keys to enter a value between "0" and "999,999" as the maximum available print volume, and then press [#].
7. Press [OK].
8. Log out.

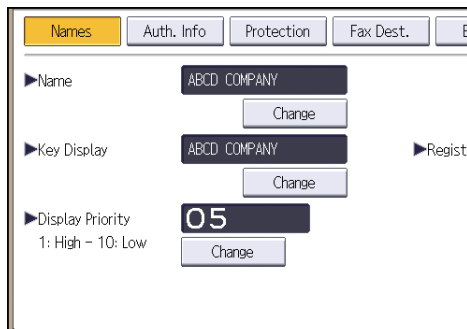
Specifying the Maximum Use Count per User

3

1. Log in as the machine administrator from the control panel.
2. Press [Address Book Mangmnt].
3. Select the user whose maximum available print volume you want to specify.

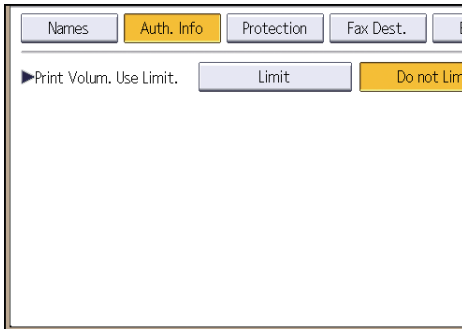


4. Press [Auth. Info].



5. Press [▼Next] four times.

6. Press [Limit] in "Print Volum. Use Limit."



3

"Print Volum. Use Limit." does not appear if you have selected [Allow Continue Use] in "Machine action when limit is reached".

If you do not want to limit user's print volume, press [Do not Limit].

7. Press [Change], and then use the number keys to enter a value between "0" and "999,999" as the maximum available print volume, and then press [#].

A user whose maximum print volume is set to "0" can only print jobs whose print conditions match those with a unit value of "0".

8. Press [OK].

9. Log out.

Note

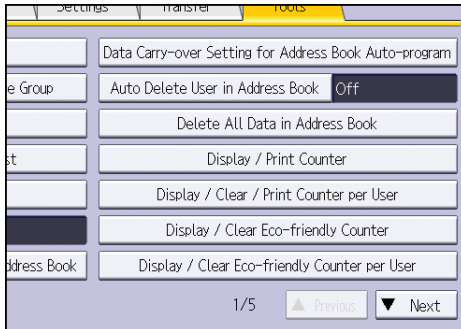
- The maximum print volume for an individual user can also be specified in [Address Book] in Web Image Monitor.
- When using the Smart Operation Panel, you can display the Address Book screen by pressing the [Address Book Management] icon on the Home screen 4.

Checking Print Volume per User

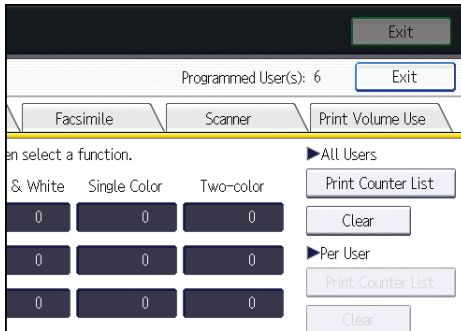
This procedure can be done by any administrator.

- 1. Log in as the administrator from the control panel.**
- 2. Press [System Settings].**
- 3. Press [Administrator Tools].**

4. Press [Display / Clear / Print Counter per User].



5. Press [Print Volume Use].



Each user's print volume limit and print volume used to date are displayed.

6. After confirming the settings, log out.

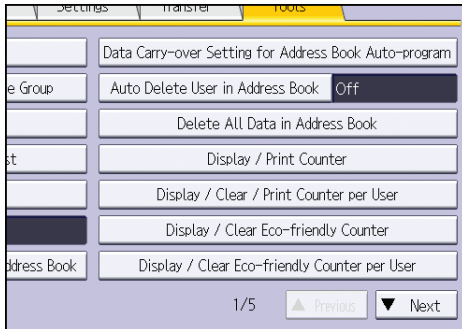
Note

- Authorized users and the user administrator can also use [Address Book] in Web Image Monitor to check users' print volume use counters.

Printing a List of Print Volume Use Counters

- Log in as the machine administrator from the control panel.
- Press [System Settings].
- Press [Administrator Tools].

4. Press [Display / Clear / Print Counter per User].

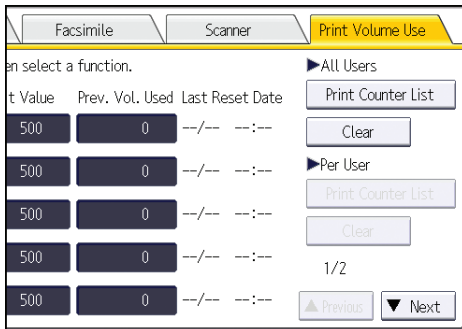


5. Press [Print Volume Use].

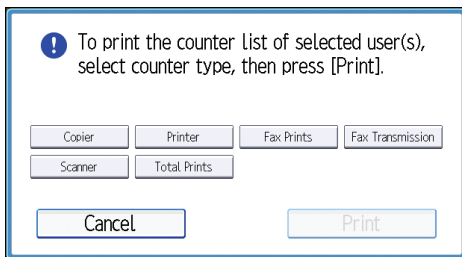
A list of users' print volume use counters is displayed.

To select all the users displayed on the page, press [Select All on the Page].

6. To print a list of the volume use counters of every user, press [Print Counter List] under "All Users". To print a list of the volume use counters of selected users only, select the users whose counters you want to print, and then press [Print Counter List] under "Per User".



7. Select the counter you want to print in the list, and then press [Print].



8. Log out.

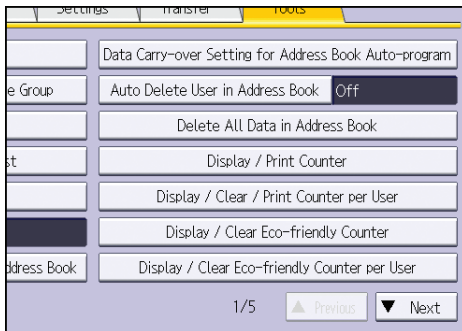
Note

- Print volume use counter lists can be printed only if the following paper sizes is loaded in the paper tray: A4, 8 1/2 × 11 in, B4, 8 1/2 × 14 in, A3, or 11 × 17 in.

Clearing Print Volume Use Counters

Clearing a user's print volume counter or increasing a user's print volume limit allows the user to continue printing beyond his/her original print volume limit.

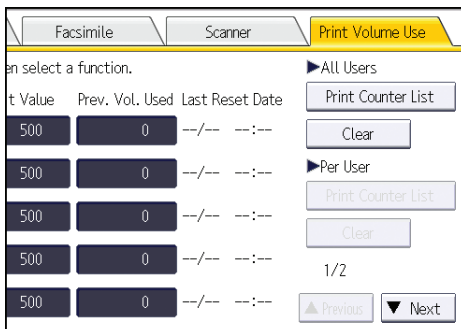
1. Log in as the user administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Display / Clear / Print Counter per User].



5. Press [Print Volume Use].

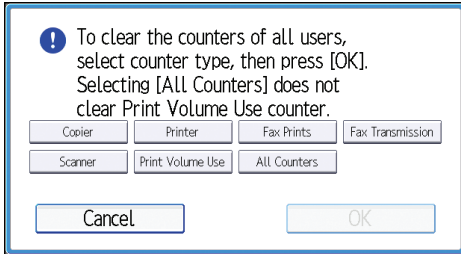
A list of users' print volume use counters is displayed.

6. To clear the print volume use counters of every user, press [Clear] under "All Users". To clear the print volume use counters of selected users only, select the users whose counters you want to clear, and then press [Clear] under "Per User".



To select all the users displayed on the page, press [Select All on the Page].

7. Select [Print Volume Use], and then press [OK].



8. Log out.

Note

- You can also use [Address Book] in Web Image Monitor to clear the print volume use counters. However if you want to clear the print volume use counters of all users simultaneously, use the control panel.

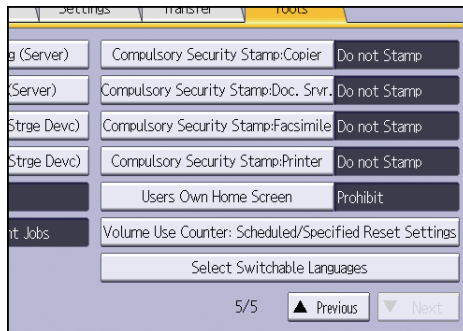
Configuring the Auto-Reset Function

The print volume counter can be reset at a specified time.

Options	Details
Every Month	Resets the print volume at the specified time/date each month.
Specify Date	Resets the print volume (only once) at the specified time/date.
Specify Cycle	Resets after the specified interval from a reference date, then resets thereafter at the same interval.

- 1. Log in as the machine administrator from the control panel.**
- 2. Press [System Settings].**
- 3. Press [Administrator Tools].**
- 4. Press [▼Next] four times.**

5. Press [Volume Use Counter: Scheduled/Specified Reset Settings].



6. Select one of [Every Month], [Specify Date] and [Specify Cycle].

7. Configure the conditions.

8. Press [OK].

9. Log out.

Note

- If the machine is turned off at the specified time on the specified date, the print volume will be reset when the power is turned on.
- If you select in [Every Month] a date, such as the 31st, which is missing on some months, the print volume will be reset at 0:00 on the 1st of the month following such a month.

4. Preventing Leakage of Information from Machines

This chapter explains how to protect information if it is stored in the machine's memory or on the hard disk.

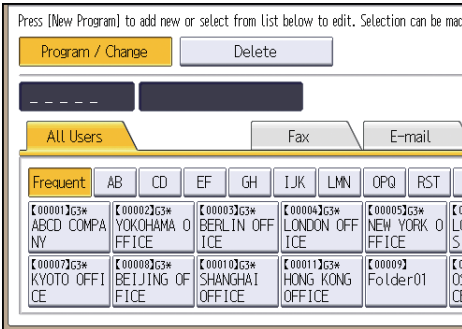
Protecting the Address Book

You can specify who is allowed to access the data in the Address Book. To protect the data from unauthorized reading, you can also encrypt the data in the Address Book.

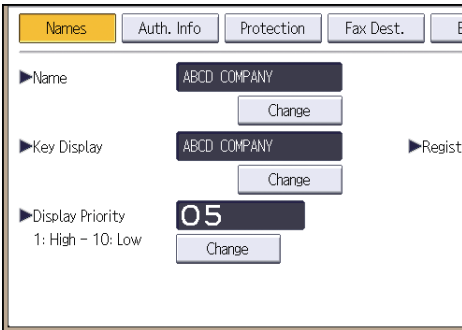
Specifying Address Book Access Permissions

These access permissions can be specified by the users registered in the Address Book, users with full control privileges, and user administrator.

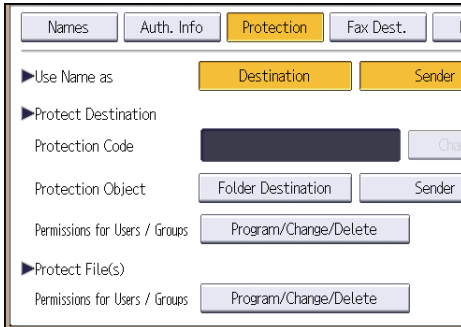
- 1. Log in as the user administrator from the control panel.
- 2. Press [Address Book Mangmnt].
- 3. Select the user whose access permission you want to change.



- 4. Press [Protection].

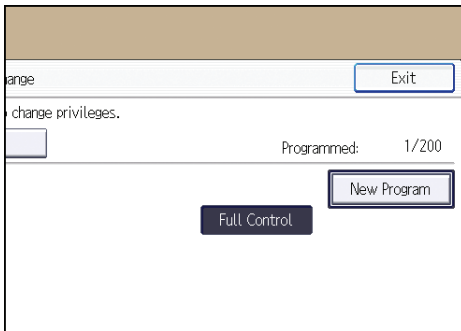


5. Press [Program/Change/Delete] for "Permissions for Users / Groups", under "Protect Destination".



4

6. Press [New Program].



7. Select the users or groups to which to apply the access permission.

You can select more than one user.

By pressing [All Users], you can select all the users.

8. Press [Exit].

9. Select the user to whom you want to assign access permission, and then select the permission.

Select the permission, from [Read-only], [Edit], [Edit / Delete], or [Full Control].

10. Press [Exit].

11. Press [OK].

12. Log out.

↓ Note

- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.
- When using the Smart Operation Panel, you can display the Address Book screen by pressing the [Address Book Management] icon on the Home screen 4.

Encrypting Data in the Address Book

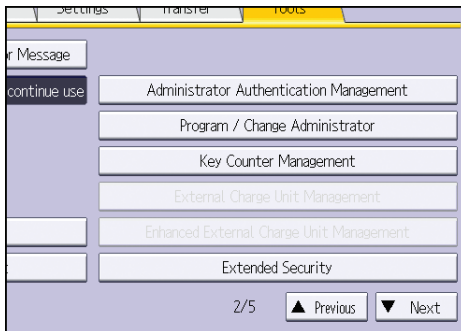
★ Important

- The machine cannot be used during encryption.

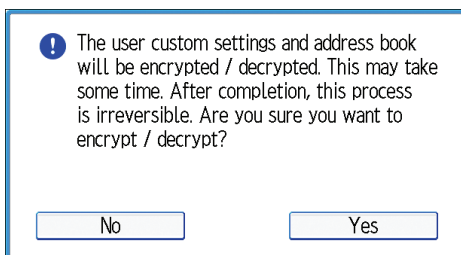
The time it takes to encrypt the data in the Address Book depends on the number of registered users.

Encrypting the data in the Address Book may take a long time.

1. Log in as the user administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [Extended Security].



6. Press [On] for "Encrypt User Custom Settings & Address Book".
7. Press [Change] for "Encryption Key".
8. Enter the encryption key, and then press [OK].
Enter the encryption key using up to 32 alphanumeric characters.
9. Press [Encrypt / Decrypt].
10. Press [Yes].



Do not switch the main power off during encryption, as doing so may corrupt the data.

If you press [Stop] during encryption, the data is not encrypted.

If you press [Stop] during decryption, the data stays encrypted.

Normally, once encryption is complete, "Encryption / Decryption is successfully complete. Press [Exit]." appears.

11. Press [Exit].

12. Press [OK].

13. Log out.

Note

- If you register additional users after encrypting the data in the Address Book, those users are also encrypted.
- The backup copy of the address book data stored in the SD card is encrypted. For details about backing up and then restoring the address book using an SD card, see "Administrator Tools", Connecting the Machine/ System Settings.

Encrypting Data on the Hard Disk

CAUTION

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

Prevent information leakage by encrypting the Address Book, authentication information, and stored documents as the data is written.

When the data encryption settings are enabled, an encryption key is generated and this is used to restore the data. This key can be changed at any time.

Data that is encrypted

This function encrypts data that is stored in the machine's NVRAM (memory that remains even after the machine has been turned off) and on the hard disk.

The following data is encrypted:

- Address Book data
- User authentication information
- Data stored in Document Server
- Temporary stored documents
- Logs
- Network I/F setting information
- System settings information

Note

- If the machine needs to be replaced, the existing data can be transferred to a new machine, even if the data is encrypted. To transfer data, contact your service representative.
- You can back up the machine's data encryption key to an SD card. For details about SD card handling, see "Inserting/Removing a Memory Storage Device", Getting Started.

Time required for encryption

When setting up encryption, specify whether to start encryption after deleting data (initialize) or encrypt existing data and retain it. If data is retained, it may take some time to encrypt it.

Setting	Data to be kept	Data to be initialized	Required time
File System Data Only	<ul style="list-style-type: none"> • Embedded Software Architecture applications' program/log • Address Book • Registered fonts • Job logs/access logs • Thumbnails of stored documents • Sent/received e-mail • Documents forwarded to the capture server • Files received via Mail to Print • Spooled jobs 	<ul style="list-style-type: none"> • Stored documents (stored documents in Document Server, Locked Print files / Sample Print files / Stored Print files / Hold Print files, and received and stored fax documents) • Registered stamps 	Approx. 1 hour
All Data	All Data: Both the data to be kept and data not kept when [File System Data Only] is specified	None	Approx. 3 hours, 15 minutes
Format All Data	None	All Data: Both the data to be kept and data not kept when [File System Data Only] is specified	Several minutes

Things to note when enabling encryption settings

- If you use Embedded Software Architecture application or App2Me, be sure to specify [File System Data Only] or [All Data].
- Note that the machine's settings will not be initialized to their system defaults even if [Format All Data], [File System Data Only], or [All Data] is specified.

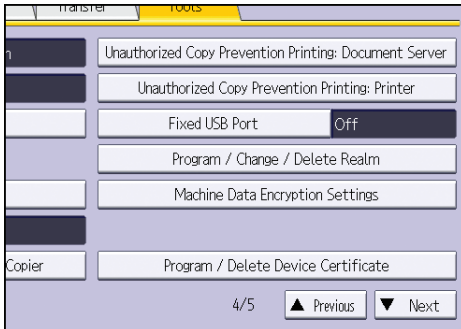
Enabling the Encryption Settings

★ Important

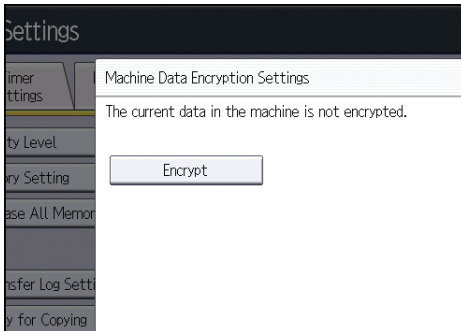
- The machine cannot be operated while data is being encrypted.
- Once the encryption process begins, it cannot be stopped. Make sure that the machine's main power is not turned off while the encryption process is in progress. If the machine's main power is turned off while the encryption process is in progress, the hard disk will be damaged and all data on it will be unusable.
- The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.
- Encryption begins after you have completed the control panel procedure and rebooted the machine by turning off and on the main power switch. If both the erase-by-overwrite function and the encryption function are specified, encryption begins after the data that is stored on the hard disk has been overwritten and the machine has been rebooted with the turning off and on of the main power switch.
- If you use hard disk erase-by-overwrite and encryption simultaneously, and select overwrite three times for "Random Numbers", the process will take up to 8 hours and 30 minutes. Re-encrypting from an already encrypted state takes the same amount of time.
- The "Erase All Memory" function also clears the machine's security settings, with the result that afterward, neither machine nor user administration will be effective. Ensure that users do not save any data on the machine after "Erase All Memory" has completed.
- Rebooting will be faster if there is no data to carry over to the hard disk and if encryption is set to [Format All Data], even if all the data on the hard disk is formatted. Before you perform encryption, we recommend you back up important data such as the Address Book and all data stored in Document Server.
- If the encryption key update was not completed, the printed encryption key will not be valid.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.

5. Press [Machine Data Encryption Settings].



6. Press [Encrypt].



7. Select the data to be carried over to the hard disk and not be reset.

To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File System Data Only]. To reset all of the data, select [Format All Data].

8. Select the backup method.

If you have selected [Save to SD Card], load an SD card into the media slot on the side of the control panel and press [OK] to back up the machine's data encryption key.

For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

If you have selected [Print on Paper], press the [Start] key and print out the machine's data encryption key.

9. Press [OK].

10. Press [Exit].

11. Press [Exit].

12. Log out.

13. Turn off the main power switch, and then turn the main power switch back on.

The machine will start to convert the data on the memory after you turn on the machine. Wait until the message "Memory conversion complete. Turn the main power switch off." appears, and then turn the main power switches off again.

For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Backing Up the Encryption Key

The encryption key can be backed up. Select whether to save it to an SD card or to print it.

★ Important

- **The encryption key is required for data recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.**

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**
5. **Press [Machine Data Encryption Settings].**
6. **Press [Back Up Encryption Key].**
7. **Select the backup method.**

If you have selected [Save to SD Card], load an SD card into the media slot on the side of the control panel and press [OK]; once the machine's data encryption key is backed up, press [Exit].

For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

If you have selected [Print on Paper], press the [Start] key and print out the machine's data encryption key.

8. **Press [Exit].**
9. **Log out.**

Updating the Encryption Key

You can update the encryption key and create a new key. Updates are possible when the machine is functioning normally.

★ Important

- **The encryption key is required for recovery if the machine malfunctions. Be sure to store the encryption key safely for retrieving backup data.**

- When the encryption key is updated, encryption is performed using the new key. After completing the procedure on the machine's control panel, turn off the main power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- If the encryption key update was not completed, the printed encryption key will not be valid.

1. Log in as the machine administrator from the control panel.

2. Press [System Settings].

3. Press [Administrator Tools].

4. Press [▼Next] three times.

5. Press [Machine Data Encryption Settings].

6. Press [Update Encryption Key].

7. Select the data to be carried over to the hard disk and not be reset.

To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File System Data Only]. To reset all of the data, select [Format All Data].

8. Select the backup method.

If you have selected [Save to SD Card], load an SD card into the media slot on the side of the control panel and press [OK] to back up the machine's data encryption key.

For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

If you have selected [Print on Paper], press the [Start] key and print out the machine's data encryption key.

9. Press [OK].

10. Press [Exit].

11. Press [Exit].

12. Log out.

13. Turn off the main power switch, and then turn the main power switch back on.

The machine will start to convert the data on the memory after you turn on the machine. Wait until the message "Memory conversion complete. Turn the main power switch off." appears, and then turn the main power switches off again.

For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Canceling Data Encryption

Use the following procedure to cancel the encryption settings when encryption is no longer necessary.

★ Important

- After completing this procedure on the machine's control panel, turn off the main power and restart the machine to enable the new settings. Restarting can be slow when there is data to be carried over to the hard disk.
- When disposing of a machine, completely erase the memory. For details on erasing all of the memory, see page 106 "Deleting Data on the Hard Disk".

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.
5. Press [Machine Data Encryption Settings].
6. Press [Cancel Encryption].
7. Select the data to be carried over to the hard disk and not be reset.

To carry all of the data over to the hard disk, select [All Data]. To carry over only the machine settings data, select [File System Data Only]. To reset all of the data, select [Format All Data].

8. Press [OK].
9. Press [Exit].
10. Press [Exit].
11. Log out.
12. Turn off the main power switch, and then turn the main power switch back on.

For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Deleting Data on the Hard Disk

The machine's hard disk stores all document data from the copier, printer and scanner functions. It also stores the data of users' Document Server and code counters, and the Address Book.

To prevent data on the hard disk being leaked before disposing of the machine, you can overwrite all data stored on the hard disk. You can also automatically overwrite temporarily-stored data.

↓ Note

- If your machine has the Smart Operation Panel, you must also format the data stored on the panel when deleting the data stored on the machine's hard disk. You can format the data stored on the panel in [Initialize Screen Features Settings] in [Screen Device Settings] under [Screen Features]. You can format the [Screen Features] settings, individual application settings, and cache memory.

4

Conditions for Use

When you use the erase-by-overwrite function, make sure to use it under the following conditions:

- The machine is used in its normal state (i.e. it is neither damaged, modified nor are there missing components).
- The machine is managed by an administrator who has carefully read and understood this manual, and can ensure the safe and effective use of this machine by general users.

Instructions for Use

- Before turning off the main power of the machine, always make sure that the Data Overwrite icon has turned to "Clear".
- If the machine enters Low Power mode when Auto Erase Memory is in progress, press the [Energy Saver] key to revive the display in order to check the icon.
- The machine will not enter Sleep mode until overwriting has been completed.
- Should the Data Overwrite icon continue to be "Dirty" even after you have made sure that there is no data to be overwritten, turn off the main power of your machine. Turn it on again and see if the icon changes to "Clear". If it does not, contact your sales or service representative.

Auto Erase Memory

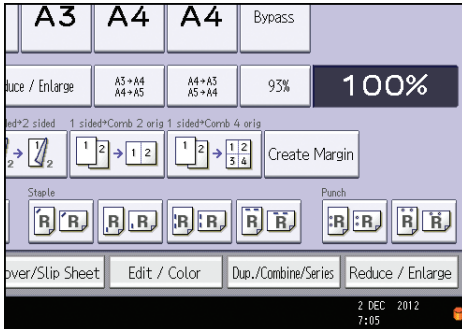
A document scanned in copier, or scanner mode, or print data sent from a printer driver is temporarily stored on the machine's hard disk. Even after the job is completed, it remains in the hard disk as temporary data. Auto Erase Memory erases the temporary data on the hard disk by writing over it.

Overwriting starts automatically once the job is completed.



The copier, fax and printer functions take priority over the Auto Erase Memory function. If a copy, fax or print job is in progress, overwriting will only be done after the job is completed.

Overwrite icon

When Auto Erase Memory is set to [On], the Data Overwrite icon will be indicated in the bottom right hand corner of the panel display of your machine.



4

Icon	Icon name	Explanation
	Dirty	This icon is lit when there is temporary data to be overwritten, and blinks during overwriting.
	Clear	This icon is lit when there is no temporary data to be overwritten.

★ Important

- The Data Overwrite icon will indicate "Clear" when there is a Sample Print/Locked Print/Hold Print/Stored Print job.

↓ Note

- If the Data Overwrite icon is not displayed, first check if Auto Erase Memory has been set to [Off]. If the icon is not displayed even though Auto Erase Memory is [On], contact your service representative.

Methods of overwriting

You can select a method of overwriting from the following:

- NSA
Temporary data is overwritten twice with random numbers and once with zeros.
- DoD

Each item of data is overwritten by a random number, then by its complement, then by another random number, and is then verified.

- Random Numbers

Temporary data is overwritten multiple times with random numbers. The number of overwrites can be selected from 1 to 9.

Note

- The default method for overwriting is "Random Numbers", and the default number of overwrites is 3.
- NSA stands for "National Security Agency", U.S.A.
- DoD stands for "Department of Defense", U.S.A.

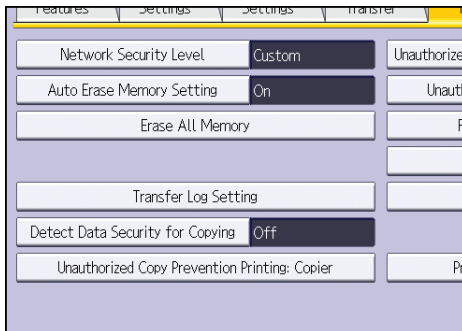
Using Auto Erase Memory

Important

- When Auto Erase Memory is set to [On], temporary data that remained on the hard disk when Auto Erase Memory was set to [Off] might not be overwritten.
- If the main power switch is turned off before Auto Erase Memory is completed, overwriting will stop and data will be left on the hard disk.
- Do not stop the overwrite mid-process. Doing so will damage the hard disk.
- Should the main power switch be turned off before Auto Erase Memory is completed, overwriting will continue once the main power switch is turned back on.
- If an error occurs before overwriting is completed, turn off the main power. Turn it on, and then repeat from step 1.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.

5. Press [Auto Erase Memory Setting].



6. Press [On].

7. Select the method of overwriting.

If you select [NSA] or [DoD], proceed to step 10.

If you select [Random Numbers], proceed to step 8.

8. Press [Change].

9. Enter the number of times that you want to overwrite using the number keys, and then press [#].

10. Press [OK].

Auto Erase Memory is set.

11. Log out.

↓ Note

- If you enable both overwriting and data encryption, the overwriting data will also be encrypted.

Canceling Auto Erase Memory

1. Log in as the machine administrator from the control panel.

2. Press [System Settings].

3. Press [Administrator Tools].

4. Press [▼Next] three times.

5. Press [Auto Erase Memory Setting].

6. Press [Off].

7. Press [OK].

Auto Erase Memory is disabled.

8. Log out.

Types of data that can or cannot be overwritten

The following are the types of data that can or cannot be overwritten by "Auto Erase Memory".

Data overwritten by Auto Erase Memory

Copier

- Copy jobs

Printer

- Print jobs
- Sample Print/Locked Print/Hold Print/Stored Print jobs

A Sample Print/Locked Print/Hold Print job can only be overwritten after it has been executed. A Stored Print job is overwritten after it has been deleted.

- Spool printing jobs

Facsimile

- LAN-Fax print data
- Faxes sent/received using remote machines

Data sent or received directly by this machine via facsimile, as well as fax numbers, will not be overwritten by Auto Erase Memory.

Scanner

- Scanned files sent by e-mail
- Files sent by Scan to Folder
- Documents sent using the ScanRouter delivery software or Web Image Monitor
- Network TWAIN scanner

Data scanned with the network TWAIN scanner when the TWAIN driver's "ADF(Read-ahead)" function is checked will be overwritten by Auto Erase Memory. Data scanned when the "ADF(Read-ahead)" function is not checked will not be overwritten.

Data Not overwritten by Auto Erase Memory

- Documents stored by the user in Document Server using the Copier, Printer, Facsimile or Scanner functions

A stored document can only be overwritten after it has been printed or deleted from Document Server.

- Information registered in the Address Book

Data stored in the Address Book can be encrypted for security. For details, see page 95 "Protecting the Address Book".

- Counters stored under each user code

Erase All Memory

You can erase all the data on the hard disk by writing over it. This is useful if you relocate or dispose of your machine.

The following data will also be erased by Erase All Memory. For details about using the machine after executing Erase All Memory, contact your sales representative.

- User codes
- Counters under each user code
- User stamps
- Data stored in the Address Book
- Printer fonts downloaded by users
- Applications using Embedded Software Architecture
- SSL server certificates
- Machine's network settings

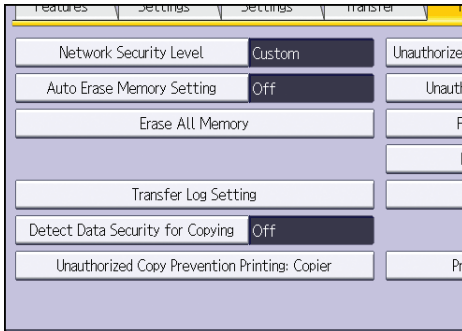
★ Important

- If the main power switch is turned off before "Erase All Memory" is completed, overwriting will be stopped and data will be left on the hard disk.
- Do not stop the overwrite mid-process. Doing so will damage the hard disk.
- We recommend that before you erase the hard disk, you use SmartDeviceMonitor for Admin/Device Manager NX Lite to back up the user codes, the counters for each user code, and the Address Book. The Address Book can also be backed up using Web Image Monitor. For details, see SmartDeviceMonitor for Admin/Device Manager NX Lite Help or Web Image Monitor Help.
- The only operation possible during the "Erase All Memory" process is pausing. If "Random Numbers" is selected and overwrite three times is set, the "Erase All Memory" process takes up to 5 hours and 15 minutes.
- The "Erase All Memory" function also clears the machine's security settings, with the result that afterward, neither machine nor user administration will be effective. Ensure that users do not save any data on the machine after "Erase All Memory" has completed.

Using Erase All Memory

1. Disconnect communication cables connected to the machine.
2. Log in as the machine administrator from the control panel.
3. Press [System Settings].
4. Press [Administrator Tools].
5. Press [▼Next] three times.

6. Press [Erase All Memory].



4

7. Select the method of overwriting.

If you select [NSA] or [DoD], proceed to step 10.

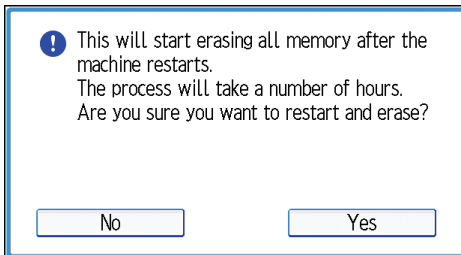
If you select [Random Numbers], proceed to step 8.

8. Press [Change].

9. Enter the number of times that you want to overwrite using the number keys, and then press [#].

10. Press [Erase].

11. Press [Yes].



12. When overwriting is completed, press [Exit], and then turn off the main power.

For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

Note

- Should the main power switch be turned off before "Erase All Memory" is completed, overwriting will start over when the main power switch is turned back on.
- If an error occurs before overwriting is completed, turn off the main power. Turn it on again, and then repeat from step 2.

Suspending Erase All Memory

The overwriting process can be suspended temporarily.

★ Important

- Erase All Memory cannot be canceled.

1. Press [Suspend] while Erase All Memory is in progress.
2. Press [Yes].

Erase All Memory is suspended.

3. Turn off the main power.

For details about turning off the main power, see "Turning On/Off the Power", Getting Started.

↓ Note

- To resume overwriting, turn on the main power.

5. Enhanced Network Security

This chapter describes the functions for enhancing security when the machine is connected to the network.

Access Control

The machine can control TCP/IP access.

Limit the IP addresses from which access is possible by specifying the access control range.

For example, if you specify the access control range as [192.168.15.16]-[192.168.15.20], the client PC addresses from which access is possible will be from [192.168.15.16] to [192.168.15.20].

★ Important

- Using access control, you can limit access involving LPR, RCP/RSH, FTP, ssh/sftp, Bonjour, SMB, WSD (Device), WSD (Printer), WSD (Scanner)/DSM, IPP, DIPRINT, RHPP, Web Image Monitor, or SmartDeviceMonitor for Client. You cannot limit the monitoring of SmartDeviceMonitor for Client. You cannot limit access involving telnet, or SmartDeviceMonitor for Admin/Device Manager NX Lite, when using the SNMPv1 monitoring.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Access Control] under "Security".
4. To specify the IPv4 address, enter an IP address that has access to the machine in "Access Control Range".

To specify the IPv6 address, enter an IP address that has access to the machine in "Range" under "Access Control Range", or enter an IP address in "Mask" and specify the "Mask Length".

5. Click [OK].
6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].
If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. Log out.

Enabling and Disabling Protocols

Specify whether to enable or disable the function for each protocol. By making this setting, you can specify which protocols are available and so prevent unauthorized access over the network. Network settings can be specified on the control panel or by using Web Image Monitor, telnet, SmartDeviceMonitor for Admin/Device Manager NX Lite or Remote Communication Gate S. In the case of SmartDeviceMonitor for Admin/Device Manager NX Lite, use it to start Web Image Monitor and configure the settings from there.

Protocol	Port	Setting method	When disabled
IPv4	-	<ul style="list-style-type: none"> Control panel Web Image Monitor telnet SmartDeviceMonitor for Admin Device Manager NX Lite Remote Communication Gate S 	<p>All applications that operate over IPv4 cannot be used.</p> <p>IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.</p>
IPv6	-	<ul style="list-style-type: none"> Control panel Web Image Monitor telnet SmartDeviceMonitor for Admin Device Manager NX Lite Remote Communication Gate S 	<p>All applications that operate over IPv6 cannot be used.</p>
IPsec	-	<ul style="list-style-type: none"> Control panel Web Image Monitor telnet SmartDeviceMonitor for Admin Device Manager NX Lite 	<p>Encrypted transmission using IPsec is disabled.</p>

Protocol	Port	Setting method	When disabled
FTP	TCP:21	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>Functions that require FTP cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
ssh/sftp	TCP:22	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>Functions that require sftp cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
telnet	TCP:23	<ul style="list-style-type: none"> • Web Image Monitor • SmartDeviceMonitor for Admin • Device Manager NX Lite 	Commands using telnet are disabled.
SMTP	TCP:25 (variable)	<ul style="list-style-type: none"> • Control panel • Web Image Monitor • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	Internet Fax or e-mail notification functions that require SMTP reception cannot be used.

Protocol	Port	Setting method	When disabled
HTTP	TCP:80	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite 	<p>Functions that require HTTP cannot be used.</p> <p>Cannot print using IPP on port 80.</p>
HTTPS	TCP:443	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite 	<p>Functions that require HTTPS cannot be used.</p> <p>@Remote cannot be used.</p> <p>You can also make settings to require SSL transmission using the control panel or Web Image Monitor.</p>
SMB	TCP:139	<ul style="list-style-type: none"> • Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	SMB printing functions cannot be used.
NBT	UDP:137 UDP:138	<ul style="list-style-type: none"> • telnet 	SMB printing functions via TCP/IP, as well as NetBIOS designated functions on the WINS server cannot be used.
SNMPv1,v2	UDP:161	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>Functions that require SNMPv1, v2 cannot be used.</p> <p>Using the control panel, Web Image Monitor or telnet, you can specify that SNMPv1, v2 settings are read-only, and cannot be edited.</p>

Protocol	Port	Setting method	When disabled
SNMPv3	UDP:161	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>Functions that require SNMPv3 cannot be used.</p> <p>You can also make settings to require SNMPv3 encrypted transmission and restrict the use of other transmission methods using the control panel, Web Image Monitor, or telnet.</p>
RSH/RCP	TCP:514	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>Functions that require RSH and network TWAIN functions cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
LPR	TCP:515	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>LPR functions cannot be used.</p> <p>You can restrict personal information from being displayed by making settings on the control panel using "Restrict Display of User Information".</p>
IPP	TCP:631	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	<p>IPP functions cannot be used.</p>

Protocol	Port	Setting method	When disabled
IP-Fax	TCP:1720 (H.323) UDP:1719 (Gatekeeper) TCP/UDP:5060 (SIP) TCP:5000 (H.245) UDP:5004, 5005 (Voice) TCP/UDP:49152 (T.38)	<ul style="list-style-type: none"> Control panel Web Image Monitor SmartDeviceMonitor for Admin Device Manager NX Lite Remote Communication Gate S 	IP-Fax connecting functions using H.323, SIP and T.38 cannot be used.
SSDP	UDP:1900	<ul style="list-style-type: none"> Web Image Monitor telnet SmartDeviceMonitor for Admin Device Manager NX Lite 	Device discovery using UPnP from Windows cannot be used.
Bonjour	UDP:5353	<ul style="list-style-type: none"> Web Image Monitor telnet SmartDeviceMonitor for Admin Device Manager NX Lite Remote Communication Gate S 	Bonjour functions cannot be used.
@Remote	TCP:7443 TCP:7444	<ul style="list-style-type: none"> Control panel telnet 	@Remote cannot be used.

Protocol	Port	Setting method	When disabled
DIPRINT	TCP:9100	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	DIPRINT functions cannot be used.
RFU	TCP:10021	<ul style="list-style-type: none"> • Control panel • telnet 	You can attempt to update firmware via FTP.
NetWare	(IPX/SPX)	<ul style="list-style-type: none"> • Control panel • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	Cannot print with NetWare. SNMP over IPX cannot be used.
WSD (Device)	TCP:53000 (variable)	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	WSD (Device) functions cannot be used.

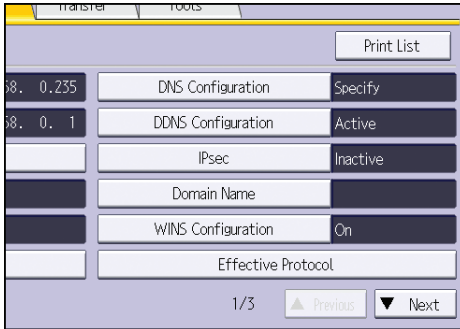
Protocol	Port	Setting method	When disabled
WSD (Printer)	TCP:53001 (variable)	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	WSD (Printer) functions cannot be used.
WSD (Scanner)/DSM	TCP-53002 (variable)	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite • Remote Communication Gate S 	WSD (Scanner) and DSM functions cannot be used.
WS-Discovery	UDP/TCP: 3702	<ul style="list-style-type: none"> • telnet • Remote Communication Gate S 	WSD (Device, Printer, Scanner) search function cannot be used.
RHPP	TCP:59100	<ul style="list-style-type: none"> • Web Image Monitor • telnet • SmartDeviceMonitor for Admin • Device Manager NX Lite 	Cannot print with RHPP.
LLTD	-	<ul style="list-style-type: none"> • telnet 	Device search function using LLTD cannot be used.
LLMNR	UDP:5355	<ul style="list-style-type: none"> • Web Image Monitor • telnet 	Name resolution requests using LLMNR cannot be respond.

Note

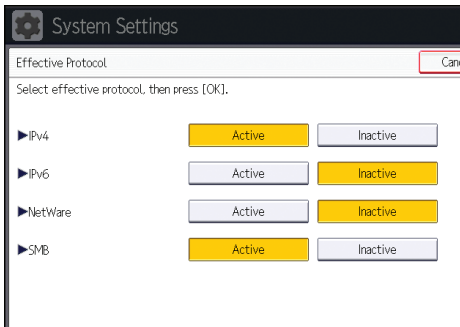
- "Restrict Display of User Information" is one of the Extended Security features. For details about making this setting, see page 257 "Specifying the Extended Security Functions".

Enabling and Disabling Protocols Using the Control Panel

1. Log in as the network administrator from the control panel.
2. Press [System Settings].
3. Press [Interface Settings].
4. Press [Effective Protocol].



5. Set the desired protocols to active/inactive.



6. Press [OK].
7. Log out.

Enabling and Disabling Protocols Using Web Image Monitor

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Network Security] under "Security".
4. Set the desired protocols to active/inactive (or open/close).
5. Click [OK].

6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. Log out.

Specifying Network Security Level

This setting lets you change the security level to limit unauthorized access. You can make network security level settings on the control panel, as well as Web Image Monitor. However, the protocols that can be specified differ.

★ Important

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

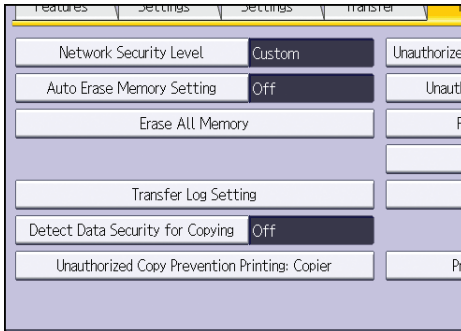
Network Security Levels

Security Level	Description
[Level 0]	Select [Level 0] to use all features. Use this setting when you have no information that needs to be protected from external threats.
[Level 1]	Select [Level 1] for moderate security to protect important information. Use this setting if the machine is connected to a local area network (LAN).
[FIPS140]	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]	Select [Level 2] for maximum security to protect confidential information. Use this setting when it is necessary to protect information from external threats.
[Custom]	For configurations other than the levels above. Configure using Web Image Monitor.

Specifying Network Security Level Using the Control Panel

1. Log in as the network administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.

5. Press [Network Security Level].



6. Select the network security level.

Select [Level 0], [Level 1], [Level 2], or [FIPS140].

7. Press [OK].

8. Log out.

5

Specifying Network Security Level Using Web Image Monitor

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

2. Point to [Device Management], and then click [Configuration].

3. Click [Network Security] under "Security".

4. Select the network security level in "Security Level".

5. Click [OK].

6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. Log out.

Status of Functions under Each Network Security Level

TCP/IP

Function	Level 0	Level 1	FIPS 140	Level 2
TCP/IP	Active	Active	Active	Active
HTTP > Port 80	Open	Open	Open	Open
IPP > Port 80	Open	Open	Open	Open

Function	Level 0	Level 1	FIPS 140	Level 2
IPP > Port 631	Open	Open	Close	Close
SSL/TLS > Port 443	Open	Open	Open	Open
SSL/TLS > Permit SSL/TLS Communication	Ciphertext Priority	Ciphertext Priority	Ciphertext Only	Ciphertext Only
SSL/TLS Version > TLS1.2	Active	Active	Active	Active
SSL/TLS Version > TLS1.1	Active	Active	Active	Active
SSL/TLS Version > TLS1.0	Active	Active	Active	Active
SSL/TLS Version > SSL3.0	Active	Active	Inactive	Inactive
Encryption Strength Setting > AES	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit	128bit/ 256bit
Encryption Strength Setting > 3DES	168bit	168bit	168bit	-
Encryption Strength Setting > RC4	-	-	-	-
DIPRINT	Active	Active	Inactive	Inactive
LPR	Active	Active	Inactive	Inactive
FTP	Active	Active	Active	Active
sftp	Active	Active	Active	Active
ssh	Active	Active	Active	Active
RSH/RCP	Active	Active	Inactive	Inactive
TELNET	Active	Inactive	Inactive	Inactive
Bonjour	Active	Active	Inactive	Inactive
SSDP	Active	Active	Inactive	Inactive
SMB	Active	Active	Inactive	Inactive
NetBIOS over TCP/IPv4	Active	Active	Inactive	Inactive
WSD (Device)	Active	Active	Active	Active
WSD (Printer)	Active	Active	Active	Active

Function	Level 0	Level 1	FIPS 140	Level 2
WSD (Scanner)/DSM	Active	Active	Active	Active
WSD (Encrypted Communication of Device)	Inactive	Inactive	Active	Active
RHPP	Active	Active	Inactive	Inactive

The same settings are applied to IPv4 and IPv6.

TCP/IP setting is not governed by the security level. Manually specify whether to activate or inactivate this setting.

NetWare

Function	Level 0	Level 1	FIPS 140	Level 2
NetWare	Active	Active	Inactive	Inactive

If NetWare is not used on your network, the above settings are not applicable.

SNMP

Function	Level 0	Level 1	FIPS 140	Level 2
SNMP	Active	Active	Active	Active
Permit Settings by SNMPv1 and v2	On	Off	Off	Off
SNMPv1,v2 Function	Active	Active	Inactive	Inactive
SNMPv3 Function	Active	Active	Active	Active
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
ssh > Encryption Algorithm	DES/3DES/ AES-128/ AES-192/ AES-256/ Blowfish/ Arcfour	3DES/ AES-128/ AES-192/ AES-256/ Arcfour	3DES/ AES-128/ AES-192/ AES-256	3DES/ AES-128/ AES-192/ AES-256

Function	Level 0	Level 1	FIPS 140	Level 2
S/MIME > Encryption Algorithm	3DES-168 bit	3DES-168 bit	3DES-168 bit	AES-256 bit
S/MIME > Digest Algorithm	SHA1	SHA1	SHA1	SHA-256 bit
SNMPv3 > Authentication Algorithm	MD5	SHA1	SHA1	SHA1
SNMPv3 > Encryption Algorithm	DES	DES	AES-128	AES-128
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	Simple Encryption	DES	AES	AES

Protecting the Communication Path via a Device Certificate

This machine can protect its communication path and establish encrypted communications using SSL/TLS, IPsec, S/MIME, or IEEE 802.1X. It can also protect PDFs by means of a PDF or PDF/A digital signature.

To use these functions, it is necessary to create and install a device certificate for the machine in advance.

The following types of device certificate can be used:

- Self-signed certificate created by the machine
- Certificate issued by a certificate authority

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.
- If SHA256 or SHA512 is selected as the "Algorithm Signature" of the device certificate, Windows XP SP3 or later is required to connect the device using Internet Explorer 6.0.

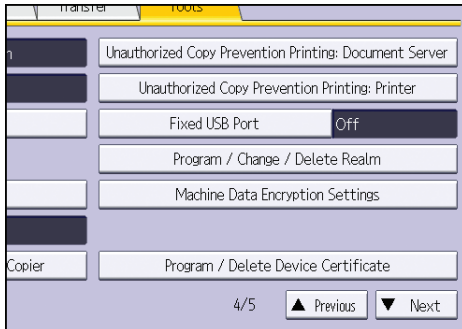
Creating and Installing a Device Certificate from the Control Panel (Self-Signed Certificate)

Create and install the device certificate using control panel.

This section explains the use of a self-signed certificate as the device certificate.

1. Log in as the network administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.

5. Press [Program / Delete Device Certificate].



6. Check that [Program] is selected.

7. Press [Certificate 1].

Only [Certificate 1] can be created from the control panel.

8. Make the necessary settings.

To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine's administrator's e-mail address in the e-mail address setting.

9. Press [OK].

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

10. Log out.

↓ Note

- Select [Delete] to delete the device certificate from the machine.
- To use the device certificate created on the machine for S/MIME or PDF/A Digital Signature, set "Certification" in Web Image Monitor to [Certificate 1].

Creating and Installing a Device Certificate from Web Image Monitor (Self-Signed Certificate)

Create and install the device certificate using Web Image Monitor. For details about the displayed items and selectable items, see Web Image Monitor Help.

This section explains the use of a self-signed certificate as the device certificate.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Device Certificate] under "Security".

4. Check the radio button next to the number of the certificate you want to create.

To use SSL/TLS, select [Certificate 1]. To use any other protocol, select the certificate number desired.

5. Click [Create].

Click [Delete] to delete the device certificate from the machine.

6. Make the necessary settings.

To use the device certificate for S/MIME, PDF Digital Signature, or PDF/A Digital Signature, enter the machine's administrator's e-mail address in the e-mail address setting.

7. Click [OK].

The setting is changed.

8. Click [OK].

9. If a security warning message appears, check the details, and then select "Continue to this website".

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

10. Log out.

Creating the Device Certificate (Issued by a Certificate Authority)

Create the device certificate using Web Image Monitor. For details about the displayed items and selectable items, see Web Image Monitor Help.

This section explains the use of a certificate issued by a certificate authority as the device certificate.

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

2. Point to [Device Management], and then click [Configuration].

3. Click [Device Certificate] under "Security".

4. Check the radio button next to the number of the certificate you want to create.

To use SSL/TLS, select [Certificate 1]. To use any other protocol, select the certificate number desired.

5. Click [Request].

6. Make the necessary settings.

7. Click [OK].

The setting is changed.

8. Click [OK].

"Requesting" appears for "Certificate Status".

9. Log out.

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

The application procedure depends on the certificate authority. For details, contact the certificate authority.

For the application, click  Web Image Monitor Details icon and use the information that appears in "Certificate Details".

Note

- The issuing location may not be displayed if you request two certificates at the same time. When you install a certificate, be sure to check the certificate destination and installation procedure.
- Web Image Monitor can be used for creating the device certificate but not for requesting the certificate to the certificate authority.
- Click [Cancel Request] to cancel the request for the device certificate.

Installing the Device Certificate (Issued by a Certificate Authority)

5

Install the device certificate using Web Image Monitor. For details about the displayed items and selectable items, see Web Image Monitor Help.

This section explains the use of a certificate issued by a certificate authority as the device certificate.

Enter the device certificate contents issued by the certificate authority.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**

4. **Check the radio button next to the number of the certificate you want to install.**

To use SSL/TLS, select [Certificate 1]. To use any other protocol, select the certificate number desired.

5. **Click [Install].**

6. **Enter the contents of the device certificate.**

In the certificate box, enter the contents of the device certificate issued by the certificate authority.

If you are installing an intermediate certificate, enter the contents of the intermediate certificate also.

For details about the displayed items and selectable items, see Web Image Monitor Help.

7. **Click [OK].**

8. **Wait for about one or two minutes, and then click [OK].**

"Installed" appears under "Certificate Status" to show that a device certificate for the machine has been installed.

9. **Log out.**

Installing an Intermediate Certificate (Issued by a Certificate Authority)

This section explains how to use Web Image Monitor to install an intermediate certificate issued by a certificate authority.

If you do not have the intermediate certificate issued by the certificate authority, a warning message will appear during communication. If the certificate authority has issued an intermediate certificate, we recommend installing the intermediate certificate.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Device Certificate] under "Security".**
4. **Check the radio button next to the number of the certificate you want to install.**
5. **Click [Install Intermediate Certificate].**
6. **Enter the contents of the intermediate certificate.**

In the certificate box, enter the contents of the intermediate certificate issued by the certificate authority. For details about the items and settings of a certificate, see Web Image Monitor Help.

7. **Click [OK].**
8. **Wait for about one or two minutes, and then click [OK].**

The intermediate certificate will be installed on the device. The "Certificate Details" screen will inform you whether or not the installation of the intermediate certificate was successful. For details about the "Certificate Details" screen, see Web Image Monitor Help.

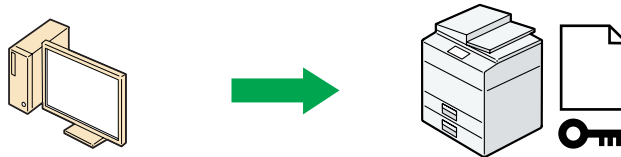
9. **Log out.**

Configuring SSL/TLS

Configuring the machine to use SSL/TLS enables encrypted communication. Doing so helps prevent data from being intercepted, cracked or tampered with during transmission.

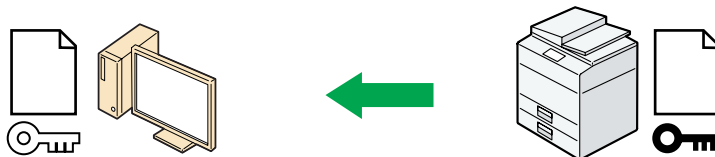
Flow of SSL/TLS encrypted communications

1. To access the machine from a user's computer, request the SSL/TLS device certificate and public key.



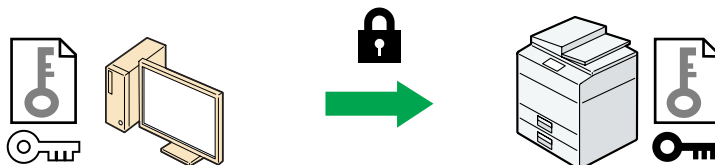
CJC002

2. The device certificate and public key are sent from the machine to the user's computer.



CJC003

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



CJC004

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



CJC005

Configuration flow when using a self-signed certificate

1. Creating and installing the device certificate

Create and install a device certificate from the control panel or Web Image Monitor.

2. Enabling SSL/TLS

Enable the SSL/TLS setting using Web Image Monitor.

Configuration flow when using an authority issued certificate

1. Creating a device certificate and applying to the authority

After creating a device certificate on Web Image Monitor, apply to the certificate authority.

The application procedure after creating the certificate depends on the certificate authority.

Follow the procedure specified by the certificate authority.

2. Installing the device certificate

Install the device certificate using Web Image Monitor.

3. Enabling SSL/TLS

Enable the SSL/TLS setting using Web Image Monitor.

5

Note

- To confirm 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

After installing the device certificate in the machine, enable the SSL/TLS setting.

This procedure is used for a self-signed certificate or a certificate issued by a certificate authority.

1. **Log in as the network administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [SSL/TLS] under "Security".**
4. **For IPv4 and IPv6, select "Active" if you want to enable SSL/TLS.**
5. **Select the encryption communication mode for "Permit SSL/TLS Communication".**
6. **If you want to disable a protocol, click [Inactive] next to "TLS1.2", "TLS1.1", "TLS1.0", or "SSL3.0".**

At least one of these protocols must be enabled.

7. Under "Encryption Strength Setting", specify the strength of encryption to be applied for "AES", "3DES", and/or "RC4". You must select at least one check box.

Note that the availability of encryption strengths will vary depending on the settings you have specified for "TLS1.2", "TLS1.1", "TLS1.0", or "SSL3.0".

8. Click [OK].

9. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

10. Log out.

Note

- If you set "Permit SSL/TLS Communication" to [Ciphertext Only], communication will not be possible if you select a protocol that does not support a Web browser, or specify an encryption strength setting only. If this is the case, enable communication by setting [Permit SSL / TLS Communication] to [Ciphertext / Cleartext] using the machine's control panel, and then specify the correct protocol and encryption strength.
- The SSL/TLS version and encryption strength settings can be changed, even under [Network Security].
- Depending on the states you specify for "TLS1.2", "TLS1.1", "TLS1.0", and "SSL3.0", the machine might not be able to connect to an external LDAP server.
- If only TLS1.2 and TLS1.1 are enabled, Integration Server authentication cannot be performed.
- The following types of communication and data are always encrypted by SSL3.0: communication via @Remote, Integration Server authentication, files sent via a delivery server, and logs transferred to Remote Communication Gate S.

User Setting for SSL/TLS

We recommend that after installing the self-signed certificate or device certificate from a private certificate authority on the main unit and enabling SSL/TLS (communication encryption), you instruct users to install the certificate on their computers. Installation of the certificate is especially necessary for users who want to print via IPP-SSL from Windows Vista/7/8, Windows Server 2008/2008 R2/2012. The network administrator must instruct each user to install the certificate.

Select [Trusted Root Certification Authorities] for the certificate store location when accessing the machine by IPP.

Note

- Take the appropriate steps when you receive a user's inquiry concerning problems such as an expired certificate.

- If a certificate issued by a certificate authority is installed in the machine, confirm the certificate store location with the certificate authority.
- To change the host name or IP address in [Common Name] of the device certificate when using the operating system's standard IPP port under Windows Vista/7/8 or Windows Server 2008/2008 R2/2012, delete any previously configured PC printer beforehand and re-install it after changing [Common Name]. Also, to change the user authentication settings (login user name and password), delete any previously configured PC printer beforehand and re-install it after changing the user authentication settings.

Setting the SSL/TLS Encryption Mode

By specifying the SSL/TLS encrypted communication mode, you can change the security level.

Encrypted communication mode

Using the encrypted communication mode, you can specify encrypted communication.

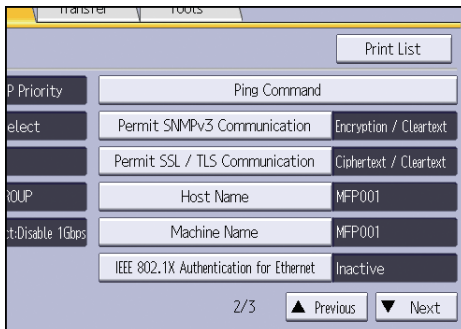
5

Encrypted communication mode	Description
Ciphertext Only	Allows encrypted communication only. If encryption is not possible, the machine does not communicate.
Ciphertext Priority	Performs encrypted communication if encryption is possible. If encryption is not possible, the machine communicates without it.
Ciphertext / Cleartext	Communicates with or without encryption, according to the setting.

After installing the device certificate, specify the SSL/TLS encrypted communication mode. By making this setting, you can change the security level.

1. Log in as the network administrator from the control panel.
2. Press [System Settings].
3. Press [Interface Settings].
4. Press [▼Next].

5. Press [Permit SSL / TLS Communication].



6. Select the encrypted communication mode.

Select [Ciphertext Only], [Ciphertext Priority], or [Ciphertext / Cleartext] as the encrypted communication mode.

7. Press [OK].

8. Log out.

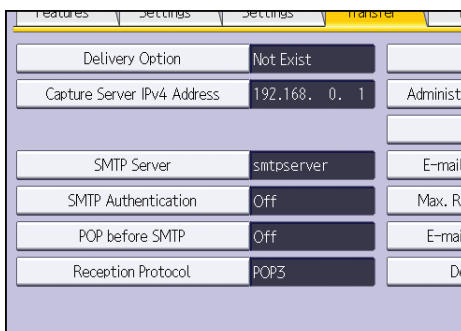
Note

- The SSL/TLS encrypted communication mode can also be specified using Web Image Monitor. For details, see Web Image Monitor Help.

Enabling SSL for SMTP Connections

Use the following procedure to enable SSL encryption for SMTP connections.

1. Log in as the network administrator from the control panel.
2. Press [System Settings].
3. Press [File Transfer].
4. Press [SMTP Server].



5. In "Use Secure Connection (SSL)", press [On].

If you are not using SSL for SMTP connections, press [Off].

When "Use Secure Connection (SSL)" is set to [On], the port number is changed to 465.

6. Press [OK].

7. Log out.

↓ Note

- If you set "Use Secure Connection (SSL)" to [On], you cannot bypass the SMTP server to send Internet Fax documents directly.

Configuring S/MIME

By registering a user certificate in the Address Book, you can send e-mail that is encrypted with a public key which prevents its content from being altered during transmission. You can also prevent sender impersonation (spoofing) by installing a device certificate on the machine, and attaching an electronic signature created with a private key. You can apply these functions separately or, for stronger security, together.

To send encrypted e-mail, both the sender (this machine) and the receiver must support S/MIME.

Compatible mailer applications

The S/MIME function can be used with the following applications:

- Microsoft Outlook 2003 and later
- Thunderbird 3.1.7 and later
- Windows Live Mail

★ Important

- To use S/MIME, you must first specify [Administrator's E-mail Address] in [System Settings].

↓ Note

- If an electronic signature is specified for an e-mail, the administrator's address appears in the "From" field and the address of the user specified as "sender" appears in the "Reply To" field.
- When you send an e-mail to both users whose mail clients support S/MIME and users whose clients lack such support, the e-mail for the S/MIME clients is encrypted, but that for the non-S/MIME clients is left as plaintext.
- When using S/MIME, the e-mail size is larger than normal.
- For details about using S/MIME with the fax function, see "Encryption and Signature for Internet Fax/E-mail", Fax.

E-mail Encryption

To send encrypted e-mail using S/MIME, the user certificate must first be prepared using Web Image Monitor and registered in the Address Book by the user administrator. Registering the certificate in the Address Book specifies each user's public key. After installing the certificate, specify the encryption algorithm using Web Image Monitor. The network administrator can specify the algorithm.

E-mail encryption

1. Prepare the user certificate.
2. Install the user certificate in the Address Book using Web Image Monitor. (The public key on the certificate is specified in the Address Book.)
3. Specify the encryption algorithm using Web Image Monitor.

4. Using the shared key, encrypt the e-mail message.
5. The shared key is encrypted using the user's public key.
6. The encrypted e-mail is sent.
7. The receiver decrypts the shared key using a secret key that corresponds to the public key.
8. The e-mail is decrypted using the shared key.

Note

- There are three types of user certificates that can be installed on this machine, "DER Encoded Binary X.509", "Base 64 Encoded X.509", and "PKCS #7" certificate.
- When installing a user certificate to the Address Book using Web Image Monitor, you might see an error message if the certificate file contains more than one certificate. If this error message appears, install the certificates one at a time.

5

Specifying the user certificate

Each user certificate must be prepared in advance.

1. **Log in as the user administrator from Web Image Monitor.**
 2. **Point to [Device Management], and then click [Address Book].**
 3. **Select the user for whom the certificate will be installed.**
 4. **Click [Detail Input], and then click [Change].**
- The Change User Information screen appears.
5. **Enter the user address in the "Email Address" field under "Email".**
 6. **Click [Change] in "User Certificate".**
 7. **Click [Browse], select the user certificate file, and then click [Open].**
 8. **Click [OK].**

The user certificate is installed.

9. **"Updating..." appears. Wait for about one or two minutes, and then click [OK].**

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

10. **Log out.**

Note

- Once the valid period of the selected user certificate elapses, encrypted messages can no longer be sent. Select a certificate that is within its valid period.

Specifying the encryption algorithm

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [S/MIME] under "Security".
4. Select the encryption algorithm from the drop-down menu next to "Encryption Algorithm" under "Encryption".
5. Click [OK].

The algorithm for S/MIME is set.

6. Log out.

Note

- Configure the settings taking into consideration the encryption algorithm and digest algorithm supported by the user's e-mail software.

Attaching an Electronic Signature

To attach an electronic signature to sent e-mail, a device certificate must be installed in advance.

As the device certificate, you can use a self-signed certificate created by the machine or a certificate issued by a certificate authority. For details about creating and installing the device certificate, see page 130 "Protecting the Communication Path via a Device Certificate".

Important

- **To install an S/MIME device certificate, you must first register "Administrator's E-mail Address" in [System Settings] as the e-mail address for the device certificate. Note that even if you will not be using S/MIME, you must still specify an e-mail address for the S/MIME device certificate.**

Electronic signature

1. Install a device certificate on the machine. (The secret key on the certificate is configured on the machine.)
2. Attach the electronic signature to an e-mail using the secret key provided by the device certificate.
3. Send the e-mail with the electronic signature attached to the user.
4. The receiver requests the public key and device certificate from the machine.
5. Using the public key, you can determine the authenticity of the attached electronic signature to see if the message has been altered.

Configuration flow (self-signed certificate)

1. Create and install the device certificate using Web Image Monitor.
2. Make settings for the certificate to be used for S/MIME using Web Image Monitor.

3. Make settings for the electronic signature using Web Image Monitor.

Configuration flow (certificate issued by a certificate authority)

1. Create the device certificate using Web Image Monitor.
The application procedure for a created certificate depends on the certificate authority. Follow the procedure specified by the certificate authority.
2. Install the device certificate using Web Image Monitor.
3. Make settings for the certificate to be used for S/MIME using Web Image Monitor.
4. Make settings for the electronic signature using Web Image Monitor.

Selecting the device certificate

Select the device certificate to be used for S/MIME using Web Image Monitor.

5

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Device Certificate] under "Security".
4. Select the certificate to be used for the electronic signature from the drop-down box in "S/MIME" under "Certification".
5. Click [OK].

The certificate to be used for the S/MIME electronic signature is set.

6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].
If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. Log out.

Note

- If the selected device certificate expires, signatures cannot be attached to e-mail. Select a certificate that is within its valid period.

Specifying the electronic signature

After installing a device certificate to the machine, configure the conditions for S/MIME signatures. The configuration procedure is the same regardless of whether you are using a self-signed certificate or a certificate issued by a certificate authority.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [S/MIME] under "Security".

4. Select the digest algorithm to be used in the electronic signature next to "Digest Algorithm" under "Signature".
5. Select the method for attaching the electronic signature when sending e-mail from the scanner next to "When Sending Email by Scanner" under "Signature".
6. Select the method for attaching the electronic signature when forwarding received fax messages next to "When Transferring by Fax" under "Signature".
7. Select the method for attaching the electronic signature when sending e-mail from the fax next to "When Sending Email by Fax" under "Signature".
8. Select the method for attaching the electronic signature when e-mail notification is sent using the fax function next to "When Emailing TX Results by Fax" under "Signature".
9. Select the method for attaching the electronic signature when forwarding stored documents next to "When Transferring Files Stored in Document Server (Utility)" under "Signature".
10. Click [OK].

The settings for the S/MIME electronic signature are enabled.

11. Log out.

↓ Note

- Configure the settings taking into consideration the encryption algorithm and digest algorithm supported by the user's e-mail software.

Specifying Checking of the Certificate Valid Period

The validity period of the certificate used with S/MIME is verified when you send e-mail.

You can change the timing at which the valid period is checked.

Operation mode	Description
Security Priority	<p>The validity period is verified at the following timings.</p> <p>User Certificate</p> <p>(a). When the address is selected</p> <p>(b). When the [Start] key is pressed</p> <p>Device certificate</p> <p>(c). When the first address is selected</p> <p>(d). When the [Start] key is pressed</p>

Operation mode	Description
Performance Priority	<p>Performing (b) and (c) are omitted.</p> <p>If it takes a long time to verify the validity period when the address is selected or when the [Start] key is pressed, the time taken can be shortened by selecting "Performance Priority".</p>

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [S/MIME] under "Security".
4. In "Operation Mode", select [Security Priority] or [Performance Priority].
5. Click [OK].
6. Log out.

Note

- If a certificate was valid when transmitted but has expired before retrieving the e-mail from the mail server to the client computer, the e-mail may not be retrieved.
- If an error occurs outside the validity period of the certificate when sending an S/MIME e-mail automatically, such as in the case of sending e-mail by Memory Transmission or at a specified time, the error will be reported by e-mail in plain text to the sender's or administrator's e-mail address. The error details can be viewed in the job log. When using S/MIME, be sure to enable the job log collection function. For details about viewing the logs, see page 203 "Managing Log Files".

Configuring PDFs with Electronic Signatures

This machine can create PDFs with electronic signatures. PDFs with electronic signatures certify the creator of the PDF document and the date and time of creation. Tampering is also prevented as documents that have been tampered with can be detected.

In order to create PDFs with electronic signatures, first select the certificate to use for the signature from the device certificates that have been created and installed.

As the device certificate, you can use a self-signed certificate created by the machine or a certificate issued by a certificate authority. For details about creating and installing a device certificate, see page 130 "Protecting the Communication Path via a Device Certificate".

★ Important

- To create digitally signed PDFs, you must first specify [Administrator's E-mail Address] in [File Transfer] in [System Settings].
- To use the device certificate for digitally signed PDFs, you must first specify the administrator's e-mail address so that it is the same as that registered as "Administrator's E-mail Address" in [System Settings].

Select the certificate to use for signatures.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Device Certificate] under "Security".
4. Select the certificate to be used for the electronic signature from the drop-down box in "PDF Digital Signature" or "PDF/A Digital Signature" under "Certification".

PDF Digital Signature: This can be attached to PDFs in formats other than PDF/A.

PDF/A Digital Signature: This can be attached to PDFs in the PDF/A format.

5. Click [OK].
6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].
If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.
7. Log out.

↓ Note

- If the selected device certificate expires, signatures cannot be attached to PDFs. Select a certificate that is within its valid period.
- The signature algorithm for the device certificate's digital signature that can be attached to PDF/A files is "sha1WithRSA-1024".

Configuring IPsec

For communication security, this machine supports IPsec. IPsec transmits secure data packets at the IP protocol level using the shared key encryption method, where both the sender and receiver retain the same key. This machine uses automatic key exchange to configure the pre-shared key for both parties. Using the auto exchange setting, you can renew the shared key exchange settings within a specified validity period, and achieve higher transmission security.

★ Important

- When "Inactive" is specified for "Exclude HTTPS Communication", access to Web Image Monitor can be lost if the key settings are improperly configured. In order to prevent this, you can specify IPsec to exclude HTTPS transmission by selecting "Active". When you want to include HTTPS transmission, we recommend that you select "Inactive" for "Exclude HTTPS Communication" after confirming that IPsec is properly configured. When "Active" is selected for "Exclude HTTPS Communication", even though HTTPS transmission is not targeted by IPsec, Web Image Monitor might become unusable when TCP is targeted by IPsec from the computer side.
- If you cannot access Web Image Monitor due to IPsec configuration problems, disable IPsec in System Settings on the control panel, and then access Web Image Monitor.
- For details about enabling and disabling IPsec using the control panel, see "Interface Settings", Connecting the Machine/ System Settings.
- IPsec is not applied to data obtained through DHCP, DNS, or WINS.
- IPsec for IPv4 is supported by Windows XP SP2 or later and Windows Server 2003/2003 R2. IPsec for both IPv4 and IPv6 is supported by Windows Vista/7/8, Windows Server 2008/2008 R2/2012, Mac OS X 10.4.8 and later, Red Hat Enterprise Linux WS 4.0 and Solaris 10. However, some setting items are not supported depending on the operating system. Make sure the IPsec settings you specify are consistent with the operating system's IPsec settings.

Encryption and Authentication by IPsec

IPsec consists of two main functions: the encryption function, which ensures the confidentiality of data, and the authentication function, which verifies the sender of the data and the data's integrity. This machine's IPsec function supports two security protocols: the ESP protocol, which enables both of the IPsec functions at the same time, and the AH protocol, which enables only the authentication function.

ESP protocol

The ESP protocol provides secure transmission through both encryption and authentication. This protocol does not provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH protocol

The AH protocol provides secure transmission through authentication of packets only, including headers.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH protocol + ESP protocol

When combined, the ESP and AH protocols provide secure transmission through both encryption and authentication. These protocols provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.
- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

Note

- Some operating systems use the term "Compliance" in place of "Authentication".

Encryption Key Auto Exchange Settings

For key configuration, this machine supports automatic key exchange to specify agreements such as the IPsec algorithm and key for both sender and receiver. Such agreements form what is known as an SA (Security Association). IPsec communication is possible only if the receiver's and sender's SA settings are identical.

If you use the auto exchange method to specify the encryption key, the SA settings are auto configured on both parties' machines. However, before setting the IPsec SA, the ISAKMP SA (Phase 1) settings are auto configured. After this, the IPsec SA (Phase 2) settings, which allow actual IPsec transmission, are auto configured.

Also, for further security, the SA can be periodically auto updated by applying a validity period (time limit) for its settings. This machine only supports IKEv1 for encryption key auto exchange.

Note that it is possible to configure multiple SAs.

Settings 1-4 and default setting

Using the auto exchange method, you can configure four separate sets of SA details (such as different shared keys and IPsec algorithms). In the default settings of these sets, you can include settings that the fields of sets 1 to 4 cannot contain.

When IPsec is enabled, set 1 has the highest priority and 4 has the lowest. You can use this priority system to target IP addresses more securely. For example, set the broadest IP range at the lowest priority (4), and then set specific IP addresses at a higher priority level (3 and higher). This way, when IPsec transmission is enabled for a specific IP address, the higher level settings will be applied.

IPsec Settings

IPsec settings for this machine can be made on Web Image Monitor. The following table explains individual setting items.

IPsec settings items

Setting	Description	Setting value
IPsec	Specify whether to enable or disable IPsec.	<ul style="list-style-type: none"> Active Inactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	<ul style="list-style-type: none"> Active Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.

The IPsec setting can also be made from the control panel.

Encryption key auto exchange security level

When you select a security level, certain security settings are automatically configured. The following table explains security level features.

Security level	Security level features
Authentication Only	Select this level if you want to authenticate the transmission partner and prevent unauthorized data tampering, but not perform data packet encryption. Since the data is sent in cleartext, data packets are vulnerable to eavesdropping attacks. Do not select this if you are exchanging sensitive information.

Security level	Security level features
Authentication and Low Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides less security than "Authentication and High Level Encryption".
Authentication and High Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides higher security than "Authentication and Low Level Encryption".

The following table lists the settings that are automatically configured according to the security level.

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Security Policy	Apply	Apply	Apply
Encapsulation Mode	Transport	Transport	Transport
IPsec Requirement Level	Use When Possible	Use When Possible	Always Require
Authentication Method	PSK	PSK	PSK
Phase 1 Hash Algorithm	MD5	SHA1	SHA256
Phase 1 Encryption Algorithm	DES	3DES	AES-128-CBC
Phase 1 Diffie-Hellman Group	2	2	2
Phase 2 Security Protocol	AH	ESP	ESP

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Phase 2 Authentication Algorithm	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256
Phase 2 Encryption Algorithm Permissions	Cleartext (NULL encryption)	3DES/AES-128/ AES-192/AES-256	AES-128/AES-192/ AES-256
Phase 2 PFS	Inactive	Inactive	2

5

Encryption key auto exchange settings items

When you specify a security level, the corresponding security settings are automatically configured, but other settings, such as address type, local address, and remote address must still be configured manually.

After you specify a security level, you can still make changes to the auto configured settings. When you change an auto configured setting, the security level switches automatically to "User Setting".

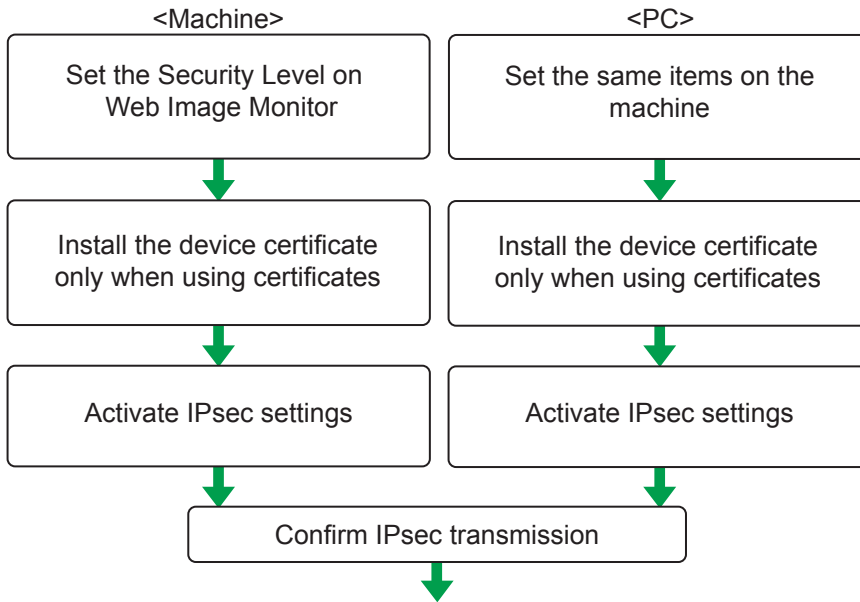
Setting	Description	Setting value
Address Type	Specify the address type for which IPsec transmission is used.	<ul style="list-style-type: none"> • Inactive • IPv4 • IPv6 • IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple addresses in IPv6, you can also specify an address range.	The machine's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.

Setting	Description	Setting value
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Security Policy	Specify how IPsec is handled.	<ul style="list-style-type: none"> • Apply • Bypass • Discard
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	<ul style="list-style-type: none"> • Transport • Tunnel <p>If you specify "Tunnel", you must then specify the "Tunnel End Point", which are the beginning and ending IP addresses. Set the same address for the beginning point as you set in "Local Address".</p>
IPsec Requirement Level	Specify whether to only transmit using IPsec, or to allow cleartext transmission when IPsec cannot be established. (auto setting)	<ul style="list-style-type: none"> • Use When Possible • Always Require

Setting	Description	Setting value
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	<ul style="list-style-type: none"> • PSK • Certificate <p>If you specify "PSK", you must then set the PSK text (using ASCII characters).</p> <p>If you are using "PSK", specify a PSK password using up to 32 ASCII characters.</p> <p>If you specify "Certificate", the certificate for IPsec must be installed and specified before it can be used.</p>
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 Hash Algorithm	Specify the Hash algorithm to be used in phase 1. (auto setting)	<ul style="list-style-type: none"> • MD5 • SHA1 • SHA256 • SHA384 • SHA512
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	<ul style="list-style-type: none"> • DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
Phase 1 Diffie-Hellman Group	Select the Diffie-Hellman group number used for IKE encryption key generation. (auto setting)	<ul style="list-style-type: none"> • 1 • 2 • 14
Phase 1 Validity Period	Specify the time period for which the SA settings in phase 1 are valid.	Set in seconds from 300 sec. (5 min.) to 172800 sec. (48 hrs.).

Setting	Description	Setting value
Phase 2 Security Protocol	Specify the security protocol to be used in Phase 2. To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH". (auto setting)	<ul style="list-style-type: none"> • ESP • AH • ESP+AH
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	<ul style="list-style-type: none"> • HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
Phase 2 Encryption Algorithm Permissions	Specify the encryption algorithm to be used in phase 2. (auto setting)	<ul style="list-style-type: none"> • Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256
Phase 2 PFS	Specify whether to activate PFS. Then, if PFS is activated, select the Diffie-Hellman group. (auto setting)	<ul style="list-style-type: none"> • Inactive • 1 • 2 • 14
Phase 2 Validity Period	Specify the time period for which the SA settings in phase 2 are valid.	Specify a period (in seconds) from 300 (5min.) to 172800 (48 hrs.).

Encryption Key Auto Exchange Settings Configuration Flow



CJD015

★ Important

- To use a certificate to authenticate the transmission partner in encryption key auto exchange settings, a device certificate must be installed.
- After configuring IPsec, you can use "Ping" command to check if the connection is established correctly. However, you cannot use "Ping" command when ICMP is excluded from IPsec transmission on the computer side. Also, because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.

Specifying Encryption Key Auto Exchange Settings

To change the transmission partner authentication method for encryption key auto exchange settings to "Certificate", you must first install and assign a certificate. For details about creating and installing a device certificate, see page 130 "Protecting the Communication Path via a Device Certificate". For the method of assigning installed certificates to IPsec, see page 157 "Selecting the certificate for IPsec".

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [IPsec] under "Security".
4. Click [Edit] under "Encryption Key Auto Exchange Settings".

5. Make encryption key auto exchange settings in [Settings 1].

If you want to make multiple settings, select the settings number and add settings.

6. Click [OK].**7. Select [Active] for "IPsec" in "IPsec".****8. Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS transmission.****9. Click [OK].****10. "Updating..." appears. Wait for about one or two minutes, and then click [OK].**

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

11. Log out.

Selecting the certificate for IPsec

Using Web Image Monitor, select the certificate to be used for IPsec. You must install the certificate before it can be used. For details about creating and installing a device certificate, see page 130 "Protecting the Communication Path via a Device Certificate".

1. Log in as the network administrator from Web Image Monitor.**2. Point to [Device Management], and then click [Configuration].****3. Click [Device Certificate] under "Security".****4. Select the certificate to be used for IPsec from the drop-down box in "IPsec" under "Certification".****5. Click [OK].**

The certificate for IPsec is specified.

6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. Log out.

Specifying the computer's IPsec settings

Configure the computer's IPsec SA settings, so that they exactly match the machine's security level on the machine. Setting methods differ according to the computer's operating system. The example procedure shown here uses Windows 7 when the "Authentication and Low Level Encryption" security level is selected.

1. On the [Start] menu, click [Control Panel], click [System and Security], and then click [Administrative Tools].

Under Windows 8, hover the mouse pointer over the top- or bottom-right corner of the screen, and then click [Settings], [Control Panel], [System and Security], and then [Administrative Tools].

If you are using Windows XP, on the [Start] menu, click [Control Panel], click [Performance and Maintenance], and then click [Administrative Tools].

2. Double-click [Local Security Policy].

If the "User Account Control" dialog box appears, click [Yes].

3. Click [IP Security Policies on Local Computer].

4. In the "Action" menu, click [Create IP Security Policy].

The IP Security Policy Wizard appears.

5. Click [Next].

6. Enter a security policy name in "Name", and then click [Next].

7. Clear the "Activate the default response rule" check box, and then click [Next].

8. Select "Edit properties", and then click [Finish].

9. In the "General" tab, click [Settings].

If you are using Windows XP, in the "General" tab, click [Advanced].

10. In "Authenticate and generate a new key after every", enter the same validity period (in minutes) that is specified on the machine in "Encryption Key Auto Exchange Settings Phase 1", and then click [Methods].

11. Check that the hash algorithm ("Integrity"), encryption algorithm ("Encryption") and "Diffie-Hellman Group" settings in "Security method preference order" all match those specified on the machine in "Encryption Key Auto Exchange Settings Phase 1".

If the settings are not displayed, click [Add].

12. Click [OK] twice.

13. Click [Add] in the "Rules" tab.

The Security Rule Wizard appears.

14. Click [Next].

15. Select "This rule does not specify a tunnel", and then click [Next].

16. Select the type of network for IPsec, and then click [Next].

17. For Windows XP, select the authentication method, and then click [Next]. For Windows 7/8, go to Step 18.

If you select "Certificate" for authentication method in "Encryption Key Auto Exchange Settings" on the machine, specify the device certificate. If you select "PSK", enter the same PSK text specified on the machine with the pre-shared key.

18. Click [Add] in the IP Filter List.

19. In [Name], enter an IP Filter name, and then click [Add].

The IP Filter Wizard appears.

20. Click [Next].

21. If required, enter a description of the IP filter, and then click [Next].

For Windows XP, go to Step 22.

22. Select "My IP Address" in "Source address", and then click [Next].

23. Select "A specific IP Address or Subnet" in "Destination address", enter the machine's IP address, and then click [Next].

If you are using Windows XP, select "A specific IP Address", and then click [Next].

24. Select the protocol type for IPsec, and then click [Next].

If you are using IPsec with IPv6, select "58" as the protocol number for the "Other" target protocol type.

25. Click [Finish].

26. Click [OK].

27. Select the IP filter that was just created, and then click [Next].

28. Click [Add].

Filter action wizard appears.

29. Click [Next].

30. In [Name], enter an IP Filter action name, and then click [Next].

31. Select "Negotiate security", and then click [Next].

32. Select "Allow unsecured communication if a secure connection connect be established.", and then [Next].

If you are using Windows XP, select "Fall back to unsecured communication", and then click [Next].

33. Select "Custom" and click [Settings].

34. In "Integrity algorithm", select the authentication algorithm that was specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".

35. In "Encryption algorithm", select the encryption algorithm that specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".

36. In Session key settings, select "Generate a new key every", and enter the validity period (in seconds) that was specified on the machine in "Encryption Key Auto Exchange Settings Phase 2".

37. Click [OK].

38. Click [Next].

39. Click [Finish].

40. Select the filter action that was just created, and then click [Next].

If you set "Encryption Key Auto Exchange Settings" to "Authentication and High Level Encryption", select the IP filter action that was just created, click [Edit], and then check "Use session key perfect forward secrecy (PFS)" on the filter action properties dialog box. If using PFS in Windows, the PFS group number used in phase 2 is automatically negotiated in phase 1 from the Diffie-Hellman group number (set in step 11). Consequently, if you change the security level specified automatic settings on the machine and "User Setting" appears, you must set the same the group number for "Phase 1 Diffie-Hellman Group" and "Phase 2 PFS" on the machine to establish IPsec transmission.

41. Select the authentication method, and then click [Next]. For Windows XP, go to Step 42.

If you select "Certificate" for authentication method in "Encryption Key Auto Exchange Settings" on the machine, specify the device certificate. If you select "PSK", enter the same PSK text specified on the machine with the pre-shared key.

42. Click [Finish].**43. Click [OK].**

If you are using Windows XP, click [Close].

The new IP security policy (IPsec settings) is specified.

44. Select the security policy that was just created, right-click, and then click [Assign].

The computer's IPsec settings are enabled.

Note

- To disable the computer's IPsec settings, select the security policy, right-click, and then click [Unassign].

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section explains telnet commands for IPsec. The default user name for logging into telnet is "admin". The password is not configured by default. For details about logging in to telnet and telnet operations, see "Remote Maintenance Using telnet", Connecting the Machine/ System Settings.

★ Important

- If you are using a certificate as the authentication method in encryption key auto exchange settings (IKE), install the certificate using Web Image Monitor. A certificate cannot be installed using telnet.

ipsec

To display IPsec related settings information, use the "ipsec" command.

Display current settings

```
msh> ipsec
```

Displays the following IPsec settings information:

- IPsec settings values
- Encryption key auto exchange settings, IKE setting 1-4 values
- Encryption key auto exchange settings, IKE default setting values

Display current settings portions

```
msh> ipsec -p
```

- Displays IPsec settings information in portions.

ipsec exclude

To display or specify protocols excluded by IPsec, use the "ipsec exclude" command.

Display current settings

```
msh> ipsec exclude
```

- Displays the protocols currently excluded from IPsec transmission.

Specify protocols to exclude

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Specify the protocol, and then enter [on] to exclude it, or [off] to include it for IPsec transmission. Entering [all] specifies all protocols collectively.

ipsec ike

To display or specify the encryption key auto exchange settings, use the "ipsec ike" command.

Display current settings

```
msh> ipsec ike {1|2|3|4|default}
```

- To display the settings 1-4, specify the number [1-4].
- To display the default setting, specify [default].
- Not specifying any value displays all of the settings.

Disable settings

```
msh> ipsec ike {1|2|3|4|default} disable
```

- To disable the settings 1-4, specify the number [1-4].
- To disable the default settings, specify [default].

Specify the user-specific local address / remote address.

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- Enter the separate setting number [1-4], and the address type to specify local and remote address.

- To set the local or remote address values, specify masklen by entering [/] and an integer 0-32 when settings an IPv4 address. When setting an IPv6 address, specify masklen by entering [/] and an integer 0-128.
- Not specifying an address value displays the current setting.

Specify the address type in default setting

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- Specify the address type for the default setting.
- To specify both IPv4 and IPv6, enter [any].

Security policy setting

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- Enter the separate setting number [1-4] or [default] and specify the security policy for the address specified in the selected setting.
- To apply IPsec to the relevant packets, specify [apply]. To not apply IPsec, specify [bypass].
- If you specify [discard], any packets to which IPsec can be applied are discarded.
- Not specifying a security policy displays the current setting.

Security protocol setting

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Enter the separate setting number [1-4] or [default] and specify the security protocol.
- To specify AH, enter [ah]. To specify ESP, enter [esp]. To specify AH and ESP, enter [dual].
- Not specifying a protocol displays the current setting.

IPsec requirement level setting

```
msh> ipsec ike {1|2|3|4|default} level {require|use}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec requirement level.
- If you specify [require], data will not be transmitted when IPsec cannot be used. If you specify [use], data will be sent normally when IPsec cannot be used. When IPsec can be used, IPsec transmission is performed.
- Not specifying a requirement level displays the current setting.

Encapsulation mode setting

```
msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}
```

- Enter the separate setting number [1-4] or [default] and specify the encapsulation mode.
- To specify transport mode, enter [transport]. To specify tunnel mode, enter [tunnel].
- If you have set the address type in the default setting to [any], you cannot use [tunnel] in encapsulation mode.
- Not specifying an encapsulation mode displays the current setting.

Tunnel end point setting

```
msh> ipsec ike {1|2|3|4|default} tunneladdr "beginning IP address" "ending IP address"
```

- Enter the separate setting number [1-4] or [default] and specify the tunnel end point beginning and ending IP address.
- Not specifying either the beginning or ending address displays the current setting.

IKE partner authentication method setting

```
msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}
```

- Enter the separate setting number [1-4] or [default] and specify the authentication method.
- Specify [psk] to use a shared key as the authentication method. Specify [rsasig] to use a certificate at the authentication method.
- You must also specify the PSK character string when you select [psk].
- Note that if you select "Certificate", the certificate for IPsec must be installed and specified before it can be used. To install and specify the certificate use Web Image Monitor.

PSK character string setting

```
msh> ipsec ike {1|2|3|4|default} psk "PSK character string"
```

- If you select PSK as the authentication method, enter the separate setting number [1-4] or [default] and specify the PSK character string.
- Specify the character string in ASCII characters. There can be no abbreviations.

ISAKMP SA (phase 1) hash algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) hash algorithm.
- Not specifying the hash algorithm displays the current setting.

ISAKMP SA (phase 1) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) encryption algorithm.
- Not specifying an encryption algorithm displays the current setting.

ISAKMP SA (phase 1) Diffie-Hellman group setting

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

ISAKMP SA (phase 1) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime "validity period"
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

IPsec SA (phase 2) authentication algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-sha384|hmac-sha512}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) authentication algorithm.
- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.
- Not specifying an authentication algorithm displays the current setting.

IPsec SA (phase 2) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) encryption algorithm.
- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.
- Not specifying an encryption algorithm displays the current setting.

IPsec SA (phase 2) PFS setting

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

IPsec SA (phase 2) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime "validity period"
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

Reset setting values

```
msh> ipsec ike {1|2|3|4|default|all} clear
```

- Enter the separate setting number [1-4] or [default] and reset the specified setting. Specifying [all] resets all of the settings, including default.

Configuring IEEE 802.1X Authentication

IEEE 802.1X is an authentication function that can be used with both wired and wireless networks. Authentication is performed by the authentication server (RADIUS server).

You can select four types of EAP authentication method: EAP-TLS, LEAP, EAP-TTLS and PEAP. Note that each EAP authentication method has different configuration settings and authentication procedures.

Types and requirements of certificates are as follows:

EAP type	Required certificates
EAP-TLS	Site certificate, Device certificate (IEEE 802.1X Client Certificate)
LEAP	-
EAP-TTLS	Site certificate
PEAP	Site certificate
PEAP (Phase 2 is for TLS only)	Site certificate, Device certificate (IEEE 802.1X Client Certificate)

5

Installing a Site Certificate

Install a site certificate (root CA certificate) for verifying the reliability of the authentication server. You need to have at least a certificate issued by the certificate authority who signed the server certificate or a certificate from a higher certificate authority.

Only PEM (Base64-encoded X.509) site certificates can be imported.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Site Certificate] under "Security".
4. Click [Browse] for "Site Certificate to Import", and then select the CA certificate you obtained.
5. Click [Open].
6. Click [Import].
7. Check that the imported certificate's [Status] shows "Trustworthy".

If [Site Certificate Check] shows [Active], and the [Status] of the certificate shows [Untrustworthy], communication might not be possible.

8. Click [OK].
9. Log out.

Selecting the Device Certificate

Select the certificate to use under IEEE 802.1X from among the device certificates created and installed in advance on the machine. For details about creating and installing a device certificate, see page 130 "Protecting the Communication Path via a Device Certificate".

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Device Certificate] under "Security".
4. Select the certificate to be used for IEEE 802.1X from the drop-down box in "IEEE 802.1X" under "Certification".
5. Click [OK].
6. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

7. Log out.

5

Setting Items of IEEE 802.1X for Ethernet

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [IEEE 802.1X] under "Security".
4. In "User Name", enter the user name set in the RADIUS server.
5. Enter the domain name in "Domain Name".
6. Select "EAP Type". Configurations differ according to the EAP Type.

EAP-TLS

- Make the following settings according to the operating system you are using:
 - Select [On] or [Off] in "Authenticate Server Certificate".
 - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
 - Enter the host name of the RADIUS server on "Server ID".
 - Select [On] or [Off] in "Permit Sub-domain".

LEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

EAP-TTLS

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

- Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".
Certain methods might not be available, depending on the RADIUS server you want to use.
- Make the following settings according to the operating system you are using:
 - Select [On] or [Off] in "Authenticate Server Certificate".
 - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
 - Enter the host name of the RADIUS server in "Server ID".
 - Select [On] or [Off] in "Permit Sub-domain".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
If [TLS] is selected for "Phase 2 Method", you do not need to specify a password.
- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".
When you select [TLS], you must install "IEEE 802.1X Client Certificate".
- Make the following settings according to the operating system you are using:
 - Select [On] or [Off] in "Authenticate Server Certificate".
 - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
 - Enter the host name of the RADIUS server on "Server ID".
 - Select [On] or [Off] in "Permit Sub-domain".

7. Click [OK].

8. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

9. Click [Interface Settings] under "Interface".

10. Select [Active] in "Ethernet Security".

11. Click [OK].

12. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

13. Log out.

Note

- If there is a problem with settings, you might not be able to communicate with the machine. In such a case, access [Print List] in [Interface Settings] on the control panel, and then print the network summary to check the status.
- If you cannot identify the problem, execute [Restore IEEE 802.1X Authentication to Defaults] in [Network] in [Interface Settings] on the control panel, and then repeat the procedure.

Setting Items of IEEE 802.1X for Wireless LAN

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [IEEE 802.1X] under "Security".
4. In "User Name", enter the user name set in the RADIUS server.
5. Enter the domain name in "Domain Name".
6. Select "EAP Type". Configurations differ according to the EAP Type.

EAP-TLS

- Make the following settings according to the operating system you are using:
 - Select [On] or [Off] in "Authenticate Server Certificate".
 - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
 - Enter the host name of the RADIUS server on "Server ID".
 - Select [On] or [Off] in "Permit Sub-domain".

LEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

EAP-TTLS

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
- Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".

Certain methods might not be available, depending on the RADIUS server you want to use.

- Make the following settings according to the operating system you are using:
 - Select [On] or [Off] in "Authenticate Server Certificate".
 - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
 - Enter the host name of the RADIUS server in "Server ID".
 - Select [On] or [Off] in "Permit Sub-domain".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
If [TLS] is selected for "Phase 2 Method", you do not need to specify a password.
- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".
When you select [TLS], you must install "IEEE 802.1X Client Certificate".
- Make the following settings according to the operating system you are using:
 - Select [On] or [Off] in "Authenticate Server Certificate".
 - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
 - Enter the host name of the RADIUS server on "Server ID".
 - Select [On] or [Off] in "Permit Sub-domain".

5

7. Click [OK].**8. "Updating..." appears. Wait for about one or two minutes, and then click [OK].**

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

9. Click [Wireless LAN Settings] under "Interface".**10. Select [Wireless LAN] in "LAN Type".****11. Select [Infrastructure Mode] in "Communication Mode".****12. Enter the alphanumeric characters (a-z, A-Z, or 0-9) in [SSID] according to the access point you want to use.****13. Select [WPA2] in "Security Method".****14. Select [WPA2] in "WPA2 Authentication Method".****15. Click [OK].****16. "Updating..." appears. Wait for about one or two minutes, and then click [OK].**

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

17. Log out.**Note**

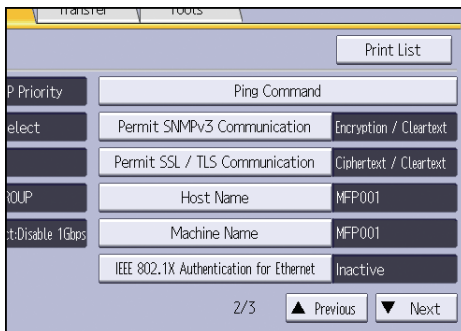
- If there is a problem with settings, you might not be able to communicate with the machine. In such a case, access [Print List] in [Interface Settings] on the control panel, and then print the network summary to check the status.
- If you cannot identify the problem, execute [Restore IEEE 802.1X Authentication to Defaults] in [Network] in [Interface Settings] on the control panel, and then repeat the procedure.

SNMPv3 Encryption

When using SmartDeviceMonitor for Admin/Device Manager NX Lite or another application that communicates via SNMPv3, you can encrypt the data transmitted.

By making this setting, you can protect data from being tampered with.

1. Log in as the network administrator from the control panel.
2. Press [System Settings].
3. Press [Interface Settings].
4. Press [▼Next].
5. Press [Permit SNMPv3 Communication].



6. Press [Encryption Only].
7. Press [OK].
8. Log out.

↓ Note

- To use SmartDeviceMonitor for Admin/Device Manager NX Lite for encrypting the data for specifying settings, you need to specify the network administrator's [Encryption Password] setting and [Encryption Password] in [SNMP Authentication Information] in SmartDeviceMonitor for Admin/Device Manager NX Lite, in addition to specifying [Permit SNMPv3 Communication] on the machine. For details about specifying [Encryption Password] in SmartDeviceMonitor for Admin/Device Manager NX Lite, see SmartDeviceMonitor for Admin/Device Manager NX Lite Help.
- 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 19 "Registering and Changing Administrators".

Encrypting Transmitted Passwords

Configuring the driver encryption key and password encryption for IPP authentication enables communication with encrypted passwords as well as increasing the security against password cracking. In order to further enhance security, we recommend using IPsec, SNMPv3 and SSL/TLS all together.

Also, encrypt the login password for administrator authentication and user authentication.

Driver Encryption Key

This key is a character string used for encrypting login passwords or document passwords sent from each driver when user authentication is ON.

To encrypt the login password, specify the driver encryption key on the machine and on the printer driver installed in the user's computer.

Password for IPP Authentication

To encrypt the IPP Authentication password on Web Image Monitor, set "Authentication" to [DIGEST], and then specify the IPP Authentication password set on the machine.

You can use telnet or FTP to manage passwords for IPP authentication, although it is not recommended.

Note

- For details on encrypting the login passwords used for administrator authentication, see page 19 "Registering and Changing Administrators".

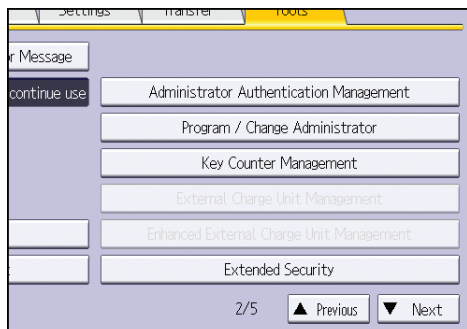
Specifying a Driver Encryption Key

Specify the driver encryption key on the machine.

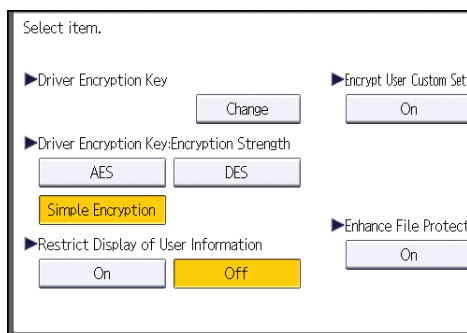
This setting enables encrypted transmission of login passwords and strengthens the security against password cracking.

1. **Log in as the network administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**

5. Press [Extended Security].



6. For "Driver Encryption Key", press [Change].



7. Enter the driver encryption key, and then press [OK].

Enter the driver encryption key using up to 32 alphanumeric characters.

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 is specified on the machine.

8. Press [OK].

9. Log out.

Note

- For details about specifying the encryption key on the printer driver or TWAIN driver, see the driver help.
- For details about specifying the encryption key on the LAN-Fax driver, see the LAN-Fax driver Help.

Specifying an IPP Authentication Password

Specify an IPP authentication password for this machine. This setting enables encrypted transmission of IPP authentication passwords and strengthens the security against password cracking.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [IPP Authentication] under "Security".
4. Select [DIGEST] from the "Authentication" list.
5. Enter the user name in the "User Name" box.
6. Enter the password in the "Password" box.
7. Click [OK].

IPP authentication is specified.

8. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

9. Log out.

Kerberos Authentication Encryption Setting

You can specify encrypted transmission between the machine and the key distribution center (KDC) server when Kerberos authentication is enabled.

Using Kerberos authentication with Windows or LDAP authentication, LDAP search, etc., ensures safe communication.

The supported encryption algorithm differs depending on the type of KDC server. Select the algorithm that suits your environment.

KDC server	Supported encryption algorithms
Windows Server 2003 Active Directory	<ul style="list-style-type: none"> • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	<ul style="list-style-type: none"> • AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2 Windows Server 2012	<ul style="list-style-type: none"> • AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	<ul style="list-style-type: none"> • AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • DES3-CBC-SHA1 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5

* To use Kerberos authentication, it must be enabled in the operating system settings.

1. Log in as the network administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Kerberos Authentication] under "Device Settings".
4. Select the encryption algorithm you want to enable.
One or more encryption algorithm must always be selected.
5. Click [OK].

6. Log out.

6. Preventing the Leaking of Documents


This chapter explains how to protect document data stored in the machine or printed using the machine.

Managing Folders

This section explains how to manage the folders in Document Server: how to delete folders, change their passwords, and unlock them when locked.

Deleting Folders

This can be done by the file administrator or a user.

To delete a folder with  icon next to it, the folder's password is required.

If a user has forgotten the password to access the folder, the file administrator can change it.

The file administrator can delete folders without using the password.

Folders containing files which the user does not have permission to delete cannot be deleted.

The shared folder cannot be deleted.

1. **Log in as the file administrator or a user from the control panel.**
2. **Close the initial settings screen.**

- When using the standard operation panel

Press the [User Tools/Counter] key.

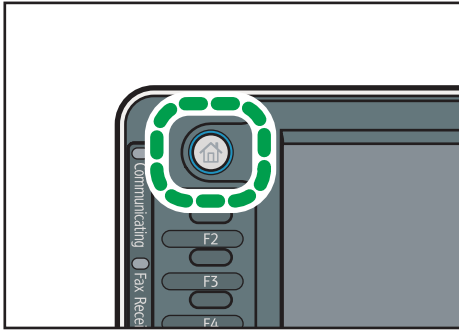
- When using the Smart Operation Panel

Press [User Tools/Counter] () on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

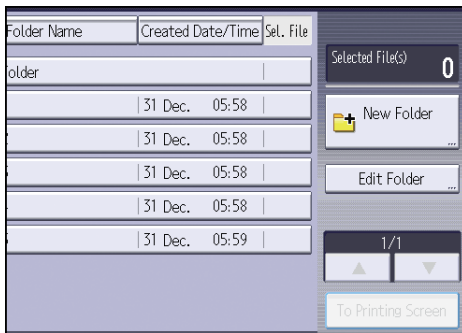
3. **Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.**

If the message "You do not have the privileges to use this function." appears, press [Exit].



CXX002

4. Press [Edit Folder].



6

5. Select the folder.

6. Press [Delete].

7. If a password entry screen appears, enter the password of the folder, and then press [OK].

The password entry screen does not appear if the file administrator is logged in.

8. Press [Delete].

9. Log out.

Note

- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Changing the Password of a Folder


This can be specified by the file administrator or a user.

If the password to access the folder has been forgotten, the file administrator can change it.

A password cannot be specified for the shared folder.

1. Log in as the file administrator or a user from the control panel.

2. Close the initial settings screen.

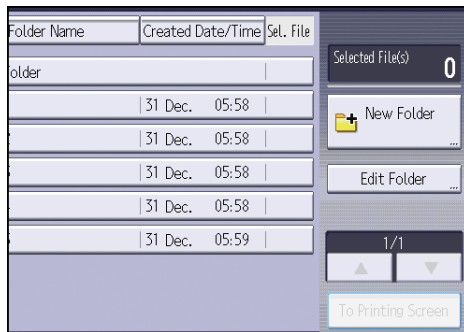
- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

4. Press [Edit Folder].



5. Select the folder.

6. Press [Change Password].

7. If a password entry screen appears, enter the password of the folder, and then press [OK].

The password entry screen does not appear if the file administrator is logged in.

8. Enter the new password for the folder, and then press [OK].

You can use 4 to 8 numbers as the password for the folder.

9. Re-enter the password for confirmation, and then press [OK].

The  icon appears next to a folder protected by password.

10. Log out.

Note

- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Unlocking Folders


Only the file administrator can unlock folders.

If you specify [On] for "Enhance File Protection", the folder will be locked and become inaccessible if an invalid password is entered ten times. This section explains how to unlock folders.

"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see page 257 "Specifying the Extended Security Functions".

1. Log in as the file administrator from the control panel.

2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

4. Press [Edit Folder].

5. Select the folder.

The  icon appears next to a folder locked by the Enhance File Protection function.

6. Press [Unlock].

The  icon changes to the  icon.

7. Press [Unlock].

8. Log out.

Note

- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Managing Stored Files

This section describes how to specify access permissions for stored files.

You can specify who is allowed to access stored scan files and files stored in Document Server.

This can prevent activities such as printing or sending of stored files by unauthorized users.

You can also specify which users can change or delete stored files.

To limit the use of stored files, you can specify four types of access permissions.

Types of access permission

Access permission	Description
Read-only	In addition to checking the content of and information about stored files, you can also print and send the files.
Edit	You can change the print settings for stored files. This includes permission to view files.
Edit / Delete	You can delete stored files. This includes permission to view and edit files.
Full Control	You can specify the user and access permission. This includes permission to view, edit, and edit / delete files.

Password for stored files

- Passwords for stored files can be specified by the file administrator or owner. You can obtain greater protection against the unauthorized use of files. For details about assigning a password to a stored file, see page 187 "Specifying Passwords for Stored Files".
- Even if user authentication is not set, passwords for stored files can be set.

Note

- Files can be stored by any user who is allowed to use Document Server, copy function, scanner function, fax function or printer function.
- Using Web Image Monitor, you can check the content of stored files. For details, see Web Image Monitor Help.
- The default access permission for the owner is "Read-only". You can also specify the access permission.
- The file administrator not only configures access permissions, but can also delete stored files. For details on the methods of deleting documents, see "Deleting Stored Documents", Copy/ Document Server.

Configuring Access Permission for Each Stored File

This can be specified by the file administrator or owner.

Specify the users and their access permissions for each stored file.

★ Important

- If files become inaccessible, reset their access permission as the owner. This can also be done by the file administrator. If you want to access a file but do not have access permission, ask the owner.
- The file administrator can change the owner of a document using the document's [Change Access Priv.] setting. This setting also allows the file administrator to change the access privileges of the owner and other users.
- The document owner and users with the [Full Control] privilege for the document can change the access privileges of the owner and other users under the [Change Access Priv.] setting.

1. Log in as the file administrator or the owner from the control panel.

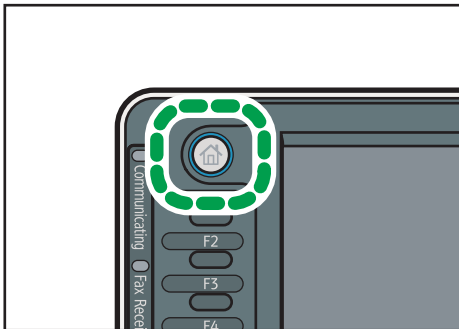
2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].



CXX002

4. Select the folder.

No.	Folder Name	Created Date/Time	Sel. File
	Shared Folder		
001	User001	31 Dec. 05:58	
002	User002	31 Dec. 05:58	
003	User003	31 Dec. 05:58	
004	User004	31 Dec. 05:58	
005	User005	31 Dec. 05:59	
006	User006	02 Dec. 08:46	

5. Select the file.

Type	User Name	File Name	Date	Page	Order
<input type="checkbox"/>	user1	ICOPY0005	01 Dec.	5	
<input type="checkbox"/>	user1	ICOPY0004	01 Dec.	5	
<input type="checkbox"/>	user1	ICOPY0003	01 Dec.	5	
<input type="checkbox"/>	user1	ICOPY0002	01 Dec.	5	
<input type="checkbox"/>	user1	ICOPY0001	01 Dec.	5	

6. Press [Change File Info.].

File Name	Date	Page	Order
ICOPY0005	01 Dec.	5	1
ICOPY0004	01 Dec.	5	
ICOPY0003	01 Dec.	5	
ICOPY0002	01 Dec.	5	
ICOPY0001	01 Dec.	5	

Details

Preview

Change File Info. ...

Delete File

Print Specified Page...

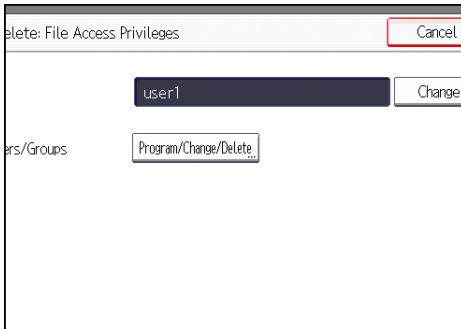
Page 2 of 1 Sided Settings

1/1

To Printing Screen

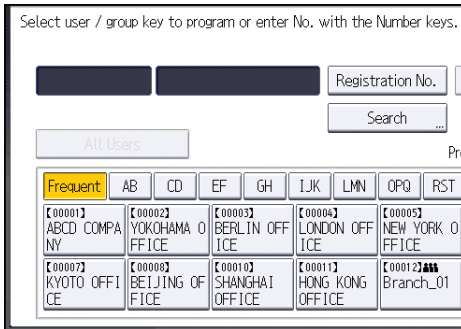
7. Press [Change Access Priv.].

8. Press [Program/Change/Delete].



9. Press [New Program].

10. Select the users or groups to whom you want to assign access permission.

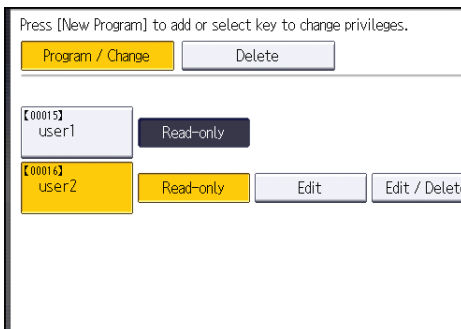


You can select more than one user.

By pressing [All Users], you can select all the users.

11. Press [Exit].

12. Select the user to whom you want to assign access permission, and then select the permission.



Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].

13. Press [Exit].

14. Press [OK].

15. Log out.

↓ Note

- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.
- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.


Changing the Owner of a Document

Use this procedure to change the owner of a document.

Only the file administrator can change the owner of a document.

1. Log in as the file administrator from the control panel.

2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

4. Select the folder.

5. Select the file.

6. Press [Change File Info.].

7. Press [Change Access Priv.].

8. Press [Change] for "Owner".

9. Select the user you want to register.

10. Press [Exit].

11. Press [OK].

12. Log out.

Configuring Access Permission for Each User for Stored Files

This can be specified by the user administrator or owner.

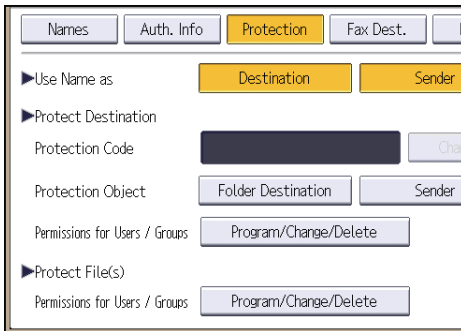
Specify the users and their access permission to files stored by a particular user.

This makes managing access permission easier than specifying and managing access permissions for each stored file.

★ Important

- If files become inaccessible, be sure to enable the user administrator, so that the user administrator can reset the access permission for the files in question.

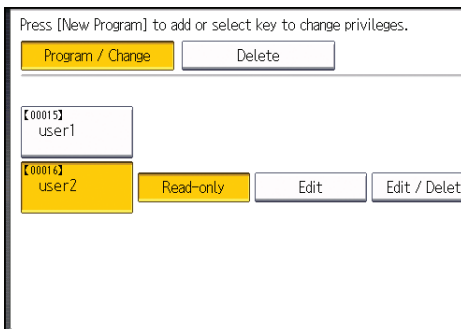
1. The user administrator or the owner logs in from the control panel.
2. Press [Address Book Mangmnt].
3. Select the user.
4. Press [Protection].
5. Under "Protect File(s)", press [Program/Change/Delete] for "Permissions for Users / Groups".



6. Press [New Program].
7. Select the users or groups to register.

You can select more than one user.

By pressing [All Users], you can select all the users.
8. Press [Exit].
9. Select the user to whom you want to assign access permission, and then select the permission.



Select the access permission from [Read-only], [Edit], [Edit / Delete], or [Full Control].

10. Press [Exit].

11. Press [OK].

12. Press [Exit].

13. Log out.

↓ Note

- The "Edit", "Edit / Delete", and "Full Control" access permissions allow a user to perform high level operations that could result in loss of or changes to sensitive information. We recommend you grant only the "Read-only" permission to general users.
- When using the Smart Operation Panel, you can display the Address Book screen by pressing the [Address Book Management] icon on the Home screen 4.

Specifying Passwords for Stored Files

This can be specified by the file administrator or owner.

1. The file administrator or the owner logs in from the control panel.

2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

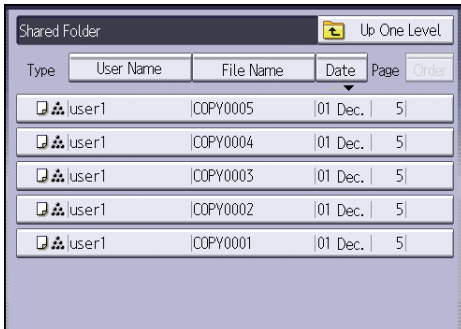
3. Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

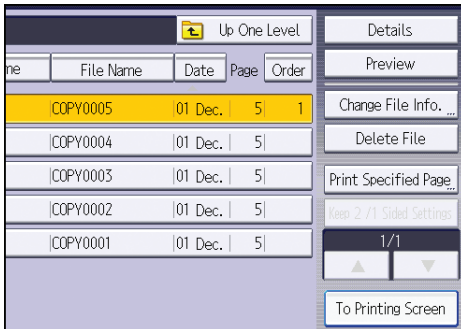
4. Select the folder.

No.	Folder Name	Created Date/Time	Set. File
	Shared Folder		
001	User001	31 Dec. 05:58	
002	User002	31 Dec. 05:58	
003	User003	31 Dec. 05:58	
004	User004	31 Dec. 05:58	
005	User005	31 Dec. 05:59	
006	User006	02 Dec. 08:46	

5. Select the file.



6. Press [Change File Info.].



7. Press [Change Password].

8. Enter the new password for the stored file, and then press [OK].

You can use 4 to 8 numbers as the password for the stored file.

9. Re-enter the password for confirmation, and then press [OK].

The  icon appears next to a stored file protected by password.

10. Press [OK].

11. Log out.

Unlocking Stored Files


Only the file administrator can unlock files.

If you specify "Enhance File Protection", the file will be locked and become inaccessible if an invalid password is entered ten times. This section explains how to unlock files.

"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see page 257 "Specifying the Extended Security Functions".

1. Log in as the file administrator from the control panel.

2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Document Server] icon on the screen.

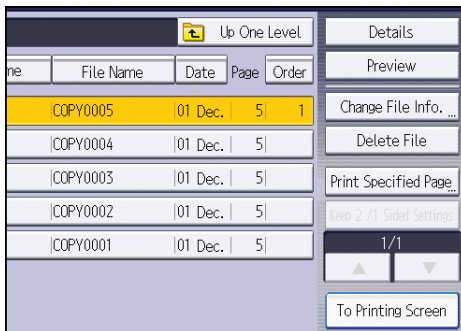
If the message "You do not have the privileges to use this function." appears, press [Exit].

4. Select the folder.

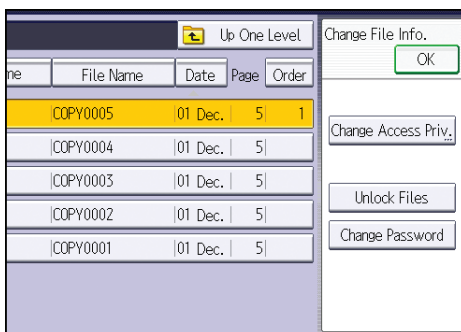
5. Select the file.

The  icon appears next to a file locked by the Enhance File Protection function.

6. Press [Change File Info.].



7. Press [Unlock Files].



8. Press [Yes].

The  icon changes to the  icon.

9. Press [OK].

10. Log out.

Managing Locked Print Files

Depending on the location of the machine, it is difficult to prevent unauthorized persons from viewing prints lying in the machine's output trays. When printing confidential documents, use the Locked Print function.

Locked Print

- Using the printer's Locked Print function, store files in the machine as Locked Print files and then print them from the control panel and retrieve them immediately, preventing others from viewing them.

Note

- Confidential documents can be printed regardless of the user authentication settings.
- To store files temporarily, select [Stored Print] in the printer driver. If you select [Stored Print (Shared)], you can also share these files.
- For details on how to use the Locked Print function, see "Locked Print", Print.

6

Deleting Locked Print Files


This can be specified by the file administrator or owner.

For the owner to delete a Locked Print file, the password to access the file is required. If the owner has forgotten the password, the file administrator can change it.

The password is not required for the file administrator to delete Locked Print files.

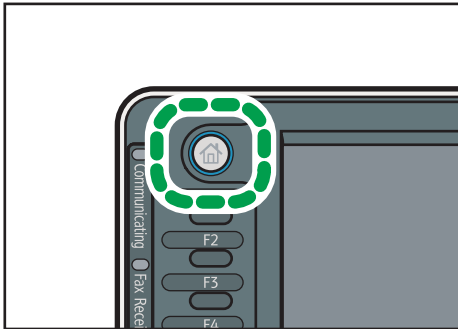
1. Log in as the file administrator or the owner from the control panel.

2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] () on the top right of the screen.

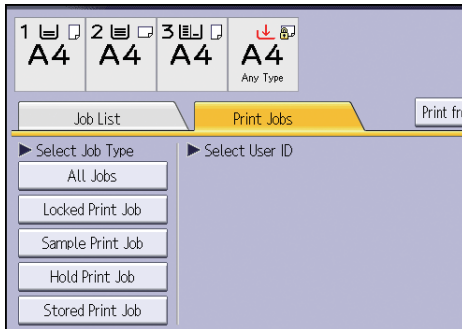
If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Printer] icon on the screen.

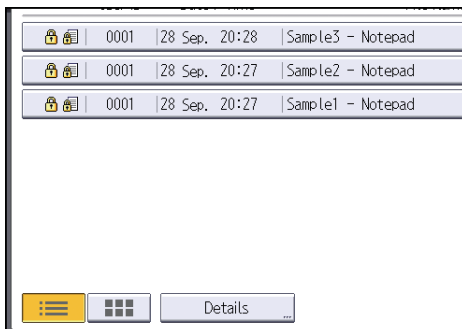


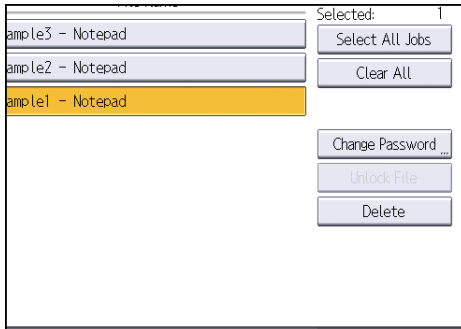
CXX002

4. Press [Print Jobs].
5. Press [Locked Print Job].



6. Select the file.



7. Press [Delete].**8. If a password entry screen appears, enter the password of the Locked Print file, and then press [OK].**

The password entry screen does not appear if the file administrator is logged in.

9. Press [Yes].**10. Log out.****Note**

- You can configure this machine to delete stored files automatically by setting the "Auto Delete Temporary Print Jobs" option to [On]. For details about "Auto Delete Temporary Print Jobs", see "Data Management", Print.
- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Changing the Password of a Locked Print File

This can be specified by the file administrator or owner.

If the owner has forgotten the password, the file administrator can change it.

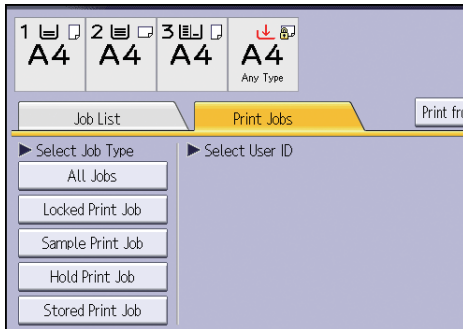
1. Log in as the file administrator or the owner from the control panel.**2. Close the initial settings screen.**

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

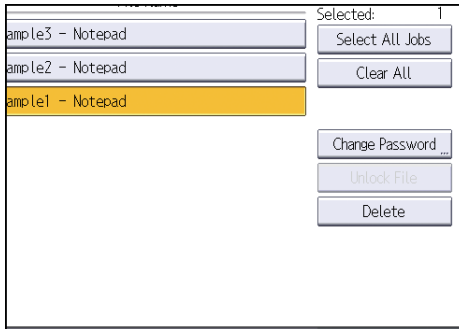
3. Press the [Home] key on the control panel, and press the [Printer] icon on the screen.**4. Press [Print Jobs].**

5. Press [Locked Print Job].



6. Select the file.

7. Press [Change Password].



8. If a password entry screen appears, enter the password for the stored file, and then press [OK].

The password entry screen will not appear if the file administrator is logged in.

9. Enter the new password for the stored file, and then press [OK].

10. Re-enter the password for confirmation, and then press [OK].

11. Log out.

↓ Note

- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Unlocking a Locked Print File

Only the file administrator can unlock files.

If you specify [On] for "Enhance File Protection", the file will be locked and become inaccessible if an invalid password is entered ten times. This section explains how to unlock files.

"Enhance File Protection" is one of the extended security functions. For details about this and other extended security functions, see page 257 "Specifying the Extended Security Functions".

1. Log in as the file administrator from the control panel.

2. Close the initial settings screen.

- When using the standard operation panel
Press the [User Tools/Counter] key.
- When using the Smart Operation Panel
Press [User Tools/Counter] (⚙️) on the top right of the screen.

If the message "You do not have the privileges to use this function." appears, press [Exit].

3. Press the [Home] key on the control panel, and press the [Printer] icon on the screen.

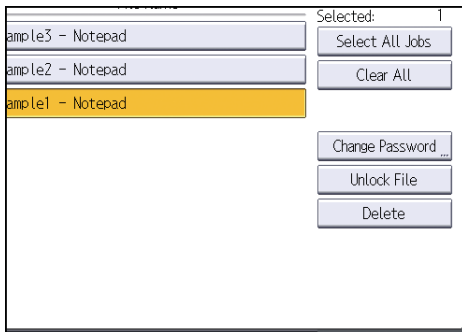
4. Press [Print Jobs].

5. Press [Locked Print Job].

6. Select the file.

The  icon appears next to a file locked by the Enhance File Protection function.

7. Press [Unlock File].



8. Press [Yes].

The  icon disappears.

9. Log out.

 **Note**

- This can also be specified via Web Image Monitor. For details, see Web Image Monitor Help.

Unauthorized Copy Prevention / Data Security for Copying

The copier, Document Server, and printer functions let you embed a pattern in a printed copy to discourage or prevent unauthorized copying.

If the Unauthorized Copy Prevention function is enabled, embedded text patterns (for instance, a warning message such as "No Copying") are displayed when documents are copied illegally. Accordingly, unauthorized copying can be prevented.

If the Data Security for Copying function is used and settings for special patterns embedded in documents are enabled, copies of documents with embedded patterns are printed with gray overprint. Accordingly, information leakage can be prevented. To protect documents by gray overprint, the copier or multi-function printer must be installed with the Copy Data Security Unit.

If a machine installed with the Copy Data Security Unit detects a file protected by the Data Security for Copying function, the machine beeps and logs the unauthorized copying.

For more information, see the information below:

Using Unauthorized Copy Prevention

1. On the machine, enable printing of the embedded pattern. The settings must be configured by the machine administrator. For details about how to configure the setting, see page 196 "Enabling Pattern Printing".
2. Specify the settings for unauthorized copy prevention in the copier, Document Server, or printer function. The privilege to specify the setting depends on the setting specified in [Compulsory Unauthorized Copy Prevention]. For details, see page 196 "Enabling Pattern Printing".

Using Data Security for Copying

1. On the machine, enable the embedded pattern print setting. The settings must be configured by the machine administrator. For details about how to configure the setting, see page 196 "Enabling Pattern Printing".
2. Specify the settings for data security for copying in the copier, Document Server, or printer function. The privilege to specify the setting depends on the setting specified in [Compulsory Unauthorized Copy Prevention]. For details, see page 196 "Enabling Pattern Printing".
3. Configure the "Detect Data Security for Copying" setting for printed copies, so that documents are printed with gray overprint when they are illegally copied, faxed, scanned, or stored in the machine. The setting must be configured by the machine administrator. For details about how to configure the setting, see page 197 "Enabling Detect Data Security for Copying".

Note

- When copying, the thickness of an embedded pattern may be uneven due to the original type setting. If this happens, change the original type setting to [Text] or [Photo].

Enabling Pattern Printing

You can enable embedded pattern printing to discourage or prevent unauthorized copying.

Enabling embedded pattern printing in the Copier/Document Server functions

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.
5. Select either [Unauthorized Copy Prevention Printing: Copier] or [Unauthorized Copy Prevention Printing: Document Server].
6. Press [Change] for "Compulsory Unauthorized Copy Prevention".
7. Specify whether or not to make printing of the embedded pattern mandatory.

- [Off]

Printing of the embedded pattern is not mandatory.

From the Copier/Document Server screen, users can specify whether or not to print with the embedded pattern and can specify its settings.

- [On:User Can Chng. Some Setg.]

Printing of the embedded pattern is mandatory.

From the Copier/Document Server screen, users can specify the embedded pattern settings except for type, color, and thickness.

- [On:User Cannot Change Setg.]

Printing of the embedded pattern is mandatory.

Users cannot specify the embedded pattern settings from the Copier/Document Server screen.

8. Press [OK] twice.

9. Log out.

↓ Note

- For details of the settings to specify the pattern using the machine, see "Administrator Tools", Connecting the Machine/ System Settings.

Enabling embedded pattern printing in the Printer function

1. Log in as the machine administrator from the control panel.

2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.
5. Press [Unauthorized Copy Prevention Printing: Printer].
6. Press [Change] for "Unauthorized Copy Prevention Setting".
7. Press [On], and then press [OK].
8. Press [Change] for "Compulsory Unauthorized Copy Prevention".
9. Specify whether or not to make printing of the embedded pattern mandatory.

- [Driver / Command]

Printing of the embedded pattern is not mandatory.

Using the printer driver, users can choose whether or not to print with the embedded pattern and can specify its settings.

- [Driver/Command (Most Settings)]

Printing of the embedded pattern is mandatory.

Using the printer driver, users can specify the embedded pattern settings except for type, color, and thickness.

- [Machine Setting(s)]

Printing of the embedded pattern is mandatory.

Users cannot specify the embedded pattern settings using the printer driver.

10. Press [OK] twice.

11. Log out.

Note

- For details of the settings to specify the pattern using the machine, see "Administrator Tools", Connecting the Machine/ System Settings.

Enabling Detect Data Security for Copying

To use this function, the Copy Data Security Unit must be installed.

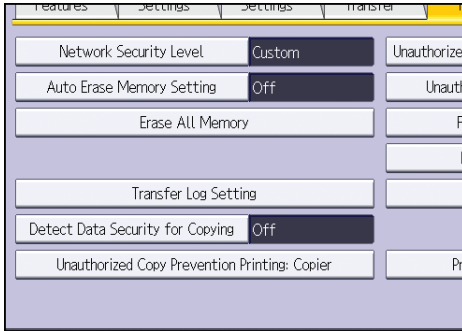
If a document printed is copied, faxed, scanned, or stored in the Document Server, the copy is grayed out.

Important

- If a document that is not copy-guarded is copied, faxed, scanned, or stored, the copy or stored file is not grayed out.

1. Log in as the machine administrator from the control panel.

2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] three times.
5. Press [Detect Data Security for Copying].



6. Press [On].
If you do not want to specify "Detect Data Security for Copying", select [Off].
7. Press [OK].
8. Log out.

Printing User Information on Paper

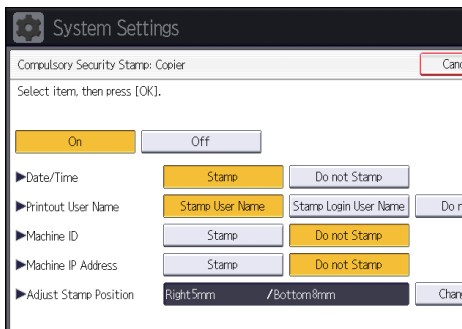
The start time of the print job, information on the person who prints it (name or login user name), machine number and machine's IP address can be compulsorily embedded on printed sheets. This function is called Compulsory Security Stamp.

Always printing out information on the person printing the job is effective for discouraging information leakage. It can also be used for identifying sources of information leakage.

Compulsory Security Stamp can be used with copying, Document Server, faxing and printing.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] four times.
5. Select the function(s) for Compulsory Security Stamp.
 - To set the copy function to be stamped, press [Compulsory Security Stamp:Copier].
 - To set the Document Server to be stamped, press [Compulsory Security Stamp:Doc. Srvr.].
 - To set the fax function to be stamped, press [Compulsory Security Stamp:Facsimile].
 - To set the printer function to be stamped, press [Compulsory Security Stamp:Printer].
6. Press [On], and then select the data to be stamped.

To turn Compulsory Security Stamp off, press [Off].



- Date/Time
 - The job start time will be printed.
- Printout User Name
 - These will be printed if user authentication is enabled.
 - Stamp User Name
 - The "Name" in the "Names" in the Address Book will be printed.
 - Stamp Login User Name

The user code or login user name in "Auth. Info" in the address book will be printed.

- Machine ID

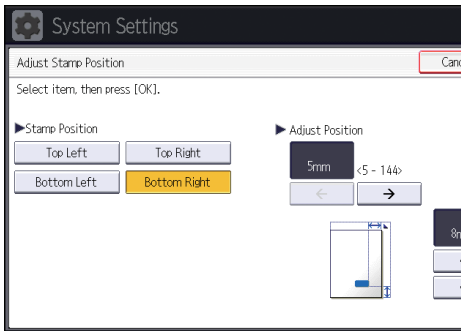
The numbers displayed as the "Serial No. of Machine" in [Inquiry] will be printed.

- Machine IP Address

The machine's IP address will be printed. If there are both IPv4 and IPv6 addresses, the IPv4 address will be printed. If no IP address has been configured, this will be left blank.

7. Press [Change] for "Adjust Stamp Position".

8. Set the stamp position.



9. Press [OK] twice.

10. Log out.

Enforced Storage of Documents to be Printed on a Printer

By making it compulsory to keep jobs in the machine before printing them, you can prevent information leakage due to users failing to collect prints or leaving prints unattended. The following print jobs are subject to compulsory storage.

- Normal Print
- Sample Print
- Store and Print

1. Log in as the machine administrator from the control panel.

2. Press [Printer Features].

3. Press [System].

4. Press [▼Next] twice.

5. Press [Restrict Direct Print Jobs].

6. Press [Automatclly. Store Jobs].

7. Press [OK].

8. Log out.

- If you select [Cncl All Direct Prt Jobs], the print jobs will be cancelled without being stored.
- For information on how to print stored documents, see "Printing Stored Documents", Print.

7. Managing the Machine

This chapter describes the functions for enhancing the security of the machine and operating the machine effectively.

Managing Log Files

Collecting the logs stored in this machine allows you to track detailed data on access to the machine, user identities, usage of the machine's various functions, and error histories.

The logs can be deleted periodically to make hard disk space available, and they can be encrypted to prevent leaking of information.

The logs can be viewed using Web Image Monitor or using the log collection server. Collected logs can be converted to CSV files and downloaded all at once. They cannot be read directly from the hard disk.

Log types

Three types of logs are stored on this machine: the job log, access log, and eco-friendly log.

- Job Log
Stores details of user file-related operations such as copying, printing, and saving in Document Server, and control panel operations such as sending and receiving faxes, sending scan files and printing reports (the configuration list, for example).
- Access Log
Stores details of login/logout activities, stored file operations such as creating, editing, and deleting, customer engineer operations such as hard disk formatting, system operations such as viewing log transfer results, and security operations such as specifying settings for encryption, unprivileged access detection, user lockout, and firmware authentication.
- Eco-friendly Log
Main power ON, OFF, transitions in power status, job run times or time interval between jobs, paper consumption per hour, power consumption.

Note

- For details about the log collection server, see the user's manual of the log collection server.
- When using the log collection server you must configure the log transfer settings on the log collection server.

Using Web Image Monitor to Manage Log Files

You can specify the types of log to store in the machine and the log collection level. You can also encrypt, bulk delete, or download log files.

Logs That Can Be Managed Using Web Image Monitor

The following tables explain the items in the job log and access log that the machine creates when you enable log collection using Web Image Monitor. If you require log collection, use Web Image Monitor to configure it. This setting can be specified in [Logs] under [Configuration] in Web Image Monitor.

Job log information items

Job Log Item	Log Type Attribute	Content
Copier: Copying	Copier: Copying	Details of normal and Sample Copy jobs.
Copier: Copying and Storing	Copier: Copying and Storing	Details of files stored in Document Server that were also copied at the time of storage.
Document Server: Storing	Document Server: Storing	Details of files stored using the Document Server screen.
Document Server: Stored File Downloading	Document Server: Stored File Downloading	Details of files stored in Document Server and downloaded using Web Image Monitor.
Stored File Printing	Stored File Printing	Details of files printed using the Document Server screen.
Scanner: Sending	Scanner: Sending	Details of sent scan files.
Scanner: URL Link Sending and Storing	Scanner: URL Link Sending and Storing	Details of scan files stored in Document Server and whose URLs were sent by e-mail at the time of storage.
Scanner: Sending and Storing	Scanner: Sending and Storing	Details of scan files stored in Document Server that were also sent at the time of storage.
Scanner: Storing	Scanner: Storing	Details of scan files stored in Document Server.

Job Log Item	Log Type Attribute	Content
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor or Desk Top Editor For Production.
Scanner: Stored File Sending	Scanner: Stored File Sending	Details of stored scan files that were also sent.
Scanner: Stored File URL Link Sending	Scanner: Stored File URL Link Sending	Details of stored scan files whose URLs were sent by e-mail.
Printer: Printing	Printer: Printing	Details of normal print jobs.
Printer: Locked Print (Incomplete)	Printer: Locked Print (Incomplete)	Log showing Locked Print documents temporarily stored on the machine.
Printer: Locked Print	Printer: Locked Print	Log showing Locked Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Sample Print (Incomplete)	Printer: Sample Print (Incomplete)	Log showing Sample Print documents temporarily stored on the machine.
Printer: Sample Print	Printer: Sample Print	Log showing Sample Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Hold Print (Incomplete)	Printer: Hold Print (Incomplete)	Log showing Hold Print documents temporarily stored on the machine.
Printer: Hold Print	Printer: Hold Print	Log showing Hold Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Stored Print	Printer: Stored Print	Details of Stored Print files stored on the machine.
Printer: Store and Normal Print	Printer: Store and Normal Print	Details of Stored Print files that were printed at the time of storage (when "Job Type:" was set to "Store and Print" in printer properties).
Printer: Stored File Printing	Printer: Stored File Printing	Details of Stored Print files printed from the control panel or Web Image Monitor.

Job Log Item	Log Type Attribute	Content
Printer: Document Server Sending	Printer: Document Server Sending	Details of files stored in Document Server when "Job Type:" was set to "Document Server" in printer properties.
Report Printing	Report Printing	Details of reports printed from the control panel.
Result Report Printing/ Emailing	Result Report Printing/ Emailing	Details of job results printed from the control panel or notified by e-mail.
Scanner: TWAIN Driver Scanning	Scanner: TWAIN Driver Scanning	Details of stored scan files that were sent using Network TWAIN Scanner.
Printer: Hold Print File Printing	Printer: Hold Print File Printing	When a document is held for printing and stored temporarily on the machine, this logs the time a user specifies it be printed via the control panel or Web Image Monitor.
Fax: Sending	Fax: Sending	Details of faxes sent from the machine.
Fax: LAN-Fax Sending	Fax: LAN-Fax Sending	Details of fax files sent from PCs.
Fax: Storing	Fax: Storing	Details of fax files stored on the machine using the facsimile function.
Fax: Stored File Printing	Fax: Stored File Printing	Details of fax files stored on the machine and printed using the facsimile function.
Fax: Stored File Downloading	Fax: Stored File Downloading	Details of fax files stored in Document Server and downloaded using Web Image Monitor.
Fax: Receiving	Fax: Receiving	Details of storage of received fax files.
Fax: Receiving and Delivering	Fax: Receiving and Delivering	Details of faxes that received and delivered by the machine.
Fax: Receiving and Storing	Fax: Receiving and Storing	Details of fax files that received and stored by the machine.

Access log information items

Access Log Item	Log Type Attribute	Content
Login	Login	Times of login and identity of logged in users.

Access Log Item	Log Type Attribute	Content
Logout	Logout	Times of logout and identity of logged out users.
File Storing	File Storing	Details of files stored in Document Server.
Stored File Deletion	Stored File Deletion	Details of files deleted from Document Server.
All Stored Files Deletion	All Stored Files Deletion	Details of deletions of all Document Server files.
HDD Format	HDD Format	Details of hard disk formatting.
Unauthorized Copying	Unauthorized Copying	Details of documents scanned with "Data Security for Copying".
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
Transfer Log Result	Transfer Log Result	Log of the result of log transfer to Remote Communication Gate S.
Log Collection Item Change	Log Collection Item Change	Details of changes to job log collection levels, access log collection levels, and types of log collected.
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Log of encrypted transmissions between the utility, Web Image Monitor or outside devices.
Access Violation	Access Violation	Details of failed access attempts.
Lockout	Lockout	Details of lockout activation.
Firmware: Update	Firmware: Update	Details of firmware updates.
Firmware: Structure Change	Firmware: Structure Change	Details of structure changes that occurred when an SD card was inserted or removed, or when an unsupported SD card was inserted.
Firmware: Structure	Firmware: Structure	Details of checks for changes to firmware module structure made at times such as when the machine was switched on.

Access Log Item	Log Type Attribute	Content
Machine Data Encryption Key Change	Machine Data Encryption Key Change	Details of changes made to encryption keys using "Machine Data Encryption Key Change" setting.
Firmware: Invalid	Firmware: Invalid	Details of checks for firmware validity made at times such as when the machine was switched on.
Date/Time Change	Date/Time Change	Details of changes made to date and time settings.
File Access Privilege Change	File Access Privilege Change	Log for changing the access privilege to the stored files.
Password Change	Password Change	Details of changes made to the login password.
Administrator Change	Administrator Change	Details of changes of administrator.
Address Book Change	Address Book Change	Details of changes made to address book entries.
Capture Error	Capture Error	Details of file capture errors.
Machine Configuration	Machine Configuration	Log of changes to the machine's settings.
Back Up Address Book	Back Up Address Book	Log of when data in the Address Book is backed up.
Restore Address Book	Restore Address Book	Log of when data in the Address Book is restored.
Enhanced Print Volume Use Limitation: Tracking Permission Result	Enhanced Print Volume Use Limitation: Tracking Permission Result	Log of when a tracking error occurs.
Counter Clear Result: Selected User(s)	Counter Clear Result: Selected User(s)	Log of when the counter for an individual user is cleared.
Counter Clear Result: All Users	Counter Clear Result: All Users	Log of when the counters for all users are cleared.

Access Log Item	Log Type Attribute	Content
Import Device Setting Information	Import Device Setting Information	Log of when a device setting information file is imported.
Export Device Setting Information	Export Device Setting Information	Log of when a device setting information file is exported.
Creating/Deleting Folders	Creating/Deleting Folders	Log reporting when folders are created and deleted.

There is no "Login" log made for SNMPv3.

If the hard disk is formatted, all the log entries up to the format are deleted and a log entry indicating the completion of the format is made.

"Access Violation" indicates the system has experienced frequent remote DoS attacks involving logon attempts through user authentication.

The first log made following power on is the "Firmware: Structure" log.

Eco-friendly log information items

Eco-friendly Log Item	Log Type Attribute	Content
Main Power On	Main Power On	Log of when the main power switch is turned on.
Main Power Off	Main Power Off	Log of when the main power switch is turned off.
Power Status Transition Result	Power Status Transition Result	Log of the results of transitions in power status.
Job Related Information	Job Related Information	Log of job-related information.
Paper Usage	Paper Usage	Log of the amount of paper used.
Power Consumption	Power Consumption	Log of power consumption.

Attributes of Logs You Can Download

If you use Web Image Monitor to download logs, a CSV file containing the information items shown in the following table is produced.

Note that a blank field indicates an item is not featured in a log.

File output format

- Character Code Set: UTF-8
- Output Format: CSV (Comma-Separated Values)
- File Names of Job Logs and Access Logs: "machine name + _log.csv"
- File names for Eco-friendly Logs: "machine name+_ecolog.csv"

Order of log entries

Log entries are printed in ascending order according to Log ID.

File structure

The data title is printed in the first line (header line) of the file.

Differences in log data formatting

- Job log

Multiple lines appear in the order of common items (job log and access log), Source (job input data), and Target (job output data). The same log ID is assigned to all lines corresponding to a single job log entry.

	Start Date/Time	...	Result	...	Access Result	Source	...	Print File Name	Target	...	Stored File Name
1	20XX-12-03T15:43:03.0	...	Completed	
2		...	Completed	...		Report	
3		...	Completed		Print	...	

CJD022

1. Common items

Each item in the common items is displayed on a separate line.

2. Source

"Result" and "Status" in the common items and the job log input entry appear.

If there are multiple sources, multiple lines appear.

3. Target

"Result" and "Status" in the common items and the job log output entry appear.

If there are multiple targets, multiple lines appear.

- Access log

The common items and access log entries appear on separate lines.

- Eco-friendly log

Eco-friendly log entries appear on separate lines.

Common items (Job log and Access log)

Start Date/Time

Indicates the start date and time of an operation or event.

End Date/Time

Indicates the end date and time of an operation or event.

Log Type

Details of the log type.

For details about the information items contained in each type of log, see page 204 "Logs That Can Be Managed Using Web Image Monitor".

Result

Indicates the result of an operation or event.

The following log items are recorded only when the logged operations are executed successfully:

"Document Server: Stored File Downloading", "Stored File Printing", "Scanner: Storing", "Scanner: Stored File Sending", "Printer: Stored File Printing", and "Fax: Stored File Downloading" (Job logs) and "File Storing" and "Stored File Deletion" (Access logs).

Value	Content
Succeeded	The operation or event completed successfully.
Failed	The operation or event was unsuccessful.
<Blank>	The operation or event is still in progress.

7

Operation Method

Indicates the operation procedure.

Value	Content
Control Panel	Control panel
Driver	Driver
Utility	Utility
Web	Web
Email	E-mail

Status

Indicates the status of an operation or event.

Value	Content
Completed	The operation or event completed successfully on a job log entry.
Failed	The operation or event was unsuccessful on a job log entry.
Succeeded	The operation or event completed successfully on an access log entry.
Password Mismatch	An access error has occurred because of a password mismatch.
User Not Programmed	An access error has occurred because the user is not registered.
Other Failures	An access error has occurred because of an unspecified failure.
User Locked Out	An access error has occurred because the user is locked out.
File Limit Exceeded	An access error has occurred because the file limit has been exceeded.
Transfer Cancelled	An access error has occurred because of a transfer cancellation.
Power Failure	An access error has occurred because of a power failure.
Lost File	An access error has occurred because the file has been lost.
Functional Problem	An access error has occurred because of a functional problem.
Communication Failure	An access error has occurred because of a communication failure.
Communication Result Unknown	An access error has occurred because of an unknown communication result.
Failure in some or all parts	Clearing user-specific counter or all-user counter failed.
Importing/Exporting by Other User	Importing or exporting is executing by another user.
Connection Failed with Remote Machine	A connection to an output destination failed.

Value	Content
Write Error to Remote Machine	An error occurred in writing to an output destination.
Specified File: Incompatible	The specified file is incompatible.
Specified File: Format Error	A format error occurred with the specified file.
Specified File: Not Exist	The specified file cannot be found.
Specified File: No Privileges	The privilege to access the specified file is missing.
Specified File: Access Error	An error occurs in accessing the specified file.
Memory Storage Device Full	The external media is full.
Memory Storage Device Error	An abnormality is found in the external media.
Encryption Failed	Encryption failed.
Decoding Failed	Decoding failed.
Common Key Not Exist	The common key is missing.
Connection Error	A communication error occurred.
Processing	The job is being processed.
Error	An error has occurred.
Suspended	The job has been suspended.

Cancelled: Details

Indicates the status in which the operation or event was unsuccessful.

Value	Content
Cancelled by User	A user canceled an operation.
Input Failure	An operation stopped abnormally during input.
Output Failure	An operation stopped abnormally during output.
Other Error	An error is detected prior to execution of a job or other errors have occurred.
Power Failure	Power is lost.

Value	Content
External Charge Unit Disconnected	The accounting device is unplugged during operation.
Insufficient No. of Original for Overlay	Pages are missing from a manuscript during execution of the overlaid copying.
Exceed Max. Stored Page (File Storage)	The storage capacity of pages on Document Server is exceeded.
Exceed Max. Stored File (File Storage)	The storage capacity of documents on Document Server is exceeded.
Hard Disk Full (File Storage Memory)	The hard disk capacity on Document Server is exceeded.
Exceeded Max. Email Size	The limit to e-mail size is exceeded.
Exceeded Max. File Size	The size limit for one document is exceeded.
Scanner Error	A read error occurred with the automatic document feed.
Timeout	A time-out occurred.
Exceed Max. Stored Page (Image Area)	The number of pages that can be captured is exceeded.
Hard Disk Full (Image Area)	The hard disk capacity for capture is exceeded.
Specified Folder to Store does not Exist	The specified folder to store the file cannot be found.
Password for Folder Specified to Store is Incorrect	The password for the specified folder to store the file is incorrect.
Folder is Locked	Folder is locked.
Memory Full	The memory range for processing data is full.
Print Data Error	An attempt to use a PDL or a port not installed on the machine has been made.

Value	Content
Data Transfer Interrupted	<p>Following cases are logged:</p> <ul style="list-style-type: none"> • The driver being used is not matching. • A network malfunction occurs. • A job is cancelled by the LAN-Fax driver. • A fax communication failure occurs.
Reception Error	Fax failed to be received.
Over Job Limit	The number of jobs that can be received is exceeded.
Specifying Destination Error	An illegal address or an address with 41 or more digits is specified.
Specifying Line Error	An error occurred in the line specified.
Authentication Failed (Access Restricted)	Device authentication failed.
Exceeded Print Volume Use Limitation	The logged in user exceeds their paper usage limit.
No Privilege	The user does not have permission to access a document or function.
Unavailable Size to Store	The size of paper specified (including custom-sizes) is of a size that cannot be stored.
Transmission Failed (Data Deleted)	A document is deleted or an undelivered document exceeds its wait time and is deleted.
Not Entered Document Password	The password for a document has not been entered.
Connection Failed with Destination	The specified server or folder is not found.
Authentication Failed with Destination	Authentication with the destination failed.
Transmission Failed with Memory Full	The destination memory is full.
Line Busy	The destination is busy.

Value	Content
No Response	There is not response from the destination.
Not Facsimile Destination	The destination is not a fax machine.
Invalid Device Certificate	Following case are logged: <ul style="list-style-type: none"> • The device certificate is missing. • The valid period has expired. • If the e-mail address of the administrator and that of the certificate do not match.
Invalid Expiration Date: Destination's Certificate	The valid period of the destination certificate is expired.
Invalid Device/Destination's Certificate	Both the destination certificate and the device certificate are invalid.
Fold Function Error	A folding function error has occurred.
Print Cancelled (Error)	The print job has been cancelled because of a system error.

7

User Entry ID

Indicates the user's entry ID.

This is a hexadecimal ID that identifies users who performed job or access log-related operations.

Value	Content
0x00000000	System operations, Operations that were performed by non-authenticated users
0x00000001 - 0xffffeff	For general users and user code
0xfffff80	System operations
0xfffff81	System operations, Operations that were performed by non-authenticated users
0xfffff86	Supervisor
0xfffff87	Administrator
0xfffff88	Administrator 1
0xfffff89	Administrator 2

Value	Content
0xfffff8a	Administrator 3
0xfffff8b	Administrator 4

User Code/User Name

Identifies the user code or user name of the user who performed the operation.

If an administrator performed the operation, this ID will contain the login name of that administrator.

Log ID

Identifies the ID that is assigned to the log.

This is a hexadecimal ID that identifies the log.

Access log information items

Access Log Type

Indicates the type of access.

Value	Content
Authentication	User authentication access
Stored File	Stored file access
System	System access
Network Attack Detection/ Encrypted Communication	Network attack or encrypted communication access
Firmware	Firmware verification access
Address Book	Address book access
Device Settings	Changes made to a setting in the User Tools menu.

Authentication Server Name

Indicates the name of the server where authentication was last attempted.

No. of Authentication Server Switches

Indicates the number of times server switching occurred when the authentication server was unavailable.

You can check whether or not the authentication server is available.

The number of server switches is indicated as 0 to 4.

"0" indicates the authentication server is available.

Logout Mode

Mode of logout.

Value	Content
by User's Operation	Manual logout by the user
by Auto Logout Timer	Automatic logout following a timeout

Login Method

Indicates the route by which the authentication request is received.

Value	Content
Control Panel	The login was performed through the control panel.
via Network	The login was performed remotely through a network computer.
Others	The login was performed through another method.

Login User Type

Indicates the type of login user.

Value	Content
User	General user
Guest	Guest user
User Administrator	User administrator
Machine Administrator	Machine administrator
Network Administrator	Network administrator
File Administrator	File administrator
Supervisor	Supervisor
Customer Engineer (Service Mode)	Customer engineer
Others	Login requests from users other than those specified above

Target User Entry ID

Indicates the entry ID of the target user.

This is a hexadecimal ID that indicates users to whom the following settings are applied:

- Lockout
- Password Change

Target User Code/User Name

User code or user name of the user whose data was accessed.

If the administrator's data was accessed, the administrator's user name is logged.

Address Book Registration No.

Indicates the registration number of the user performing the operation.

Address Book Operation Mode

Indicates the method applied for changing the data registered in the Address Book.

Address Book Change Item

Indicates which item in the Address Book is changed.

Address Book Change Request IP Address

Indicates the IP address type (IPv4/IPv6) of the user using the Address Book.

Lockout/Release

Indicates the lockout status.

Value	Content
Lockout	Activation of password lockout
Release	Deactivation of password lockout

Lockout/Release Method

Indicates the method applied for releasing the lockout.

Value	Content
Manual	The machine is unlocked manually.
Auto	The machine is unlocked by the lockout release timer.

Lockout Release Target Administrator

Indicates which administrator(s) is (are) released when releasing the lockout.

Counter to Clear

Indicates which counter is reset for each user.

Export Target

Indicates the settings to be included in the device setting file to be exported.

Value	Content
System Settings	System Settings
Copier Features	Copier Features
Facsimile Features	Facsimile Features
Printer Features	Printer Features
Scanner Features	Scanner Features
Program (Copier)	Program (Copier)
Program (Scanner)	Program (Scanner)
Program (Document Server)	Program (Document Server)
Browser Features	Browser Features
Web Image Monitor Setting	Web Image Monitor Setting
Web Service Settings	Web Service Settings
System/Copier SP	System/Copier SP
Scanner SP	Scanner SP
Printer SP	Printer SP
Facsimile SP	Facsimile SP

Target File Name

Indicates the name of the device information file to be imported/exported.

Stored File ID

Identifies a created or deleted file.

This is a hexadecimal ID that indicates created or deleted stored files.

Stored File Name

Indicates the name of a created or deleted file.

Delete File Type

Indicates the type of file deletion.

Value	Content
Delete Normal File	Normal file deletion
Auto Delete	Automatic file deletion
Others	File deletion for other reason

Folder Number

Indicates the folder number.

Folder Name

Indicates the folder name.

Creating/Deleting Folders

Indicates the operations performed on folders.

Value	Content
Delete Folder	Folder deleted
New Folder	Folder created

File Location

Region of all file deletion. "Document Server" indicates a deletion of all files from the machine's hard disk.

Collect Job Logs

Indicates the status of the job log collection setting.

Value	Content
Active	Job log collection setting is enabled.
Inactive	Job log collection setting is disabled.
Not Changed	No changes have been made to the job log collection setting.

Collect Access Logs

Indicates the status of the access log collection setting.

Value	Content
Active	Access log collection setting is enabled.
Inactive	Access log collection setting is disabled.

Value	Content
Not Changed	No changes have been made to the access log collection setting.

Collect Eco-friendly Logs

Indicates the status of the eco-friendly log collection setting.

Value	Content
Active	Eco-friendly log collection setting is enabled.
Inactive	Eco-friendly log collection setting is disabled.
Not Changed	No changes have been made to the eco-friendly log collection setting.

Transfer Logs

Indicates the status of the log transfer setting.

Value	Content
Active	Log transfer setting is enabled.
Inactive	Log transfer setting is disabled.
Not Changed	No changes have been made to the log transfer setting.

Encrypt Logs

Indicates the status of the log encryption setting.

Value	Content
Active	Log encryption setting is enabled.
Inactive	Log encryption setting is disabled.
Not Changed	No changes have been made to the log transfer setting.

Log Type

If a log's collection level setting has been changed, this function indicates details of the change.

Value	Content
Job Log	Job log
Access Log	Access log
Eco-friendly Log	Eco-friendly log

Log Collect Level

Indicates the level of log collection.

Value	Content
Level 1	Level 1
Level 2	Level 2
User Settings	User settings

Encryption/Cleartext

Indicates whether communication encryption is enabled or disabled.

Value	Content
Encryption Communication	Encryption is enabled.
Cleartext Communication	Encryption is disabled.

7

Machine Port No.

Indicates the machine's port number.

Protocol

Destination protocol.

"Unknown" indicates the destination's protocol could not be identified.

IP Address

Destination IP address.

Port No.

Destination port number.

This is in decimal.

MAC Address

Destination MAC (physical) address.

Primary Communication Protocol

Indicates the primary communication protocol.

Secondary Communication Protocol

Indicates the secondary communication protocol.

Encryption Protocol

Indicates the protocol used to encrypt the communication.

Communication Direction

Indicates the direction of communication.

Value	Content
Communication Start Request Receiver (In)	The machine received a request to start communication.
Communication Start Request Sender (Out)	The machine sent a request to start communication.

Communication Start Log ID

Indicates the log ID for the communication start time.

This is a hexadecimal ID that indicates the time at which the communication started.

Communication Start/End

Indicates the times at which the communication started and ended.

Network Attack Status

Indicates the machine's status when network attacks occur.

Value	Content
Violation Detected	An attack on the network was detected.
Recovered from Violation	The network recovered from an attack.
Max. Host Capacity Reached	The machine became inoperable due to the volume of incoming data reaching the maximum host capacity.
Recovered from Max. Host Capacity	The machine became operable again following reduction of the volume of incoming data.

Network Attack Type

Identifies network attack types.

Value	Content
Password Entry Violation	Password entry violation
Device Access Violation	Device access violation

Network Attack Type Details

Indicates details of network attack types.

Value	Content
Authentication Error	Authentication error
Encryption Error	Encryption error

Network Attack Route

Identifies the route of the network attack.

Value	Content
Attack from Control Panel	Attack by an unauthorized operation using the machine's control panel
Attack from Other than Control Panel	Attack by means other than an unauthorized operation using the machine's control panel

Login User Name used for Network Attack

Identifies the login user name that the network attack was performed by.

Add/Update/Delete Firmware

Indicates the method used to add, update, or delete the machine's firmware.

Value	Content
Updated with SD Card	An SD card was used to perform the firmware update.
Added with SD Card	An SD card was used to install the firmware.
Deleted with SD Card	An SD card was used to delete the firmware.
Moved to Another SD Card	The firmware was moved to another SD card.
Updated via Remote	The firmware was updated from a remote computer.

Value	Content
Updated for Other Reasons	The firmware update was performed using a method other than any of the above.

Module Name

Firmware module name.

Parts Number

Firmware module part number.

Version

Firmware version.

Machine Data Encryption Key Operation

Indicates the type of encryption key operation performed.

Value	Content
Back Up Machine Data Encryption Key	An encryption key backup was performed.
Restore Machine Data Encryption Key	An encryption key was restored.
Clear NVRAM	The NVRAM was cleared.
Start Updating Machine Data Encryption Key	An encryption key update was started.
Finish Updating Machine Data Encryption Key	An encryption key update was finished.

Machine Data Encryption Key Type

Identifies the type of the encryption key.

Value	Content
Encryption Key for Hard Disk	Encryption key for hard disk
Encryption Key for NVRAM	Encryption key for NVRAM
Device Certificate	Device certificate

Validity Error File Name

Indicates the name of the file in which a validity error was detected.

Configuration Category

Indicates the categories with changed settings.

Value	Content
User Lockout Policy	User lockout policy
Auto Logout Timer	Auto logout timer
Device Certificate	Device certificate
IPsec	IPsec
Compulsory Security Stamp	Compulsory security stamp
S/MIME	S/MIME
WIM Auto Logout Timer	Web Image Monitor auto logout timer

Configuration Name / Configuration Value

Indicates the attributes of the categories.

Indicates the values of the attributes.

Attribute	Description
Lockout	Whether the lockout is active (Active) or inactive (Inactive) is recorded.
Number of Attempts before Lockout	The number of times a user may enter a login password is recorded.
Lockout Release Timer	Whether the lockout release timer is active (Active) or inactive (Inactive) is recorded.
Lock Out User for	The time until lockout release is recorded.
Auto Logout Timer	Whether Auto Logout Timer is set to (On) or (Off) is recorded.
Auto Logout Timer (seconds)	The time until the auto logout operates is recorded.
Operation Mode	The type of operation is recorded.
Certificate No.	The number of the certificate to be used is recorded.

Attribute	Description
Certificate No.: IEEE 802.1X (WPA/WPA2)	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: S/MIME	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: IPsec	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: Digital Signature PDF	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
Certificate No.: Digital Signature PDF/A	The number of the certificate for applications is recorded. When a certificate is not used, "Do not Use" is recorded.
IPsec	Whether IPsec is active (Active) or inactive (Inactive) is recorded.
Encryption Key Auto Exchange: Setting 1-4: Remote Address	The remote address is recorded.
Encryption Key Auto Exchange: Setting 1-4, Default: Security Level	The security level is recorded. When [Authentication Only] is selected, "Authentication Only" is recorded. When [Authentication and Low Level Encryption] is selected, "Authentication and Low Level Encryption" is recorded. When [Authentication and High Level Encryption] is selected, "Authentication and High Level Encryption" is recorded. When [User Settings] is selected, "User Settings" is recorded.
Encryption Key Auto Exchange: Setting 1-4, Default: Authentication Method	The authentication method used for the auto key exchange format is recorded. Either "PSK" or "Certificate" is recorded.
Compulsory Security Stamp	Whether [Compulsory Security Stamp] is set to (On) or (Off) is recorded.
Operation Mode	The mode of operation is recorded.
Scanner: Email Sending	The signature is recorded when the scanner is used for sending e-mail.

Attribute	Description
Fax: Transferring	The signature is recorded when transferring by fax.
Fax: Email Sending	The signature is recorded when the fax is used for sending email.
Fax: Notification Email Sending	The signature is recorded when the fax is used for sending email notification.
Document Server (Utility): Stored File Transferring	The signature is recorded when Document Server (utility) is used for transferring documents stored on it.
WIM Auto Logout Timer (minutes)	Web Image Monitor's auto logout timer log is recorded in increments of one minute.

Destination Server Name

Indicates the name of the destination server to which the tracking information failed to be sent if the log type is "Enhanced Print Volume Use Limitation: Tracking Permission Result".

Indicates the name of the server from which the data export or import request is issued if the log type is import or export of preference information.

HDD Format Partition

Indicates the initial status of each hard disk partition.

Access Result

Indicates the results of logged operations.

Value	Content
Completed	An operation completed successfully.
Failed	An operation completed unsuccessfully.

Job log (source)

Source

Indicates the source of the job file.

Value	Content
Scan File	The job file was scanned.
Stored File	The job file was stored on the hard disk.

Value	Content
Printer	The job file was sent from the printer driver.
Received File	The job file was received over the network.
Report	The job file was a printed report.

Start Date/Time

Dates and times "Scan File", "Received File" and "Printer" operations started.

End Date/Time

Dates and times "Scan File", "Received File" and "Printer" operations ended.

Stored File ID

Indicates the ID of data that is output as a stored file.

This is a decimal ID that identifies the stored file.

Stored File Name

Names of "Stored File" files.

Folder Number

Indicates the number of the folder in which the file has been stored.

Folder Name

Indicates the name of the folder in which the file has been stored.

Print File Name

Name of "Printer" files.

Job log (target)

Printing stored faxes from the Fax screen before transmission will not be recorded in the job log.

Target

Type of the job target.

Value	Content
Print	Print
Store	Store
Send	Send

Start Date/Time

Dates and times "Print", "Store", and "Send" operations started.

End Date/Time

Dates and times "Print", "Store", and "Send" operations ended.

Destination Name

Names of "Send" destinations.

Destination Address

IP address, path, or e-mail address of "Send" destinations.

Stored File ID

Indicates the ID of data that is output as a store file.

This is a decimal ID that identifies the stored file.

Stored File ID logs are not logged for documents processed using fax functions.

Stored File Name

Indicates the name of the stored file when Target Type is "Store".

Stored File Name logs are not logged for documents processed using fax functions.

Folder Number

Indicates the number of the folder in which you have stored the file.

Folder Name

Indicates the name of the folder in which you have stored the file.

Eco-friendly log information items**Start Date/Time**

The event start date and time is recorded.

End Date/Time

The event end date and time is recorded.

Log Type

The type of eco-friendly log is recorded.

Value	Content
Main Power On	Main power on
Main Power Off	Main power off
Power Status Transition Result	Power status transition result

Value	Content
Job Related Information	Job related information
Paper Usage	Paper usage
Power Consumption	Power consumption

Log Result

Whether the event has ended or not is displayed.

Value	Content
Completed	Completed
Failed	Failed

Result

The result of the event is recorded.

Value	Content
Succeeded	Succeeded
Failed	Failed

Log ID

Identifies the ID that is assigned to the log. This is a hexadecimal ID that identifies the log.

Power Mode

The power status of the machine (after state transition) is logged.

Value	Content
Standby	Standby status
Low Power	Low power status
Silent	Silent status
HDD On	HDD on status
Engine Off	Engine off status
Controller Off	Controller off status

Value	Content
STR	STR status
Silent Print	Silent print status
Low Power Print	Low power print status
Fusing Unit Off	Fusing unit off status

Log Type

The type of job log is recorded.

Job Interval (seconds)

Indicates the elapsed time from the start of the previous job to the start of the present job.

Job Duration (seconds)

Indicates the elapsed time from the start of a job to its end.

Paper Usage (Large Size)

Indicates the number of one-sided prints per hour on large paper.

Large size means A3 (11 × 17 inches) or larger.

Paper Usage (Small Size)

Indicates the number of one-sided prints per hour on small paper.

Small size means smaller than A3 (11 × 17 inches).

Paper Usage (2 Sided: Large Size)

Indicates the number of two-sided prints per hour on large paper.

Large size means A3 (11 × 17 inches) or larger.

Paper Usage (2 Sided: Small Size)

Indicates the number of two-sided prints per hour on small paper.

Small size means smaller than A3 (11 × 17 inches).

Detected Power

The power consumption status of the machine is measured and registered in the log while the machine is being used.

Value	Content
Controller Standby	Controller standby mode
STR	Suspend to RAM (STR) mode
Main Power Off	The main power is turned off.

Value	Content
Scanning/Printing	Simultaneous scanning and printing
Printing	Machine's printing status
Scanning	Machine's printing status
Engine Standby	Engine's standby status
Engine Low	Engine's low-power status
Engine Night	Engine's silent status
Engine Total	Machine's total electricity consumption
Fusing Unit Off	Fusing unit off status

Power Consumption(Wh)

Indicates the power consumption in each power state.

7

Specifying Log Collect Settings

Enable the collection settings for each kind of log and configure the collection level.

Job Log Collect Level

If "Job Log Collect Level" is set to [Level 1], all job logs are collected.

Access Log Collect Level

If "Access Log Collect Level" is set to [Level 1], the following information items are recorded in the access log:

- HDD Format
- All Logs Deletion
- Log Setting Change
- Log Collection Item Change

If "Access Log Collect Level" is set to [Level 2], all access logs are collected.

Eco-friendly Log Collect Level

If "Eco-friendly Log Collect Level" is set to [Level 1], eco-friendly logs are not collected.

If "Eco-friendly Log Collect Level" is set to [Level 2], all eco-friendly logs are collected.

1. Log in as the machine administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].

3. Click [Logs] under "Device Settings".
4. Select [Active] for each function: "Collect Job Logs", "Collect Access Logs" and "Collect Eco-friendly Logs".
5. Specify the collection level for each function, "Job Log Collect Level", "Access Log Collect Level", and "Eco-friendly Log Collect Level".

When a level is changed, the selection status of log details changes according to the level.

To change individual items of the log details, configure the setting for each item. Even if the collection level is set to [Level 1] or [Level 2], once individual items of the log details are changed, the level changes to [User Settings].

6. Click [OK].
7. "Updating..." appears. Wait for about one or two minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

8. Log out.

Note

- The greater "Access Log Collect Level" setting value, the more logs are collected.

Specifying Log Encryption

Use the following procedure to enable/disable log encryption.

To encrypt the logs, it is necessary to set the collection setting to active for job log, access log, or eco-friendly log.

If the data stored in the machine has been encrypted, the log files will still be encrypted, regardless of this setting.

1. Log in as the machine administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Logs] under "Device Settings".
4. Select [Active] in the [Encrypt Logs] area under "Common Settings for All Logs".

To disable log encryption, select [Inactive].

5. Click [OK].

A confirmation message appears.

6. Click [OK].
7. Log out.

Downloading Logs

Use the following procedure to convert the logs stored in the machine into a CSV file for simultaneous batch download.

To collect logs, set the collection setting for the job log, access log and eco-friendly log to [Active].

This setting can be specified in [Logs] under [Configuration] in Web Image Monitor.

1. **Log in as the machine administrator from Web Image Monitor.**
2. **Point to [Device Management], and then click [Configuration].**
3. **Click [Download Logs] under "Device Settings".**
4. **Click [Logs to Download] and select the type of log to download.**
The security log includes two kinds of logs: job log and access log.
5. **Click [Download].**
6. **Specify the folder in which you want to save the file.**
7. **Click [Back].**
8. **Log out.**

Note

- Downloaded logs contain data recorded up till the time you click the [Download] button. Any logs recorded after the [Download] button is clicked will not be downloaded. The "Result" field of the log entry for uncompleted jobs will be blank.
- Download time may vary depending on the number of logs.
- If an error occurs while the CSV file is downloading or being created, the download is canceled and details of the error are included at the end of the file.
- If a log is downloaded successfully, "Download completed." will appear in the last line of the log file.
- For details about saving CSV log files, see your browser's Help.
- Downloaded log files use UTF-8 character encoding. To view a log file, open it using an application that supports UTF-8.
- For details about the items contained in the logs, see page 209 "Attributes of Logs You Can Download".

Number of Logs That Can Be Kept on the Machine

When the maximum number of job log, access log or eco-friendly log that can be kept on the machine is exceeded and new logs are generated, old logs are overwritten by new ones. If the logs are not downloaded periodically, it may not be possible to record the old logs onto files.

When using Web Image Monitor to manage logs, download the logs at an interval appropriate to the conditions in the table.

After downloading the logs, perform a batch deletion of the logs.

If you change the [Collect] / [Do not Collect] setting for log collection, you must perform a batch deletion of the logs.

Maximum number of logs that can be stored in the machine

Log types	Maximum number of logs
Job logs	4000
Access logs	12000
Eco-friendly logs	4000

If your machine does not have the HDD as standard and the optional HDD is not installed, the maximum number of eco-friendly logs that can be stored in the machine is 500.

Estimated number of logs created per day

Log types	Number of logs created per day
Job logs	100
Access logs	300 This number is based on 100 operations such as initialization and access operations over the Web, and 200 job entries (two entries per job: one login and one logout).
Eco-friendly logs	100

According to these conditions, the machine can maintain logs for 40 days without overwriting, but to be cautious, we recommend downloading after half that time, 20 days, to leave room for error.

Manage downloaded log files appropriately under the responsibility of the machine administrator.

Note

- During log downloads, do not perform operations that will create log entries, as logs that are in the process of downloading cannot be updated with new entries.
- Batch deletion of logs can be performed from the control panel or through Web Image Monitor.

Notes on Operation When the Number of Log Entries Reaches Maximum

If the number of logs that can be stored on the machine exceeds the specified maximum limit, old logs are overwritten by new logs. The maximum number of logs that can be stored is defined for each of the job log, access log and eco-friendly log.

The job log and access log are downloaded as one file.

"If logs are downloaded without overwriting" below indicates that the job log and access log are mixed after download.

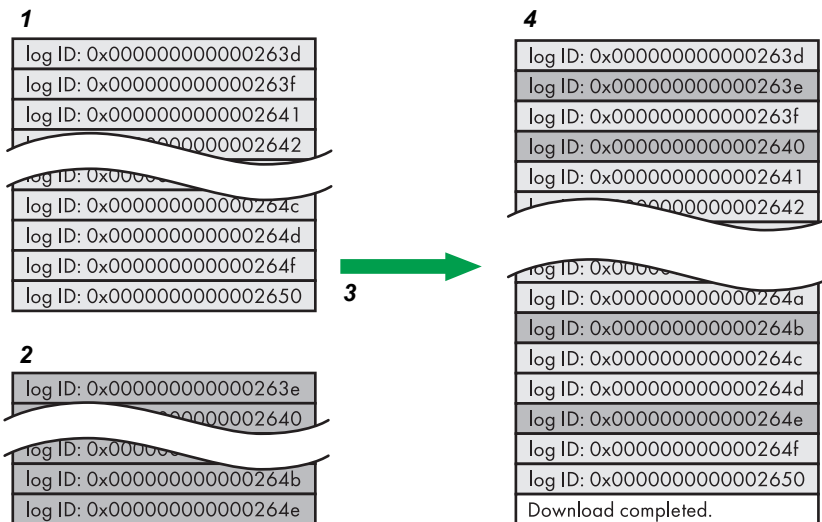
"If logs are downloaded during overwriting" below indicates that part of the access log is overwritten.

In this example, part of the access log is overwritten by a downloaded log and deleted.

The eco-friendly log is downloaded as an independent file.

Log entries are overwritten in the order of priority. Log entries with higher priority will not be overwritten or deleted.

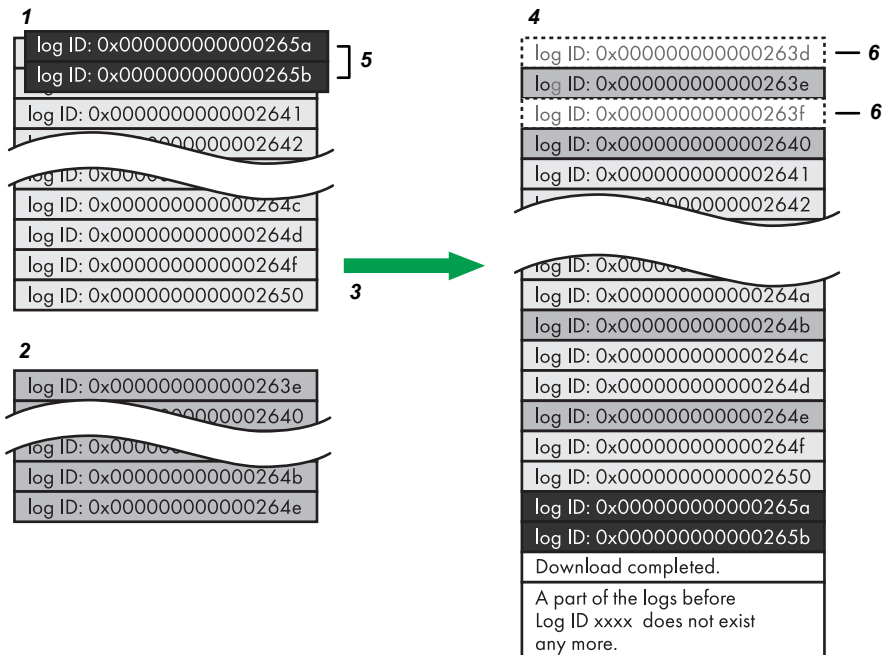
If logs are downloaded without overwriting



1. Access log
2. Job log
3. Download
4. Downloaded logs

CJD006

If logs are downloaded during overwriting



CJD007

7

1. Access log
2. Job log
3. Download
4. Downloaded logs
5. Overwriting
6. Deleted by overwriting

To determine whether or not overwriting occurred while the logs were downloading, check the message in the last line of the downloaded logs.

- If overwriting did not occur, the last line will contain the following message: Download completed.
- If overwriting did occur, the last line will contain the following message: Download completed. A part of the logs before Log ID xxxx does not exist any more.

↓ Note

- If overwriting has occurred, a part of the logs will have been erased by the overwriting, so check the log "Log ID xxxx" and more recent logs.

Printer Job Logs

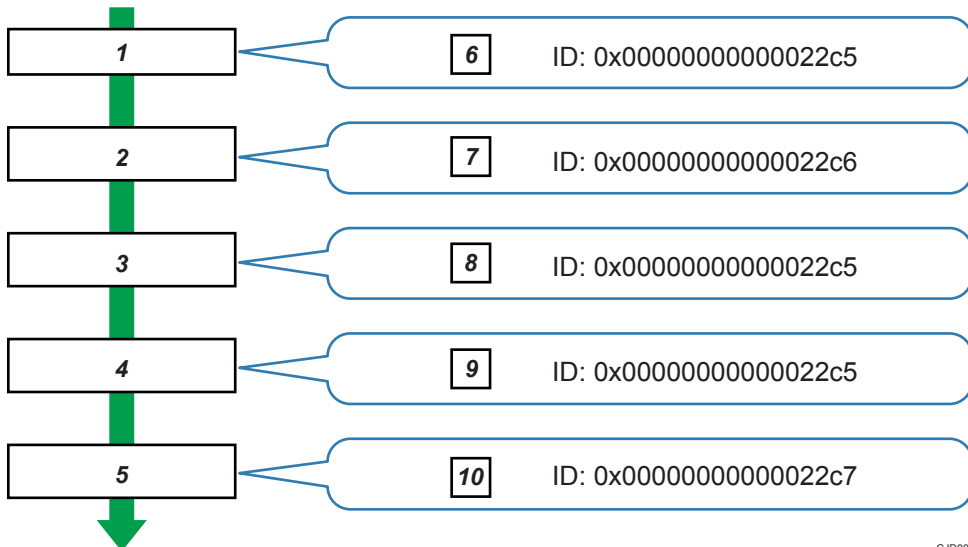
Print Log entries are made before the login entry is made in the Access Log.

Details of series of jobs (including reception, processing, and output of the jobs' data) are combined into single entries.

When the machine receives a print job, it creates an ID for the job and records this in the job log. The machine then creates a login ID for the print job and records this in the access log. It then creates a job log entry detailing the job's processing and outputting (under the same login ID). When the machine has finished processing the job, it creates a logout entry and places this in the access log.

Entries detailing the reception, processing, and output of a series of print jobs are created in the job log first, and then the login and logout details of those jobs are recorded in the access log.

Print job flowchart



CJD008

1. Print job data is received.
2. Authentication (login) data is received.
3. Print job is processed.
4. Print job is output.
5. Authentication (login) data is received.
6. An ID is assigned to the print job and recorded as an entry in the Job Log.
7. Authentication (login) data is recorded as an entry in the Access Log.
8. Information about the processing of the print job is recorded as an entry in the Job Log (using the same ID).

9. Information about the outputting of the print job is recorded as an entry in the Job Log (using the same ID).
10. Authentication (logout) data is recorded as an entry in the Access Log.

Deleting All Logs

Use the following procedure to delete all logs stored in the machine.

"Delete All Logs" appears if one of the job log, access log, or eco-friendly log is set to [Active].

1. Log in as the machine administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Logs] under "Device Settings".
4. Click [Delete] under "Delete All Logs".
5. Click [OK].
6. Log out.

Disabling Log Transfer to the Log Collection Server

Use the following procedure to disable log transfer to the log collection server. Note that you can switch the log transfer setting to [Inactive] only if it is already set to [Active].

1. Log in as the machine administrator from Web Image Monitor.
2. Point to [Device Management], and then click [Configuration].
3. Click [Logs] under "Device Settings".
4. Select [Inactive] in the [Transfer Logs] area under "Common Settings for All Logs".
5. Click [OK].
6. Log out.

Managing Logs from the Machine

You can specify settings such as whether or not to transfer logs to the log collection server and whether or not to delete all logs.

Disabling Log Transfer to the Log Collection Server

Use the following procedure to disable log transfer from the machine to the log collection server. Note that you can switch the log transfer setting to [Off] only if it is already set to [On].

For details about the log collection server, contact your sales representative.

For details about the transfer log setting, see the log collection server manual.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**
5. **Press [Transfer Log Setting].**
6. **Press [Off].**
7. **Press [OK].**
8. **Log out.**

7

Specifying Delete All Logs

Use the following procedure to delete all logs stored in the machine.

Deleting all logs from the machine as a batch can be achieved only if the log collection server is in use or if the Web Image Monitor setting has been specified to collect job log, access log or eco-friendly log.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next] three times.**
5. **Press [Delete All Logs].**
6. **Press [Yes].**
7. **Press [Exit].**
8. **Log out.**

Managing Logs from the Log Collection Server

For details about using the log collection server to manage Log Files, see the manual supplied with the log collection server.

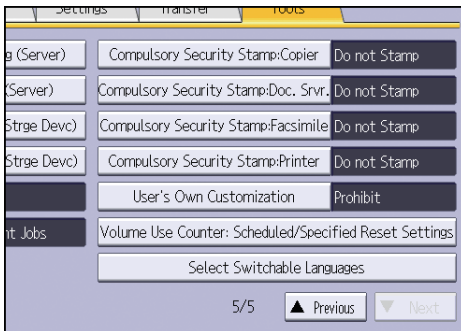
Configuring the Home Screen for Individual Users

This allows each user to use their own home screen.

When a user logs in, their personalized home screen is displayed.

This setting is applied to the standard operation panel.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] four times.
5. Press [User's Own Customization].



6. Press [Allow], and then press [OK].
7. Log out.

↓ Note

- This can also be configured from Web Image Monitor. For details, see Web Image Monitor Help.
- The home information for each user is maintained even when "User's Own Customization" is set to [Prohibit]. When the setting is changed back to [Allow], the information can be used again.

Warnings About Using User's Own Home Screens

Consider these warnings before using this function.

- When a user is registered in the Address Book, a home screen is created for that user. At that time, their user's own home screen is configured with the default settings (arrangement of icons).
- If Menu Protect is set to either [Level 1] or [Level 2], the user cannot use that function's program registration, editing or delete. However, there is no restriction on adding icons to the user's own home screen.

- When Menu Protect has been set to [Level 1] or [Level 2], have the administrator create any necessary programs.
- Only the icons of functions an administrator has permitted to be used are displayed.
- When a user is deleted from the Address Book, that user's home screen information is also deleted.
- When a user has edited a program, the changes are reflected to all the users who have the program's icon distributed to their own home screen.
- When a user deletes a program, the icon of the program is deleted from all the user's home screens to which it is distributed.
- Because each user manages and uses their own home screen, the administrator cannot check each user's own home information (customized state of users' own home screens).

Configuring the Browser Functions

Precautions for Using the Browser Function

The communication between the MFP and the server via a Web browser is exposed to the risk of unauthorized viewing and modification. Because of this, it is recommended to install the site certificates issued for the Web sites the MFP is allowed to browse and enable the machine's Site Certificate Check function in advance. By allowing the machine to access only the Web sites whose certificates are installed in the machine, you can prevent access to unauthorized Web sites.

It is recommended to enable [Site Certificate Check] especially when sending data using Extended JavaScript.

To enable [Site Certificate Check], it is necessary to enable the machine's SSL function and install site certificates.

For details about configuring SSL, see page 135 "Configuring SSL/TLS".

For details about installing site certificates, see page 166 "Configuring IEEE 802.1X Authentication".

The machine's Site Certificate Check settings can be specified only via Web Image Monitor.

See the related articles in the Web Image Monitor Help.

If [Site Certificate Check] is disabled and the user accesses an untrusted Web site, a warning message may appear.

If this is the case, the connected Web site may have a security problem. In such a case, the machine administrator must refer to page 246 "Troubleshooting", and then instruct the users to take appropriate measures accordingly.

Further, even if such a message does not appear, to minimize the risk of information leakages and unauthorized modification, the administrator should instruct the users to check the certificates and URLs of the connected Web sites so that access to unauthorized Web sites can be prevented.

Untrusted Web site

An "untrusted Web site" meets any of the following criteria:

- Its certificate has not been issued.
- Its certificate has been issued by an unknown source.
- Its certificate has expired.

Troubleshooting

If the connected Web site has a security problem, a message may appear.

If this is the case, the machine administrator must check the message and instruct the users to take appropriate measures accordingly.

Messages

- "This site has a security problem. The certificate has expired."
- "This site has a security problem. The root certificate for verification does not exist."
- "This site has a security problem. Verification of the server to connect to cannot be performed."
- "This site has a security problem. The http subcontents are included in the https site."*¹

* 1 The connected Web site contains non-encrypted data.

Managing Device Information

CAUTION

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

The machine's device information can be set by an administrator with privileges to manage everything — devices, users, networks and files.

The machine's device information can be exported to an external device as a device setting information file. By importing an exported device setting information file to the machine, you can use it as a backup file to restore device settings.

Data that can be imported and exported

- Copier / Document Server Features
- Printer Features
- Scanner Features
- Facsimile Features
- Browser Features
- Program (Document Server)
- Program (Copier)
- Program (Scanner)
- Web Image Monitor Setting
- Web Service Settings
- System Settings

Data that cannot be imported or exported

- Some System Settings *1 *2
- *1 The setting for the date, settings that require the device certificate, and settings that need to be adjusted for each machine (for example, image adjustment settings) cannot be imported or exported.
- *2 Settings only for executing functions and settings only for viewing cannot be imported or exported.
- Extended Feature Settings
 - Address book
 - Programs (fax function)
 - Programs (printer function)
 - User stamp in Copier / Document Server Features
 - Settings that can be specified via telnet
 - @Remote-related data

- Counters
- Settings that can only be specified via Web Image Monitor or Web Service (for example, Bonjour, SSDP setting)

↓ Note

- The file format for exports is CSV.
- The device configuration of the machine importing the device setting information file must be the same as that of the machine, which exported the device setting information file. Otherwise, the device setting information file cannot be imported.
- Import/export is possible between machines only if their models, region of use, and the following device configuration match.
 - Input Tray
 - Output Tray
 - Whether or not equipped with the duplex function
 - Whether or not equipped with a finisher and the type of finisher
 - Whether or not equipped with a hard disk
 - Whether or not equipped with the Remote Machine function
- If the device configuration is changed, export the updated device setting information file.
- If there are machines with the same device configuration, you can specify their settings identically by importing the same device setting file.
- If the home screen contains JPG image files, they will also be exported.
- While a user is operating the machine, nothing can be imported or exported until the user completes the operation.
- During export and import, the machine cannot be otherwise operated.
- For details about SD card handling, see "Inserting/Removing a Memory Storage Device", Getting Started.

Exporting Device Information

When exporting device information from the control panel, the data is saved on an SD card.

1. Insert an SD card into the media slot on the side of the control panel.

For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

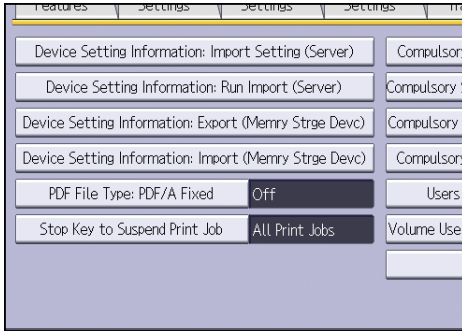
2. Log in from the control panel as an administrator with all privileges.

3. Press [System Settings].

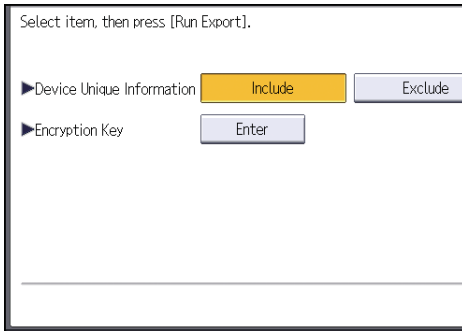
4. Press [Administrator Tools].

5. Press [▼Next] four times.

6. Press [Device Setting Information: Export (Memry Strge Devc)].



7. Set the export conditions.



- Specify whether to [Include] or [Exclude] the "Device Unique Information". "Device Unique Information" includes the IP address, host name, fax number, etc.
- Specify an encryption key.

8. Press [Run Export].

9. Press [OK].

10. Press [Exit].

11. Log out.

Note

- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

Importing Device Information

Import device information saved on an SD card.

1. Insert an SD card into the media slot on the side of the control panel.

For details about inserting the SD card, see "Inserting/Removing a Memory Storage Device", Getting Started.

2. Log in from the control panel as an administrator with all privileges.

3. Press [System Settings].

4. Press [Administrator Tools].

5. Press [▼Next] four times.

6. Press [Device Setting Information: Import (Memory Storage Device)].

7. Configure the import conditions.

Select item, then press [Run Import].

- ▶ Device Setting Info. File
- ▶ Image for Home Screen
- ▶ Device Unique Information
- ▶ Encryption Key

- Press [Select] of the "Device Setting Info. File" to select the file(s) to import.
- When adding an image to a home screen, press [Select] for "Image for Home Screen", and then select the file.
This setting is applied to the standard operation panel.
- Specify whether to [Include] or [Exclude] the "Device Unique Information". "Device Unique Information" includes the IP address, host name, fax number, etc.
- Enter the encryption key that was specified when the file was exported.

8. Press [Run Import].

9. Press [OK].

10. Press [Exit].

The machine restarts.

Note

- If import or export fails, you can check the log for the error. The log is stored in the same location as the exported device setting information file.

Troubleshooting

If an error occurs, check the log's result code first. Values other than 0 indicate that an error occurred. The result code will appear in the circled area illustrated below.

Example of a log file

```

"1.0.0"
"ExecType", "Date", "SerialNo", "PnP", "Model", "Destination", "IP", "Host", "Storage", "FileName", "FileID", "TotalItem", "NumOfOkItem", "ResultCode", "ResultName", "Identifier"
"IMPORT"
"20XX-07-05T15:29:16+09:00"
"3C35-7M0014"
"Brand Name"
"Product Name"
"0"
"10"
"10.250.155.125"
"RNP00267332582D"
"SD"
"20XX07051519563C35-710220.csv"
"20XX07051519563C35-710220"
" 0"
" 2"
"REQUEST"
"TargetID", "ModuleID", "PrefID", "Item", "NgCode", "NgName"
    
```

CJD023

If you cannot solve the problem or do not know how to solve it after checking the code, write down the error log entry, and then contact your service representative.

ResultCode	Cause	Solutions
2 (INVALID REQUEST)	A file import was attempted between different models or machines with different device configurations.	Import files exported from the same model with the same device configurations.
4 (INVALID OUTPUT DIR)	Failed to write the device information to the destination device.	Check whether the destination device is operating normally.
7 (MODULE ERROR)	An unexpected error has occurred during an import or export.	Turn the power off and then back on, and then try the operation again. If the error persists, contact your service representative.
8 (DISK FULL)	The available storage space on the external medium is insufficient.	Execute the operation again after making sure there is enough storage space.

ResultCode	Cause	Solutions
9 (DEVICE ERROR)	Failed to write or read the log file.	Check whether the path to the folder for storing the file or the folder in which the file is stored is missing.
10 (LOG ERROR)	Failed to write the log file. The hard disk is faulty.	Contact your service representative.
20 (PART FAILED)	Failed to import some settings.	<p>The reason for the failure is logged in "NgName". Check the code.</p> <p>Reason for the Error (NgName)</p> <p>2 INVALID VALUE The specified value exceeds the allowable range.</p> <p>3 PERMISSION ERROR The permission to edit the setting is missing.</p> <p>4 NOT EXIST The setting does not exist in the system.</p> <p>5 INTERLOCK ERROR The setting cannot be changed because of the system status or interlocking with other specified settings.</p> <p>6 OTHER ERROR The setting cannot be changed for some other reason.</p>
21 (INVALID FILE)	Failed to import the file because it is in the wrong format in the external medium.	Check whether the file format is correct. The log is in the form of a CSV file.
22 (INVALID KEY)	The encryption key is not valid.	Use the correct encryption key.

Managing Eco-friendly Counter

When user authentication is being used, information on the eco-friendly counter is displayed at login.

The eco-friendly counter displays the ratio of use of color, duplex and combine printing to the total number of printed sheets.

How much toner and paper are being saved is indicated by the eco-friendly index. Higher eco-friendly index leads to greater resource saving.

Note

- When Basic, Windows, LDAP or Integration Server authentication is used for user authentication, the machine compiles the data and displays the eco-friendly counter for each user.
- When user code authentication is used for user authentication, or when user authentication is not in use, the machine compiles the data and displays it's overall eco-friendly counter.

Configuring the Display of Eco-friendly Counters

Set up the period for collecting data for the eco-friendly counter and an administrator's message.

1. **Log in as the machine administrator from the control panel.**
2. **Press [System Settings].**
3. **Press [Administrator Tools].**
4. **Press [▼Next].**
5. **Press [Eco-friendly Counter Period / Administrator Message].**
6. **Change the settings.**
7. **Press [OK].**
8. **Press [Exit].**
9. **Log out.**

Count Period

Set up the period for collecting data for the eco-friendly counter.

When [Specify Days] is selected, data for the eco-friendly counter is compiled for each number of days specified.

Default: [Do not Count]

Administrator Message

Select the message to be displayed when a user logs in.

If you select "Fixed Message 1" or "Fixed Message 2", a preset message is displayed.

If you select "User Message", the machine administrator can enter a message to be displayed.

Default: [Fixed Message 1]

Display Information Screen

Specify whether or not to display the information screen at user login.

Default: [Off]

Display Time

Specify the timing for displaying the information screen.

Default: [Every Time Login]

Clearing a Machine's Eco-friendly Counter

A machine's eco-friendly counter can be cleared.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Display / Clear Eco-friendly Counter].
5. Press [Clear Current Value] or [Clear Crnt. & Prev. Val.].
6. Press [OK].
7. Log out.

7

Clearing Users' Eco-friendly Counters

By clearing the users' eco-friendly counter, all users' eco-friendly counters are cleared.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Display / Clear Eco-friendly Counter per User].
5. Press [Clear Current Value] or [Clear Crnt. & Prev. Val.].
6. Press [OK].
7. Log out.

Managing the Address Book

Specifying Auto Deletion of Address Book Data

Specify how the machine handles a request for auto registration after the registered data in the address book has reached the limit.

If you set this to [On], new user accounts are added by automatically deleting old user accounts. Accounts that have not been used for the longest time are deleted first.

If you set this to [Off], old user accounts are not deleted, so new user accounts cannot be added once the limit has been reached.

1. Log in as the user administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Auto Delete User in Address Book].
5. Select [On], and then press [OK].
6. Log out.

Note

- The data is automatically deleted only when the machine receives a request for data registration. Auto deletion is not executed if user accounts are manually added.
- Only user accounts with user codes or login user names and passwords will be automatically deleted.

Deleting All Data in the Address Book

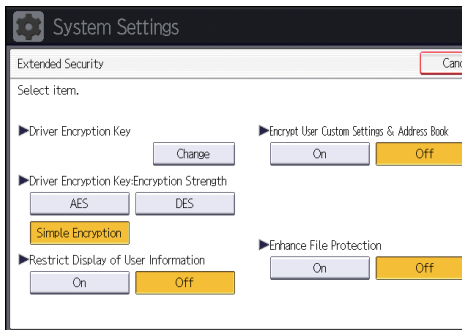
You can delete all the data registered in the Address Book.

1. Log in as the user administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [Delete All Data in Address Book].
5. Press [Yes], and then press [Exit].
6. Log out.

Specifying the Extended Security Functions

In addition to providing basic security through user authentication and each administrator's specified limits to access the machine, security can also be increased by encrypting transmitted data and data in the Address Book.

1. Log in from the control panel as an administrator with privileges.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next].
5. Press [Extended Security].
6. Press the setting you want to change, and change the settings.



7. Press [OK].
8. Log out.

Note

- The operation privileges of an administrator differs depending on the setting.

Driver Encryption Key

This can be specified by the network administrator.

Specify the string of text for decrypting the login passwords or file passwords sent from the driver when user authentication is ON.

To specify the driver encryption key, register the encryption key specified using the machine in the driver.

For details, see page 172 "Specifying a Driver Encryption Key".

Driver Encryption Key:Encryption Strength

This can be specified by the network administrator.

Specify the encryption strength for sending jobs from the driver to the machine.

The machine confirms the encryption strength of the password appended to a job and processes it.

If [Simple Encryption] is specified, all jobs that pass user authentication are accepted.

If [DES] is specified, jobs encrypted with DES or AES are accepted.

If [AES] is specified, jobs encrypted with AES are accepted.

If you select [AES] or [DES], specify the encryption settings using the printer driver. For details about specifying the printer driver, see the printer driver Help.

Default: [Simple Encryption]

Restrict Display of User Information

This can be specified by the machine administrator.

This can be specified if user authentication is specified. When the job history is checked using a network connection for which authentication is not available, all personal information can be displayed as "*****". For example, when someone not authenticated as an administrator checks the job history using SNMP in SmartDeviceMonitor for Admin/Device Manager NX Lite, personal information can be displayed as "*****" so that users cannot be identified. Because information identifying registered users cannot be viewed, unauthorized users are prevented from obtaining information about the registered files.

Default: [Off]

Encrypt User Custom Settings & Address Book

This can be specified by the user administrator.

Encrypt the individual settings of the machine's users and the data in the Address Book.

Even if information on an internal part has been leaked, encryption prevents the individual user settings or the Address Book data from being read.

For details, see page 95 "Protecting the Address Book".

Default: [Off]

Enhance File Protection

This can be specified by the file administrator.

By specifying a password, you can limit operations such as printing, deleting, and sending files, and can prevent unauthorized people from accessing the files. However, it is still possible for the password to be cracked.

By specifying "Enhance File Protection", files are locked and so become inaccessible if an invalid password is entered ten times. This can protect the files from unauthorized access attempts in which a password is repeatedly guessed.

When "Enhance File Protection" is specified,  appears in the lower right corner of the screen.

The locked files can only be unlocked by the file administrator.

When files are locked, you cannot select them even if the correct password is entered.

Default: [Off]

Restrict Use of Destinations (Fax), Restrict Use of Destinations (Scanner)

This can be specified by the user administrator.

The available fax and scanner destinations are limited to the destinations registered in the Address Book.

A user cannot directly enter the destinations for transmission.

If "Restrict Use of Destinations (Scanner)" is set to [On], you can register fax numbers only.

If you specify the setting to receive e-mails via SMTP, you cannot use "Restrict Use of Destinations (Fax)" and "Restrict Use of Destinations (Scanner)".

The destinations searched by "LDAP Search" can be used.

For details, see page 75 "Restricting Usage of the Destination List".

Default: [Off]

Restrict Adding of User Destinations (Fax), Restrict Adding of User Destinations (Scanner)

This can be specified by the user administrator.

If you set "Restrict Adding of User Destinations (Fax)" and/or "Restrict Adding of User Destinations (Scanner)" to [Off], users will be able to register a fax or scanner destination in the Address Book simply by entering the destination and then pressing [Prg. Dest.]. If you set these functions to [On], the [Prg. Dest.] key will not appear. Users will still be able to enter a destination directly using the fax or scanner screen, but cannot then register that destination in the Address Book by pressing [Prg. Dest.].

Also, note that even if you set these functions to [On], users registered in the address book can change their passwords. Only the user administrator can change items other than the password.

Default: [Off]

Transfer to Fax Receiver

This can be specified by the machine administrator.

If you use [Forwarding] or [Transfer Box] under the fax function, files stored in the machine can be transferred or delivered.

To prevent stored files being transferred by mistake, select [Prohibit] for this setting.

Default: [Do not Prohibit]

If you select [Prohibit] for this setting, the following functions are disabled:

- Forwarding
- Transfer Box
- Delivery from Personal Box
- Information Box
- Delivery of Mail Received via SMTP
- Routing Received Documents

For details, see "Reception Functions", Fax.

Authenticate Current Job

This can be specified by the machine administrator.

This setting lets you specify whether or not authentication is required for operations such as canceling jobs under the copier and printer functions.

If you select [Login Privilege], authorized users and the machine administrator can operate the machine. When this is selected, authentication is not required for users who logged in to the machine before [Login Privilege] was selected.

If [Access Privilege] is specified, any user who performed a copy or print job can cancel the job. Also, the machine administrator can cancel the user's copy or print job.

Even if you select [Login Privilege] and log on to the machine, you cannot cancel a copy or print job that is being processed if you are not privileged to use the copy and printer functions.

You can specify "Authenticate Current Job" only if "User Authentication Management" was specified.

Default: [Off]

@Remote Service

This can be specified by the machine administrator.

Communication via HTTPS for @Remote Service is disabled if you select [Prohibit].

When setting it to [Prohibit], consult with your service representative.

If it is set to [Proh. Some Services], it becomes impossible to change settings via a remote connection, providing optimally secure operation.

Default: [Do not Prohibit]

Update Firmware

This can be specified by the machine administrator.

Specify whether to allow firmware updates on the machine. Firmware update means having a service representative update the firmware or updating the firmware via the network.

If you select [Prohibit], firmware on the machine cannot be updated.

If you select [Do not Prohibit], there are no restrictions on firmware updates.

Default: [Do not Prohibit]

Change Firmware Structure

This can be specified by the machine administrator.

Specify whether to prevent changes in the machine's firmware structure. The Change Firmware Structure function detects when the SD card is inserted, removed or replaced.

If you select [Prohibit], the machine stops during startup when a firmware structure change is detected and a message requesting administrator login is displayed. After the machine administrator logs in, the machine finishes startup with the updated firmware.

The administrator can confirm if the updated structure change is permissible or not by checking the firmware version displayed on the control panel screen. If the firmware structure change is not permissible, contact your service representative before logging in.

When "Change Firmware Structure" is set to [Prohibit], administrator authentication must be enabled.

After [Prohibit] is specified, disable administrator authentication. When administrator authentication is enabled again, you can return the setting to [Do not Prohibit].

If you select [Do not Prohibit], firmware structure change detection is disabled.

Default: [Do not Prohibit]

Password Policy

This can be specified by the user administrator.

This setting lets you specify [Complexity Setting] and [Minimum Character No.] for the password. By making this setting, you can limit the available passwords to only those that meet the conditions specified in "Complexity Setting" and "Minimum Character No.".

If you select [Level 1], specify the password using a combination of two types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

If you select [Level 2], specify the password using a combination of three types of characters selected from upper-case letters, lower-case letters, decimal numbers, and symbols such as #.

Default: [Off], Minimum required number of characters not specified

Settings by SNMPv1, v2

This can be specified by the network administrator.

When the machine is accessed using the SNMPv1, v2 protocol, authentication cannot be performed, allowing machine administrator settings such as the paper setting to be changed. If you select [Prohibit], the setting can be viewed but not specified with SNMPv1, v2.

Default: [Do not Prohibit]

Security Setting for Access Violation

This can be specified by the machine administrator.

When logging in to the machine via a network application, a user may be locked out erroneously because the number of authentication attempts of the user does not match the number of attempts logged internally.

For example, access may be denied when a print job for multiple sets of pages is sent from an application.

If you select [On] under "Security Setting for Access Violation", you can prevent such authentication errors.

- On
 - Denial Durtn. for Accs. Viol.

Specify the time to limit repeated access by a user.

Use the number keys to enter the time between "0" and "60", and then press [#].

Default: [15]

- Managed User Host Limit

Specify the number of user accounts to manage under "Security Setting for Access Violation".

Use the number keys to enter the number between "50" and "200", and then press [#].

Default: [200]

- Password Entry Host Limit

Specify the number of passwords to manage under "Security Setting for Access Violation".

Use the number keys to enter the number between "50" and "200", and then press [#].

Default: [200]

- Status Monitor Interval

Specify the monitoring interval of "Managed User Host Limit" and "Password Entry Host Limit".

Use the number keys to enter the time between "1" and "10", and then press [#].

Default: [3]

- Off

Default: [Off]

Password Entry Violation

This can be specified by the machine administrator.

If the number of authentication requests exceeds the setting, the system classifies the access session as a password attack. The access session is recorded in the Access Log and the log data is sent to the machine administrator by e-mail.

If the "Max. Allowed No. of Access" is set to [0], password attacks are not detected.

- Max. Allowed No. of Access

Specify the maximum number of allowable authentication attempts.

Use the number keys to enter the number between "0" and "100", and then press [#].

Default: [30]

- Measurement Time

Specify the interval to count the number of repeated failed authentication attempts. When the measurement time is over, the logged counts of failed authentication attempts are cleared.

Use the number keys to enter the time between "1" and "10", and then press [#].

Default: [5]

↓ Note

- Depending on the values of the settings for [Max. Allowed No. of Access] and [Measurement Time], you may frequently receive violation detection e-mail.
- If violation detection e-mail is received frequently, check the content and review the setting values.

Device Access Violation

This can be specified by the machine administrator.

If the number of log in requests exceeds the setting, the system classifies the access session as an access violation. The access session is recorded in the Access Log and the log data is sent to the machine administrator by e-mail. Also, a message is displayed on the control panel and on Web Image Monitor.

If the "Max. Allowed No. of Access" is set to [0], over access is not detected.

In "Authentication Delay Time", you can specify response delay time for log-in requests to prevent the system from becoming unavailable when an access violation is detected.

In "Simultns. Access Host Limit", you can specify the limit number of hosts accessing the machine at one time. If the number of access exceeds the setting, monitoring becomes unavailable and the detected unavailability is recorded in the Log.

- Max. Allowed No. of Access

Specify the maximum number of allowable access attempts.

Use the number keys to enter the number between "0" and "500", and then press [#].

Default: [100]

- Measurement Time

Specify the interval to count the number of excessive access. When the measurement time is over, the logged counts of access are cleared.

Use the number keys to enter the number between "10" and "30", and then press [#].

Default: [10]

- Authentication Delay Time

Specify the authentication delay time when an access violation is detected.

Use the number keys to enter the number between "0" and "9", and then press [#].

Default: [3]

- Simultns. Access Host Limit

Specify the number of acceptable authentication attempts when authentications are delayed due to an access violation.

Use the number keys to enter the number between "50" and "200", and then press [#].

Default: [200]

 **Note**

- Depending on the values of the settings for [Max. Allowed No. of Access] and [Measurement Time], you may frequently receive violation detection e-mail.
- If violation detection e-mail is received frequently, check the content and review the setting values.

Other Security Functions

This is an explanation of the settings for preventing leakage of information.

It also explains the functions that are restricted when user authentication is used.

Fax Function

Not displaying destinations and senders in reports and lists

This can be specified by the machine administrator.

In [Facsimile Features], you can specify whether to display destinations and sender names by setting "Switch 04, Bit No. 4" and "Switch 04, Bit No. 5" in [Parameter Setting], under [Initial Settings]. Making this setting helps prevent information leaks, because unintended users cannot read destinations and sender names on both the sending and receiving side.

For details, see "Facsimile Features", Fax.

Stored Reception File User Setting

This can be specified by the file administrator.

In [Facsimile Features], you can specify which users can manage fax files stored on the hard disk by setting [Stored Reception File User Setting] to [On], under [Reception Settings]. To access the machine over the network, specified users must enter their user codes or login user names and passwords. Only authorized users can manage fax files stored on the hard disk.

For details, see "Facsimile Features", Fax.

Printing the Journal

When user authentication is specified, the Journal is automatically set not to be printed in order to prevent automatic printing of personal information in transmission history. Also, if more than 200 transmissions are made, transmissions shown in the Journal are overwritten each time a further transmission is made.

To prevent the transmission history from being overwritten, perform the following procedures:

- In the Initial Settings menu under Facsimile Features, specify "Switch 03, Bit 7" in [Parameter Setting] to automatically print the Journal.
- In the Initial Settings menu under Facsimile Features, specify "Switch 21, Bit 4" in [Parameter Setting] to send the Journal by e-mail.

For details, see "Facsimile Features", Fax.

Scanner Function

Print & Delete Scanner Journal

When user authentication is enabled, "Print & Delete Scanner Journal" is automatically set to [Do not Print: Disable Send] in order to prevent personal information in transmission/delivery history from being automatically printed. In this case, the scanner is automatically disabled when the journal history exceeds 250 transmissions/deliveries. When this happens, select [Print Scanner Journal] or [Delete Scanner Journal]. To print the scanner journal automatically, set [Print and Delete All] for "Print & Delete Scanner Journal".

For details, see "Scanner Features", Scan.

WSD scanner function

WSD scanner function is automatically disabled when user authentication is specified. Even if automatically disabled, it can be enabled from "Initial Settings" available in Web Image Monitor.

For details, see "Preparing to Use WSD Scanner (Push Type)" and "Preparing to Use WSD Scanner (Pull Type)", Scan.

System Status

7

Pressing the [Check Status] key on the control panel allows you to check the machine's current status and settings. If administrator authentication has been specified, [Machine Address Info] is displayed in [Maintnc./Inquiry/Mach. Info] only if you have logged in to the machine as an administrator.

Confirming Firmware Validity

When the machine starts up, this function verifies the validity of its firmware.

If an error occurs during the verification, a verification error is displayed on the control panel.

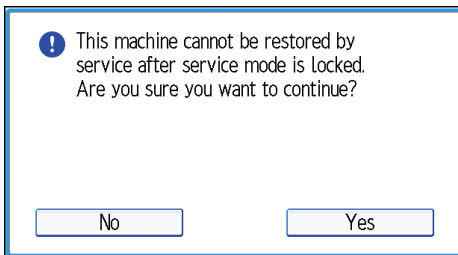
Note that this can also be checked on Web Image Monitor after startup of the machine. If an error occurs in the verification of Web Image Monitor itself, Web Image Monitor cannot be used, so check the display on the control panel.

Restricting a Customer Engineer Operation

You can restrict the customer engineer's access to the service mode.

Service mode is used by a customer engineer for inspection or repair. If you set "Service Mode Lock" to [On], service mode cannot be used unless the machine administrator logs on to the machine and cancels the service mode lock to allow a customer engineer to operate the machine for inspection and repair. This ensures that the inspection and repair are done under the supervision of the machine administrator.

1. Log in as the machine administrator from the control panel.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] twice.
5. Press [Service Mode Lock].
6. Press [On], and then press [OK].
7. Press [Yes].



8. Log out.

Additional Information for Enhanced Security

This section explains the settings that you can configure to enhance the machine's security.

Settings You Can Configure Using the Control Panel

Use the control panel to configure the security settings shown in the following table.

System Settings

Tab	Item	Setting
Timer Settings	Auto Logout Timer	On: 180 seconds or less. See page 71 "Auto Logout".
Administrator Tools	User Authentication Management	Select [Basic Auth.], and then set "Printer Job Authentication" to [Entire]. See page 37 "Basic Authentication".
Administrator Tools	Administrator Authentication Management → User Management	Select [On], and then select [Administrator Tools] for "Available Settings". See page 16 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management → Machine Management	Select [On], and then select each of "Available Settings". See page 16 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management → Network Management	Select [On], and then select [Interface Settings], [File Transfer], and [Administrator Tools] for "Available Settings". See page 16 "Configuring Administrator Authentication".
Administrator Tools	Administrator Authentication Management → File Management	Select [On], and then select [Administrator Tools] for "Available Settings". See page 16 "Configuring Administrator Authentication".

Tab	Item	Setting
Administrator Tools	Extended Security → Settings by SNMPv1, v2	Prohibit See page 257 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security → Driver Encryption Key:Encryption Strength	AES See page 257 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security → Authenticate Current Job	Access Privilege See page 257 "Specifying the Extended Security Functions".
Administrator Tools	Extended Security → Password Policy	"Complexity Setting": Level 1 or higher, "Minimum Character No.": 8 or higher See page 257 "Specifying the Extended Security Functions".
Administrator Tools	Network Security Level	Level 2 To acquire the machine status through printer driver or Web Image Monitor, set "SNMP" to Active on Web Image Monitor. See page 125 "Specifying Network Security Level".
Administrator Tools	Service Mode Lock	On See page 267 "Restricting a Customer Engineer Operation".
Administrator Tools	Machine Data Encryption Settings	Select [Encrypt], and then select [All Data] for "Carry over all data or file system data only (without formatting), or format all data." If [Encrypt] is already selected, further encryption settings are not necessary. See page 99 "Encrypting Data on the Hard Disk".

Scanner Features

Tab	Item	Setting
Initial Settings	Menu Protect	Level 2 See page 78 "Specifying Menu Protect".

Facsimile Features

Tab	Item	Setting
Reception Settings	Stored Reception File User Setting	Select [On], and then specify the users or groups who can perform operations on the received documents. See page 265 "Other Security Functions".
Initial Settings	Menu Protect	Level 2 See page 78 "Specifying Menu Protect".

Note

- The SNMP setting can be specified in [SNMP] under [Configuration] in Web Image Monitor.

Settings You Can Configure Using Web Image Monitor

Use Web Image Monitor to configure the security settings shown in the following table.

Category	Item	Setting
Device Settings → Logs	Collect Job Logs	Active
Device Settings → Logs	Collect Access Logs	Active
Security → User Lockout Policy	Lockout	Active For details, see page 69 "User Lockout Function".
Security → User Lockout Policy	Number of Attempts before Lockout	5 times or less. For details, see page 69 "User Lockout Function".

Category	Item	Setting
Security → User Lockout Policy	Lockout Release Timer	Set to [Active] or [Inactive]. When setting to [Active], set the Lockout release timer to 60 minutes or more. For details, see page 69 "User Lockout Function".
Security → User Lockout Policy	Lock Out User for	When setting "Lockout Release Timer" to [Active], set the Lockout release timer to 60 minutes or more. For details, see page 69 "User Lockout Function".
Network → SNMPv3	SNMPv3 Function	Inactive To use SNMPv3 functions, set "SNMPv3 Function" to [Active], and set "Permit SNMPv3 Communication" to [Encryption Only]. Because SNMPv3 enforces authentication for each packet, Login log will be disabled as long as SNMPv3 is active.
Security → Network Security	FTP	Inactive Before specifying this setting, set "Network Security Level" to [Level 2] on the control panel.
Security	S/MIME	"Encryption Algorithm": AES-128 bit, AES-256 bit, or 3DES-168 bit You must register the user certificate in order to use S/MIME.
Address Book → Detail Input → Add User/Change → Email	User Certificate	You must register the user certificate in order to use S/MIME.

Note

- The administrator must indicate which strength level is to be specified for the encryption algorithm.
- For details about specifying an encryption algorithm and registering a user certificate, see page 141 "Configuring S/MIME".

Settings You Can Configure When IPsec Is Available/Unavailable

All communication to and from machines on which IPsec is enabled is encrypted.

If your network supports IPsec, we recommend you enable it.

Settings you can configure when IPsec is available

If IPsec is available, configure the settings shown in the following table to enhance the security of the data traveling on your network.

Control panel settings

System Settings

Tab	Item	Setting
Interface Settings	IPsec	Active
Interface Settings	Permit SSL / TLS Communication	Ciphertext Only

Web Image Monitor settings

Category	Item	Setting
Security → IPsec → Encryption Key Auto Exchange Settings	Edit → Security Level	Authentication and High Level Encryption

Settings you can configure when IPsec is unavailable

If IPsec is not available, configure the settings shown in the following table to enhance the security of the data traveling on your network.

Control panel settings

System Settings

Tab	Item	Setting
Interface Settings	IPsec	Inactive
Interface Settings	Permit SSL / TLS Communication	Ciphertext Only

Note

- You can set "IPsec" and "Permit SSL/TLS Communication" using Web Image Monitor.

Securing data when IPsec is unavailable

The following procedures make user data more secure when IPsec is unavailable.

Administrators must inform users to carry out these procedures.

Fax

- Sending and receiving faxes without using IP-Fax
When sending faxes, specify destinations by fax number, Internet Fax destination, e-mail address, or folder destination. Do not specify destinations by IP-Fax destination. For details about specifying the destination for a facsimile, see "Specifying a Destination", Fax.

Printer

- Printing with protocols that support encryption
To use the printer functions, specify sftp as the protocol, or specify IPP and enable SSL/TLS. For details about sftp, see "Printing Files Directly from Windows", Connecting the Machine/System Settings.
For details about IPP settings, see "Installing the Printer Driver for the Selected Port", Driver Installation Guide.
For details about SSL/TLS settings, see page 135 "Configuring SSL/TLS".

Scanner

- Sending the URL address of stored files
Send the URL of scanned files to destinations by configuring [Send Settings] in [Scanner Features], instead of sending the actual scanned files. For details, see "Sending the URL by E-mail", Scan.
- Managing scanned files using Web Image Monitor
Use Web Image Monitor through your network to view, delete, send, and download scanned files.
- S/MIME authentication function
When sending scanned files attached to e-mail, protect them by applying an S/MIME certificate. To do this, configure the "Security" settings prior to sending. For details about sending e-mail from the scanner, see "Security Settings to E-mails", Scan.

Note

- For details about enabling and disabling IPsec using the control panel, see "Interface Settings", Connecting the Machine/System Settings.

- For details about specifying the IPsec setting via Web Image Monitor, see page 148 "Configuring IPsec".

8. Troubleshooting

This chapter describes what to do if the machine does not function properly.

If a Message is Displayed

This section explains how to deal with problems if a message appears on the screen during user authentication.

If a message not shown below is displayed, follow the message to resolve the problem.

"You do not have the privileges to use this function."

The privileges to use the function is not specified.

If this appears when trying to use a function:

- The function is not specified in the Address Book management setting as being available.
- The user administrator must decide whether to additionally assign the privileges to use the function.

If this appears when trying to specify a machine setting:

- The administrator differs depending on the machine settings you wish to specify.
- Using the list of settings, the administrator responsible must decide whether to additionally assign the privileges to use the function.

"Authentication has failed."

The cause depends on the error code.

For details, see page 277 "If an Error Code is Displayed".

"Administrator Authentication for User Management must be set to on before this selection can be made."

User administrator privileges have not been enabled in [Administrator Authentication Management].

- To specify Basic authentication, Windows authentication, LDAP authentication, or Integration Server authentication, you must first enable user administrator privileges in [Administrator Authentication Management].

For details, see page 16 "Configuring Administrator Authentication".

"Failed to obtain URL."

The machine cannot connect to the server or cannot establish communication.

- Make sure the server's settings, such as the IP address and host name, are specified correctly on the machine.
- Make sure the host name of the UA Server is specified correctly.

"Failed to obtain URL."

The machine is connected to the server, but the UA service is not responding properly.

- Make sure the UA service is specified correctly.

"Failed to obtain URL."

SSL is not specified correctly on the server.

- Specify SSL using Authentication Manager.

"Failed to obtain URL."

Server authentication failed.

- Make sure server authentication is specified correctly on the machine.

"The selected file(s) contained file(s) without access privileges. Only file(s) with access privileges will be deleted."

You have tried to delete files without the privileges to do so.

- Files can be deleted by the owner or file administrator. To delete a file which you are not privileged to delete, contact the owner.

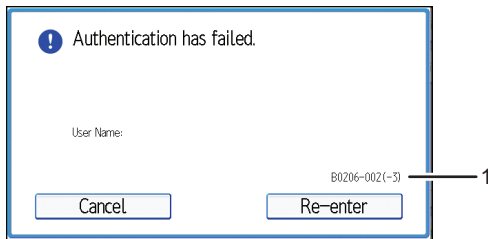
Note

- If a service call message appears, contact your service representative.

If an Error Code is Displayed

When authentication fails, the message "Authentication has failed." appears with an error code. The following lists provide solutions for each error code. If the error code that appears is not on the lists, write down the error code and contact your service representative.

Error code display position



CJD014

1. Error code

An error code appears.

Basic Authentication

B0103-000

A TWAIN operation occurred during authentication.

- Make sure no other user is logged on to the machine, and then try again.

B0104-000

Failed to decrypt password.

- A password error occurred.
Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".
You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.
Make sure that the encryption key is correctly specified on the driver.

B0206-002 : Case 1

A login user name or password error occurred.

- Make sure the login user name and password are entered correctly and then log in.

B0206-002 : Case 2

The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.

- Only the administrator has login privileges on this screen.
- Log in as a general user from the application's login screen.

B0206-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

B0207-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

B0208-000 / B0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

Windows Authentication

W0103-000

A TWAIN operation occurred during authentication.

- Make sure no other user is logged in to the machine, and then try again.

W0104-000

Failed to encrypt password.

- A password error occurred.
Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".
You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.
Make sure that the encryption key is correctly specified on the driver.

W0206-002

The user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.

- Only the administrator has login privileges on this screen.
- Log in as a general user from the application's login screen.

W0206-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

W0207-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

W0208-000 / W0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

W0400-102

Kerberos authentication failed because the server is not functioning correctly.

- Make sure that the server is functioning properly.

W0400-200

Due to the high number of authentication attempts, all resources are busy.

- Wait a few minutes and then try again.

W0400-202 : Case 1

The SSL settings on the authentication server and the machine do not match.

- Make sure the SSL settings on the authentication server and the machine match.

W0400-202 : Case 2

The user entered sAMAccountName in the user name to log in.

- If a user enters sAMAccountName as the login user name, ldap_bind fails in a parent/subdomain environment. Use UserPrincipalName for the login name instead.

W0406-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log on again.

W0406-101

Authentication cannot be completed because of the high number of authentication attempts.

- Wait a few minutes and then try again.
- If the situation does not return to normal, make sure that an authentication attack is not occurring.
- Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.

W0406-107 : Case 1

The UserPrincipalName (user@domainname.xxx.com) form is being used for the login user name.

- The user group cannot be obtained if the UserPrincipalName (user@domainname.xxx.com) form is used.
- Use "sAMAccountName(user)" to log in, because this account allows you to obtain the user group.

W0406-107 : Case 2

Current settings do not allow group retrieval.

- Make sure the user group's group scope is set to "Global Group" and the group type is set to "Security" in group properties.
- Make sure the account has been added to user group.
- Make sure the user group name registered on the machine and the group name on the DC (domain controller) are exactly the same. The DC is case sensitive.
- Make sure that "Use Auth. Info at Login" has been specified in "Auth. Info" in the user account registered on the machine.
- If there is more than one DC, make sure that a confidential relationship has been configured between each DC.

W0406-107 : Case 3

The domain name cannot be resolved.

- Make sure that DNS/WINS is specified in the domain name in "Interface Settings".

W0406-107 : Case 4

Cannot connect to the authentication server.

- Make sure that connection to the authentication server is possible.
- Use the "Ping Command" in "Interface Settings" to check the connection.

W0406-107 : Case 5

A login name or password error occurred.

- Make sure that the user is registered on the server.
- Use a registered login user name and password.

W0406-107 : Case 6

A domain name error occurred.

- Make sure that the Windows authentication domain name is specified correctly.

W0406-107 : Case 7

Cannot resolve the domain name.

- Specify the IP address in the domain name and confirm that authentication is successful.

If authentication was successful:

- If the top-level domain name is specified in the domain name (such as domainname.xxx.com), make sure that DNS is specified in "Interface Settings".
- If a NetBIOS domain name is specified in domain name (such as DOMAINNAME), make sure that WINS is specified in "Interface Settings".

If authentication was unsuccessful:

- Make sure that Restrict LM/NTLM is not set in either "Domain Controller Security Policy" or "Domain Security Policy".
- Make sure that the ports for the domain control firewall and the firewall on the machine to the domain control connection path are open.
- Under Windows 7/8, if the Windows firewall is activated, create a firewall rule in the Windows firewall's "Advanced settings" to authorize ports 137 and 139.
- Under Windows XP, if the Windows firewall is activated, open the properties for "Network Connections", and then click "Settings" on the "Advanced" tab. On the "Exceptions" tab, specify ports 137 and 139 as exceptions.
- In the Properties window for "Network Connections", open TCP/IP properties. Then click detail settings, WINS, and then check the "Enable NetBIOS over TCP/IP" box and set number 137 to "Open".

W0406-107 : Case 8

Kerberos authentication failed.

- Kerberos authentication settings are not correctly configured.

Make sure the realm name, KDC (Key Distribution Center) name and corresponding domain name are specified correctly.

- The KDC and machine timing do not match.

Authentication will fail if the difference between the KDC and machine timing is more than 5 minutes. Make sure the timing matches.

- Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.
- Kerberos authentication will fail if automatic retrieval for KDC fails.

Ask your service representative to make sure the KDC retrieval settings are set to "automatic retrieval".

If automatic retrieval is not functioning properly, switch to manual retrieval.

W0409-000

Authentication timed out because the server did not respond.

- Check the network configuration, or settings on the authenticating server.

W0511-000

The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in LDAP authentication settings.)

- Delete the old, duplicated name or change the login name.
- If the authentication server has just been changed, delete the old name on the server.

W0606-004

Authentication failed because the user name contains language that cannot be used by general users.

- Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.

W0607-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

W0612-005

Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)

- Ask the user administrator to delete unused user accounts in the Address Book.

W0707-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

LDAP Authentication

L0103-000

A TWAIN operation occurred during authentication.

- Make sure no other user is logged in to the machine, and then try again.

L0104-000

Failed to encrypt password.

- A password error occurred.
Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".
You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.
Make sure that the encryption key is correctly specified on the driver.

L0206-002

A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.

- Only the administrator has login privileges on this screen.
- Log in as a general user from the application's login screen.

L0206-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

L0207-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

L0208-000 / L0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

L0307-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

L0400-210

Failed to obtain user information in LDAP search.

- The login attribute's search criteria might not be specified or the specified search information is unobtainable.
- Make sure the login name attribute is specified correctly.

L0406-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

L0406-200

Authentication cannot be completed because of the high number of authentication attempts.

- Wait a few minutes and then try again.
- If the situation does not return to normal, make sure that an authentication attack is not occurring.
- Notify the administrator of the screen message by e-mail, and check the system log for signs of an authentication attack.

L0406-201

Authentication is disabled in the LDAP server settings.

- Change the LDAP server settings in administrator tools, in "System Settings".

L0406-202 / L0406-203 : Case 1

There is an error in the LDAP authentication settings, LDAP server, or network configuration.

- Make sure that a connection test is successful with the current LDAP server configuration.
If connection is not successful, there might be an error in the network settings.
Check the domain name or DNS settings in "Interface Settings".
- Make sure the LDAP server is specified correctly in the LDAP authentication settings.
- Make sure the login name attribute is entered correctly in the LDAP authentication settings.
- Make sure the SSL settings are supported by the LDAP server.

L0406-202 / L0406-203 : Case 2

A login user name or password error occurred.

- Make sure the login user name and password are entered correctly.
- Make sure a usable login name is registered on the machine.
Authentication will fail in the following cases:
If the login user name contains a space, colon (:), or quotation mark (").
If the login user name exceeds 128 bytes.

L0406-202 / L0406-203 : Case 3

There is an error in the simple encryption method.

- Authentication will fail if the password is left blank in simple authentication mode.
To allow blank passwords, contact your service representative.

- In simple authentication mode, the DN of the login user name is obtained in the user account. Authentication fails if the DN cannot be obtained.
Make sure there are no errors in the server name, login user name/password, or information entered for the search filter.

L0406-204

Kerberos authentication failed.

- Kerberos authentication settings are not correctly configured.
Make sure the realm name, KDC (Key Distribution Center) name, and supporting domain name are specified correctly.
- The KDC and machine timing do not match.
Authentication will fail if the difference between the KDC and machine timing is more than 5 minutes. Make sure the timing matches.
- Kerberos authentication will fail if the realm name is specified in lower-case letters. Make sure the realm name is specified in capital letters.

L0409-000

Authentication timed out because the server did not respond.

- Contact the server or network administrator.
- If the situation does not return to normal, contact your service representative.

L0511-000

The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)

- Delete the old, duplicated name or change the login name.
- If the authentication server has just been changed, delete the old name on the server.

L0606-004

Authentication failed because the user name contains language that cannot be used by general users.

- Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.

L0607-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

L0612-005

Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)

- Ask the user administrator to delete unused user accounts in the Address Book.

L0707-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

Integration Server Authentication

I0103-000

A TWAIN operation occurred during authentication.

- Make sure no other user is logged in to the machine, and then try again.

I0104-000

Failed to decrypt password.

- A password error occurred.
Make sure the password is entered correctly.
- Either [DES] or [AES] is selected for "Driver Encryption Key: Encryption Strength".
You can make access by specifying the driver encryption key.
- A driver encryption key error occurred.
Make sure that the encryption key is correctly specified on the driver.

I0206-002

A user attempted authentication from an application on the "System Settings" screen, where only the administrator has authentication ability.

- Only the administrator has login privileges on this screen.
- Log in as a general user from the application's login screen.

I0206-003

An authentication error occurred because the user name contains a space, colon (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If the account name was entered incorrectly, enter it correctly and log in again.

I0207-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

I0208-000 / I0208-002

The account is locked because you have reached the maximum number of failed authentication attempts allowed.

- Ask the user administrator to unlock the account.

I0406-003

An authentication error occurred because the user name contains a space (:), or quotation mark (").

- Recreate the account if the account name contains any of these prohibited characters.
- If account name was entered incorrectly, enter it correctly and log in again.

I0406-301 : Case 1

The URL could not be obtained.

- Obtain the URL using Obtain URL in Integration Server authentication.

I0406-301 : Case 2

A login user name or password error occurred.

- Make sure the login user name and password are entered correctly.
- Make sure that a usable login name is registered on the machine.

Authentication will fail in the following cases:

If the login user name contains a space (:), or quotation mark (").

If the login user name exceeds 128 bytes.

I0409-000

Authentication timed out because the server did not respond.

- Contact the server or network administrator.
- If the situation does not return to normal, contact your service representative.

I0511-000

The authentication server login name is the same as a user name already registered on the machine. (Names are distinguished by the unique attribute specified in the LDAP authentication settings.)

- Delete the old, duplicated name or change the login name.
- If the authentication server has just been changed, delete the old name on the server.

I0606-004

Authentication failed because the user name contains language that cannot be used by general users.

- Do not use "other", "admin", "supervisor" or "HIDE*" in general user accounts.

I0607-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

I0612-005

Authentication failed because no more users can be registered. (The number of users registered in the Address Book has reached capacity.)

- Ask the user administrator to delete unused user accounts in the Address Book.

I0707-001

An authentication error occurred because the Address Book is being used at another location.

- Wait a few minutes and then try again.

If the Machine Cannot Be Operated

If the following conditions arise while users are operating the machine, provide the instructions on how to deal with them.

Condition	Cause	Solution
Cannot perform the following: <ul style="list-style-type: none"> • Print with the printer driver • Connect with the TWAIN driver • Send or print with the LAN-Fax driver 	User authentication has been rejected.	Confirm the user name and login name with the administrator of the network in use if using Windows authentication, LDAP authentication, or Integration Server authentication. Confirm with the user administrator if using Basic authentication.
Cannot perform the following: <ul style="list-style-type: none"> • Print with the printer driver • Connect with the TWAIN driver • Send or print with the LAN-Fax driver 	The encryption key specified in the driver does not match the machine's driver encryption key.	Specify the driver encryption key registered in the machine. For details, see page 172 "Specifying a Driver Encryption Key".
Cannot connect with the TWAIN driver.	The SNMPv3 account, password, and encryption algorithm do not match settings specified on this machine.	Specify the account, password and the encryption algorithm of SNMPv3 registered in the machine using network connection tools.
Cannot authenticate using the TWAIN driver.	Another user is logging in to the machine.	Wait for the user to log out.
Cannot authenticate using the TWAIN driver.	Authentication is taking time because of operating conditions.	Make sure the LDAP server setting is correct. Make sure the network settings are correct.
Cannot authenticate using the TWAIN driver.	Authentication is not possible while the machine is editing the Address Book data.	Wait until editing of the Address Book data is complete.

Condition	Cause	Solution
<p>After starting "User Management Tool" or "Address Management Tool" in SmartDeviceMonitor for Admin/Device Manager NX Lite and entering the correct login user name and password, a message that an incorrect password has been entered appears.</p>	<p>"Driver Encryption Key:Encryption Strength" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.</p>	<p>Set "Driver Encryption Key:Encryption Strength" to [Simple Encryption]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer.</p> <p>For details, see page 257 "Specifying the Extended Security Functions" and page 135 "Configuring SSL/TLS".</p>
<p>Cannot access the machine using ScanRouter EX Professional V3 / ScanRouter EX Enterprise V2.</p>	<p>"Driver Encryption Key:Encryption Strength" is not set correctly. Alternatively, "SSL/TLS" has been enabled although the required certificate is not installed in the computer.</p>	<p>Set "Driver Encryption Key:Encryption Strength" to [Simple Encryption]. Alternatively, enable "SSL/TLS", install the server certificate in the machine, and then install the certificate in the computer.</p> <p>For details, see page 257 "Specifying the Extended Security Functions" and page 135 "Configuring SSL/TLS".</p>
<p>Cannot connect to the ScanRouter delivery software.</p>	<p>The ScanRouter delivery software may not be supported by the machine.</p>	<p>Update to the latest version of the ScanRouter delivery software.</p>
<p>Cannot access the machine using ScanRouter EX Professional V2.</p>	<p>ScanRouter EX Professional V2 does not support user authentication.</p>	<p>ScanRouter EX Professional V2 does not support user authentication.</p>
<p>Cannot log out when using the copying or scanner functions.</p>	<p>The original has not been scanned completely.</p>	<p>When the original has been scanned completely, press [#], remove the original, and then log out.</p>

Condition	Cause	Solution
<p>"Prg. Dest." does not appear on the fax or scanner screen for specifying destinations.</p>	<p>"Restrict Adding of User Destinations (Fax)" and/or "Restrict Adding of User Destinations (Scanner)" is set to [On] in "Restrict Use of Destinations (Fax)" and/or "Restrict Use of Destinations (Scanner)" under "Extended Security", so only the user administrator can register destinations in the Address Book on the fax or scanner screen.</p>	<p>Registration must be done by the user administrator.</p>
<p>Cannot send e-mail from the scanner.</p> <p>Similarly:</p> <ul style="list-style-type: none"> • Cannot select an address. • Cannot specify a signature. • Cannot store data in a media. 	<p>The following are possible causes:</p> <ul style="list-style-type: none"> • The validity period of the user certificate (destination certificate) has expired. • The validity period of the device certificate (S/MIME) has expired. • The device certificate (S/MIME) does not exist or is invalid. • The validity period of the device certificate (PDF with digital signature or PDF/A with digital signature) has expired. • The device certificate (PDF with digital signature or PDF/A with digital signature) does not exist or is invalid. • The administrator's e-mail address is incorrect. 	<ul style="list-style-type: none"> • Install a user certificate (destination certificate). You can install a user certificate (destination certificate) from the Web Image Monitor address book. The user certificate (destination certificate) itself must be prepared in advance. • Install a device certificate for S/MIME. • Install a device certificate for PDF with digital signature or PDF/A with digital signature. For details, see page 130 "Protecting the Communication Path via a Device Certificate". • Specify the administrator's e-mail address. For details, see "File Transfer", Connecting the Machine/ System Settings.

Condition	Cause	Solution
<p>Cannot transfer faxed documents.</p> <p>Similarly:</p> <ul style="list-style-type: none"> • Cannot select an address. • Cannot specify a signature. 	<p>The following are possible causes:</p> <ul style="list-style-type: none"> • The validity period of the user certificate (destination certificate) has expired. • The validity period of the device certificate (S/MIME) has expired. • The device certificate (S/MIME) does not exist or is invalid. • The validity period of the device certificate (PDF with digital signature or PDF/A with digital signature) has expired. • The device certificate (PDF with digital signature or PDF/A with digital signature) does not exist or is invalid. • The administrator's e-mail address is incorrect. 	<ul style="list-style-type: none"> • Install a user certificate (destination certificate). You can install a user certificate (destination certificate) from the Web Image Monitor address book. The user certificate (destination certificate) itself must be prepared in advance. • Install a device certificate for S/MIME. • Install a device certificate for PDF with digital signature or PDF/A with digital signature. For details, see page 130 "Protecting the Communication Path via a Device Certificate". • Specify the administrator's e-mail address. For details, see "File Transfer", Connecting the Machine/ System Settings.
<p>User authentication is disabled, yet stored files do not appear.</p>	<p>User authentication might have been disabled without "All Users" being selected for user access to stored files.</p>	<p>Re-enable user authentication, and select [All Users] as the access permission setting of the files you want to display. For details, see page 181 "Managing Stored Files".</p>

Condition	Cause	Solution
User authentication is disabled, yet destinations specified using the machine do not appear.	User authentication might have been disabled without "All Users" being selected for "Protect Destination".	Re-enable user authentication, and select [All Users] as the access permission setting of the destinations you want to display. For details, see page 95 "Protecting the Address Book".
Cannot print when user authentication has been enabled.	User authentication may not be specified in the printer driver.	Specify user authentication in the printer driver. For details, see the printer driver Help.
[Finish Job and Limit] is selected in "Machine action when limit is reached", but the current job is canceled before it is finished.	Depending on the application you are using, the machine might recognize a job as multiple jobs, causing cancelation of the job before it is finished.	Reset the print volume use setting for the user by, for example, clearing the print volume use counter, and then perform printing again. For details, see page 91 "Clearing Print Volume Use Counters".
If you try to interrupt a job while copying or scanning, an authentication screen appears.	With this machine, you can log out while copying or scanning. If you try to interrupt copying or scanning after logging out, an authentication screen appears.	Only the user who executed a copying or scanning job can interrupt it. Wait until the job has completed or check with the user who executed the job. The machine administrator can delete jobs.
After executing "Encrypt User Custom Settings & Address Book", the "Exit" message does not appear despite waiting a long time.	Authentication may be taking time because a large number of items are registered in the address book. Alternatively, a file may be corrupt or the hard disk may be faulty.	If the screen has still not updated even though the "File System Data Only" time specified in accordance with page 99 "Encrypting Data on the Hard Disk" has elapsed, contact your service representative.

9. List of Operation Privileges for Settings

This chapter specifies a list of the administrator and user operation privileges for the machine settings when administrator authentication or user authentication is enabled.

How to Read

Understanding headers

- User
The user administrator has privileges for this operation.
- Mach
The machine administrator has privileges for this operation.
- N/W
The network administrator has privileges for this operation.
- File
The file administrator has privileges for this operation.
- Unset
The logged in user has privileges for this operation.
In cases where no settings are selected in "Available Settings" of [Administrator Authentication Management].
- Set
The logged in user has privileges for this operation.
Status when settings are selected in "Available Settings" of [Administrator Authentication Management].
- Lv.1
In cases where the [Menu Protect] setting is set to [Level 1].
- Lv.2
In cases where the [Menu Protect] setting is set to [Level 2].

Understanding the symbols

R/W: Execute, change and reading possible.

R: Reading is possible.

-: Execute, change and reading are not possible.

System Settings

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[General Features]

Settings	User	Mach	N/W	File	Unset	Set
[Program / Change / Delete User Text]	R	R/W	R	R	R/W	R
[Panel Key Sound]	R	R/W	R	R	R/W	R
[Warm-up Beeper]	R	R/W	R	R	R/W	R
[Copy Count Display]	R	R/W	R	R	R/W	R
[Function Priority]	R	R/W	R	R	R/W	R
[Function Key Allocation] ^{* 1}	R	R/W	R	R	R/W	R
[Screen Color Setting]	R	R/W	R	R	R/W	R
[Print Priority]	R	R/W	R	R	R/W	R
[Function Reset Timer]	R	R/W	R	R	R/W	R
[Output: Copier]	R	R/W	R	R	R/W	R
[Output: Document Server]	R	R/W	R	R	R/W	R
[Output: Facsimile]	R	R/W	R	R	R/W	R
[Output: Printer]	R	R/W	R	R	R/W	R
[Key Repeat]	R	R/W	R	R	R/W	R
[System Status/Job List Display Time]	R	R/W	R	R	R/W	R
[External Keyboard]	R	R/W	R	R	R/W	R
[Compatible ID]	R	R/W	R	R	R/W	R
[Erase Margin for Stapleless Stapler]	R	R/W	R	R	R/W	R
[Stapling Method for Stapleless Stapler]	R	R/W	R	R	R/W	R

* 1 This does not appear on Smart Operation Panel.

[Tray Paper Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Tray Priority: Copier]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Facsimile]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Printer]	R	R/W	R	R	R/W	R
[Tray Paper Size: Tray 1-4]	R	R/W	R	R	R/W	R
[Printer Bypass Paper Size]	R	R/W	R	R	R/W	R
[Paper Type: Bypass Tray]	R	R/W	R	R	R/W	R
[Paper Type: Tray 1-4]	R	R/W	R	R	R/W	R
[Cover Sheet Tray]	R	R/W	R	R	R/W	R
[Slip Sheet Tray]	R	R/W	R	R	R/W	R
[Double Feed Detect]	R	R/W	R	R	R/W	R

[Timer Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Low Power Mode Timer]	R	R/W	R	R	R/W	R
[System Auto Reset Timer]	R	R/W	R	R	R/W	R
[Copier / Document Server Auto Reset Timer]	R	R/W	R	R	R/W	R
[Facsimile Auto Reset Timer]	R	R/W	R	R	R/W	R
[Printer Auto Reset Timer]	R	R/W	R	R	R/W	R
[Scanner Auto Reset Timer]	R	R/W	R	R	R/W	R
[Set Date]	R	R/W	R	R	R/W	R
[Set Time]	R	R/W	R	R	R/W	R
[Auto Logout Timer]	R	R/W	R	R	R/W	R
[Fusing Unit Off Mode (Energy Saving) On/Off]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Weekly Timer]	R	R/W	R	R	R/W	R

[Interface Settings]

[Network]

Settings	User	Mach	N/W	File	Unset	Set
[Machine IPv4 Address] ^{*2}	R	R	R/W	R	R/W	R
[IPv4 Gateway Address]	R	R	R/W	R	R/W	R
[Machine IPv6 Address]	R	R	R	R	R	R
[IPv6 Gateway Address]	R	R	R	R	R	R
[IPv6 Stateless Address Autoconfiguration]	R	R	R/W	R	R/W	R
[DHCPv6 Configuration]	R	R	R/W	R	R/W	R
[DNS Configuration] ^{*3}	R	R	R/W	R	R/W	R
[DDNS Configuration]	R	R	R/W	R	R/W	R
[IPsec]	R	R	R/W	R	R/W	R
[Domain Name] ^{*2}	R	R	R/W	R	R/W	R
[WINS Configuration]	R	R	R/W	R	R/W	R
[Effective Protocol]	R	R	R/W	R	R/W	R
[NCP Delivery Protocol]	R	R	R/W	R	R/W	R
[NW Frame Type]	R	R	R/W	R	R/W	R
[SMB Computer Name]	R	R	R/W	R	R/W	R
[SMB Work Group]	R	R	R/W	R	R/W	R
[Ethernet Speed]	R	R	R/W	R	R/W	R
[LAN Type]	R	R	R/W	R	R/W	R
[Ping Command]	-	-	R/W	-	R/W	R
[Permit SNMPv3 Communication]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Permit SSL / TLS Communication]	R	R	R/W	R	R/W	R
[Host Name]	R	R	R/W	R	R/W	R
[Machine Name]	R	R	R/W	R	R/W	R
[IEEE 802.1X Authentication for Ethernet]	R	R	R/W	R	R/W	R
[Restore IEEE 802.1X Authentication to Defaults]	–	–	R/W	–	R/W	–

*2 When auto-obtain is set, the data is read-only.

*3 All administrators and users can run a test of connections.

[Parallel Interface]

Settings	User	Mach	N/W	File	Unset	Set
[Parallel Timing]	R	R/W	R	R	R/W	R
[Parallel Communication Speed]	R	R/W	R	R	R/W	R
[Selection Signal Status]	R	R/W	R	R	R/W	R
[Input Prime]	R	R/W	R	R	R/W	R
[Bidirectional Communication]	R	R/W	R	R	R/W	R
[Signal Control]	R	R/W	R	R	R/W	R

[Wireless LAN]

Settings	User	Mach	N/W	File	Unset	Set
[Communication Mode]	R	R	R/W	R	R/W	R
[SSID Setting]	R	R	R/W	R	R/W	R
[Ad-hoc Channel]	R	R	R/W	R	R/W	R
[Security Method]	R	R	R/W	R	R/W	R
[Wireless LAN Easy Setup]	–	–	R/W	–	R/W	–
[Wireless LAN Signal]	R	R	R	R	R	R
[Restore Factory Defaults]	–	–	R/W	–	R/W	–

[Print List]

Settings	User	Mach	N/W	File	Unset	Set
[Print List]	-	-	R/W	-	R/W	-

[File Transfer]

Settings	User	Mach	N/W	File	Unset	Set
[Delivery Option]* ⁴	R	R/W	R	R	R/W	R
[Capture Server IPv4 Address]	R	R/W	R	R	R/W	R
[Fax RX File Transmission]	R	R/W	R	R	R/W	R
[SMTP Server]	R	R	R/W	R	R/W	R
[SMTP Authentication]* ⁵	R	R/W	R	R	R/W	R
[POP before SMTP]	R	R/W	R	R	R/W	R
[Reception Protocol]	R	R/W	R	R	R/W	R
[POP3 / IMAP4 Settings]	R	R/W	R	R	R/W	R
[Administrator's E-mail Address]	R	R/W	R	R	R/W	R
[E-mail Communication Port]	R	R	R/W	R	R/W	R
[E-mail Reception Interval]	R	R	R/W	R	R/W	R
[Max. Reception E-mail Size]	R	R	R/W	R	R/W	R
[E-mail Storage in Server]	R	R	R/W	R	R/W	R
[Default User Name / Password (Send)]* ⁵	R	R/W	R	R	R/W	R
[Program / Change / Delete E-mail Message]	R	R/W	R	R	R/W	R/W
[Auto Specify Sender Name]	R	R	R/W	R	R/W	R
[Fax E-mail Account]	R	R/W	R	R	R/W	R
[Scanner Resend Interval Time]	R	R	R/W	R	R/W	R
[Number of Scanner Resends]	R	R	R/W	R	R/W	R

*4 The primary and secondary delivery server addresses are read-only.

*5 Passwords cannot be read.

[Administrator Tools]

Settings	User	Mach	N/W	File	Unset	Set
[Address Book Management]	R/W	R/W *6	R/W *6	R/W *6	R/W *7	R*7
[Address Book: Program / Change / Delete Group]	R/W	R/W *6	R/W *6	R/W *6	R/W *7	R*7
[Address Book: Change Order]	R/W	-	-	-	R/W	-
[Print Address Book: Destination List]	R/W	-	-	-	R/W	R/W
[Address Book: Edit Title]	R/W	-	-	-	R/W	-
[Address Book: Switch Title]	R/W	-	-	-	R/W	R
[Backup/Restore: User Custom Settings & Address Book]	R/W	-	-	-	R/W	-
[Data Carry-over Setting for Address Book Auto-program]	R/W	R	R	R	R/W	R
[Auto Delete User in Address Book]	R/W	-	-	-	R/W	-
[Delete All Data in Address Book]	R/W	-	-	-	R/W	-
[Display / Print Counter]	R	R/W	R	R	R/W	R/W
[Display / Clear / Print Counter per User]	R/W *8	R/W *9	R	R	R/W	-
[Display / Clear Eco-friendly Counter]	-	R/W	-	-	-	-
[Display / Clear Eco-friendly Counter per User]	-	R/W	-	-	-	-
[Eco-friendly Counter Period / Administrator Message]	R	R/W	R	R	R	R
[Machine action when limit is reached]	R	R/W	R	R	R	R
[Print Volume Use Limitation: Unit Count Setting]	R	R/W	R	R	R	R
[Enhanced Print Volume Use Limitation]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Print Volum. Use Limit.: Default Limit Value]	R/W	R	R	R	R	R
[Media Slot Use]	R	R/W	R	R	R	R
[User Authentication Management]	R	R/W	R	R	R/W	R
[Enhanced Authentication Management]	R	R/W	R	R	R/W	R
[Administrator Authentication Management]	R/W *10*11	R/W *11	R/W *11	R/W *11	R/W	-
[Program / Change Administrator]	R/W *12	R/W *12	R/W *12	R/W *12	-	-
[Key Counter Management]	R	R/W	R	R	R/W	R
[External Charge Unit Management]	R	R/W	R	R	R/W	R
[Enhanced External Charge Unit Management]	R	R/W	R	R	R/W	R
[Extended Security]						
• [Driver Encryption Key]	-	-	R/W	-	R/W	-
• [Driver Encryption Key:Encryption Strength]	R	R	R/W	R	R/W	R
• [Restrict Display of User Information]	R	R/W	R	R	R/W	R
• [Encrypt User Custom Settings & Address Book]	R/W	R	R	R	R	R
• [Enhance File Protection]	R	R	R	R/W	R	R
• [Restrict Use of Destinations (Fax)]	R/W	R	R	R	R	R
• [Restrict Adding of User Destinations (Fax)]	R/W	R	R	R	R	R
• [Restrict Use of Destinations (Scanner)]	R/W	R	R	R	R	R
• [Restrict Adding of User Destinations (Scanner)]	R/W	R	R	R	R	R
• [Transfer to Fax Receiver]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
• [Remote Diagnostics (Facsimile)]	–	–	–	–	R/W	–
• [Authenticate Current Job]	R	R/W	R	R	R/W	R
• [@Remote Service]	R	R/W	R	R	R/W	R
• [Update Firmware]	R	R/W	R	R	–	–
• [Change Firmware Structure]	R	R/W	R	R	–	–
• [Password Policy]	R/W	–	–	–	–	–
• [Settings by SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Security Setting for Access Violation]	–	R/W	–	–	–	–
• [Password Entry Violation]	–	R/W	–	–	–	–
• [Device Access Violation]	–	R/W	–	–	–	–
[Auto Delete File in Document Server]	R	R	R	R/W	R/W	R
[Delete All Files in Document Server]	–	–	–	R/W	R/W	–
[Capture Priority]	–	R/W	–	–	R/W	R
[Capture: Delete All Unsent Files]	–	R/W	–	–	R/W	–
[Capture: Ownership]	–	R/W	–	–	R/W	R
[Capture: Public Priority]	–	R/W	–	–	R/W	R
[Capture: Owner Defaults]	–	R/W	–	–	R/W	R
[Program / Change / Delete LDAP Server] ^{*5}	–	R/W	–	–	R/W	R
[LDAP Search]	R	R/W	R	R	R/W	R
[Service Test Call]	–	R/W	–	–	R/W	–
[Notify Machine Status]	–	R/W	–	–	R/W	–
[Service Mode Lock]	R	R/W	R	R	R/W	R
[Firmware Version]	R	R	R	R	R	R
[Network Security Level]	R	R	R/W	R	R	R
[Auto Erase Memory Setting]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Erase All Memory]	-	R/W	-	-	-	-
[Delete All Logs]	-	R/W	-	-	R/W	-
[Transfer Log Setting]* ¹³	R	R/W	R	R	R/W	R
[Detect Data Security for Copying]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Copier]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Document Server]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Printer]	R	R/W	R	R	R/W	R
[Fixed USB Port]	R	R/W	R	R	R/W	R
[Program / Change / Delete Realm]	-	R/W	-	-	R/W	R
[Machine Data Encryption Settings]	-	R/W	-	-	-	-
[Program / Change / Delete Remote Machine]	-	R/W	-	-	R/W	-
[Program / Delete Device Certificate]	-	-	R/W	-	-	-
[Device Setting Information: Export (Memry Strge Devc)]* ¹⁴	-	-	-	-	-	-
[Device Setting Information: Import (Memry Strge Devc)]* ¹⁴	-	-	-	-	-	-
[PDF File Type: PDF/A Fixed]	R	R/W	R	R	R/W	R
[Stop Key to Suspend Print Job]	R	R/W	R	R	R/W	R
[Energy Saver Key to Change Mode]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Copier]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Doc. Srvr.]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Facsimile]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp:Printer]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[User's Own Customization]	R	R/W	R	R	R/W	R
[Volume Use Counter: Scheduled/Specified Reset Settings]	R	R/W	R	R	R	R
[Select Switchable Languages]	–	R/W	–	–	R/W	–

- *5 Passwords cannot be read.
- *6 Only changing headings and user searches are possible.
- *7 The items that can be executed, changed and read differ according to access privilege.
- *8 Can only be cleared.
- *9 Can only be printed.
- *10 Cannot be changed when using the individual authentication function.
- *11 Only the administrator privilege settings can be changed.
- *12 Administrators can only change their own accounts.
- *13 Can only be changed to [Off].
- *14 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

Edit Home (When Using the Standard Operation Panel)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

You cannot use this setting when using the Smart Operation Panel.

[Edit Home]

Settings	User	Mach	N/W	File	Unset	Set
[Move Icon]	R	R/W	R	R	R/W	R
[Delete Icon]	R	R/W	R	R	R/W	R
[Add Icon]	-	R/W	-	-	R/W	-
[Restore Default Icon Display]	-	R/W	-	-	R/W	-
[Insert Image on Home Screen]	-	R/W	-	-	R/W	-

Copier / Document Server Features

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Features]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Auto Image Density Priority]	R	R/W	R	R	R	R
[Original Type Priority]	R	R/W	R	R	R	R
[Original Photo Type Priority]	R	R/W	R	R	R	R
[Original Type Display]	R	R/W	R	R	R	R
[Paper Display]	R	R/W	R	R	R	R
[Original Orientation in Duplex Mode]	R	R/W	R	R	R	R
[Copy Orientation in Duplex Mode]	R	R/W	R	R	R	R
[Max. Copy Quantity]	R	R/W	R	R	R	R
[Auto Tray Switching]	R	R/W	R	R	R	R
[Alert Sound: Original left on Exposure Glass]	R	R/W	R	R	R	R
[Job End Call]	R	R/W	R	R	R	R
[Paper Settings Screen for Bypass]	R	R/W	R	R	R	R
[Customize Function: Copier]	R	R/W	R	R	R/W	R
[Customize Function: Document Server Storage]	R	R/W	R	R	R/W	R

[Reproduction Ratio]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Shortcut Reduce/Enlarge]	R	R/W	R	R	R	R
[Reproduction Ratio]	R	R/W	R	R	R	R
[Reduce/Enlarge Ratio Priority]	R	R/W	R	R	R	R
[Ratio for Create Margin]	R	R/W	R	R	R	R

[Edit]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Front Margin: Left / Right]	R	R/W	R	R	R	R
[Back Margin: Left / Right]	R	R/W	R	R	R	R
[Front Margin: Top / Bottom]	R	R/W	R	R	R	R
[Back Margin: Top / Bottom]	R	R/W	R	R	R	R
[1 Sided→2 Sided Auto Margin: TtoT]	R	R/W	R	R	R	R
[1 Sided→2 Sided Auto Margin: TtoB]	R	R/W	R	R	R	R
[Erase Border Width]	R	R/W	R	R	R	R
[Erase Original Shadow in Combine]	R	R/W	R	R	R/W	R
[Erase Center Width]	R	R/W	R	R	R	R
[Front Cover Copy in Combine]	R	R/W	R	R	R/W	R
[Copy Order in Combine]	R	R/W	R	R	R/W	R
[Orientation: Booklet, Magazine]	R	R/W	R	R	R/W	R
[Copy on Designating Page in Combine]	R	R/W	R	R	R/W	R
[Image Repeat Separation Line]	R	R/W	R	R	R/W	R
[Double Copies Separation Line]	R	R/W	R	R	R/W	R
[Separation Line in Combine]	R	R/W	R	R	R/W	R

[Stamp]

[Background Numbering]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Size]	R	R/W	R	R	R/W	R
[Density]	R	R/W	R	R	R/W	R
[Stamp Color]	R	R/W	R	R	R	R

[Preset Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Language]	R	R/W	R	R	R/W	R
[Stamp Priority]	R	R/W	R	R	R	R
[Stamp Format]: COPY	R	R/W	R	R	R/W *1	R
[Stamp Format]: URGENT	R	R/W	R	R	R/W *1	R
[Stamp Format]: PRIORITY	R	R/W	R	R	R/W *1	R
[Stamp Format]: For Your Info.	R	R/W	R	R	R/W *1	R
[Stamp Format]: PRELIMINARY	R	R/W	R	R	R/W *1	R
[Stamp Format]: For Internal Use Only	R	R/W	R	R	R/W *1	R
[Stamp Format]: CONFIDENTIAL	R	R/W	R	R	R/W *1	R
[Stamp Format]: DRAFT	R	R/W	R	R	R/W *1	R
[Stamp Color]: COPY	R	R/W	R	R	R	R
[Stamp Color]: URGENT	R	R/W	R	R	R	R
[Stamp Color]: PRIORITY	R	R/W	R	R	R	R
[Stamp Color]: For Your Info.	R	R/W	R	R	R	R
[Stamp Color]: PRELIMINARY	R	R/W	R	R	R	R
[Stamp Color]: For Internal Use Only	R	R/W	R	R	R	R
[Stamp Color]: CONFIDENTIAL	R	R/W	R	R	R	R
[Stamp Color]: DRAFT	R	R/W	R	R	R	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[User Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Program / Delete Stamp]	R	R/W	R	R	R/W	R
[Stamp Format]: 1-4	R	R/W	R	R	R/W	R
[Stamp Color]: 1-4	R	R/W	R	R	R/W	R

[Date Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Format]	R	R/W	R	R	R	R
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Color]	R	R/W	R	R	R	R
[Stamp Setting]	R	R/W	R	R	R/W *1	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[Page Numbering]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Format]	R	R/W	R	R	R	R
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Duplex Back Page Stamping Position]	R	R/W	R	R	R/W	R
[Page Numbering in Combine]	R	R/W	R	R	R/W	R
[Stamp on Designating Slip Sheet]	R	R/W	R	R	R/W	R
[Stamp Position:P1 ,P2...]	R	R/W	R	R	R/W *1	R
[Stamp Position:1 /5,2/5...]	R	R/W	R	R	R/W *1	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Stamp Position:- 1-, -2-...]	R	R/W	R	R	R/W *1	R
[Stamp Position:P.1, P.2...]	R	R/W	R	R	R/W *1	R
[Stamp Position: 1, 2...]	R	R/W	R	R	R/W *1	R
[Stamp Position: 1-1, 1-2...]	R	R/W	R	R	R/W *1	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Color]	R	R/W	R	R	R/W	R
[Page Numbering Initial Letter]	R	R/W	R	R	R	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[Stamp Text]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Color]	R	R/W	R	R	R	R
[Stamp Setting]	R	R/W	R	R	R/W	R
[Change Job Serial No. for First Job]	R	R/W	R	R	R	R

[Input / Output]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Switch to Batch]	R	R/W	R	R	R/W	R
[SADF Auto Reset]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Memory Full Auto Scan Restart]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Staple Position]	R	R/W	R	R	R/W	R
[Punch Type]	R	R/W	R	R	R/W	R
[Simplified Screen: Finishing Types]	R	R/W	R	R	R/W	R

[Adjust Color Image]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Background Density of ADS (Full Color / Two-color)]	R	R/W	R	R	R/W	R
[Color Sensitivity]	R	R/W	R	R	R/W	R
[A.C.S. Sensitivity]	R	R/W	R	R	R/W	R
[A.C.S. Priority]	R	R/W	R	R	R/W	R

[Administrator Tools]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R

Facsimile Features

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Quick Operation Key 1-3]	R	R/W	R	R	R/W	R
[Switch Title]	R	R/W	R	R	R/W	R
[Search Destination]	R	R/W	R	R	R/W	R
[Communication Page Count]	R	R	R	R	R	R
[Adjust Sound Volume]	R	R/W	R	R	R/W	R
[Box Setting]	–	R/W	–	–	R	–
[Box Setting: Print List]	–	R/W	–	–	R/W	–
[On Hook Mode Release Time]	R	R/W	R	R	R/W	R
[Delete Recent Destinations]	–	R/W	–	–	–	–
[Auto Print Fax Journal]	R	R/W	R	R	R	R

[Scan Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Program / Change / Delete Scan Size]	R	R/W	R	R	R/W	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Max. E-mail Size]	R	R	R/W	R	R	R
[Program / Change / Delete Standard Message]	R	R/W	R	R	R	R
[Memory File Transfer]	–	R/W	–	–	–	–
[Backup File TX Setting]	R	R/W	R	R	R	R

[Reception Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Reception File Settings]	R	R/W	R	R	R	R
[Switch Reception Mode]	R	R/W	R	R	R	R
[Program Special Sender]	–	R/W	–	–	–	–
[Program Special Sender: Print List]	–	R/W	–	–	–	–
[Stored Reception File User Setting]	R	R	R	R/W	R	R
[SMTP RX File Delivery Settings]	R	R/W	R	R	R	R
[2 Sided Print]	R	R/W	R	R	R/W	R
[Checkered Mark]	R	R/W	R	R	R/W	R
[Center Mark]	R	R/W	R	R	R/W	R
[Print Reception Time]	R	R/W	R	R	R/W	R
[Reception File Print Quantity]	R	R/W	R	R	R/W	R
[Paper Tray]	R	R/W	R	R	R/W	R
[Specify Tray for Lines]	R	R/W	R	R	R/W	R
[Folder Transfer Result Report]	R	R/W	R	R	R	R
[Remote Reception Setting per Line]	R	R/W	R	R	R	R

[Initial Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Parameter Setting]	R	R/W	R	R	R	R
[Parameter Setting: Print List]	–	R/W	–	–	R/W	–
[Program Closed Network Code]	–	R/W	–	–	R	–
[Program Memory Lock ID]	–	R/W	–	–	R	–
[Internet Fax Setting]	R	R/W	R	R	R	R
[Select Dial / Push Phone]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Program Fax Information]	R	R/W	R	R	R	R
[Enable H.323]	R	R	R/W	R	R	R
[Enable SIP]	R	R	R/W	R	R	R
[H.323 Settings]	R	R	R/W	R	R	R
[SIP Settings]	R	R	R/W	R	R	R
[Program / Change / Delete Gateway]	R	R	R/W	R	R	R
[Menu Protect]	R	R/W	R	R	R	R
[E-mail Setting]	R	R/W	R	R	R	R
[Folder Setting]	R	R/W	R	R	R	R
[File Type to Transfer]	R	R/W	R	R	R	R
[Security for E-mail TX Results]	R	R/W	R	R	R	R

Printer Functions

This section lists the printer function items that appear if [Printer] on the Home screen is pressed.

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

Printer Functions

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Job List]	R	R	R	R	R	R
[Print Jobs]	R	R	R	R/W	R/W	R/W
[Print from Memory Storage Device]	–	–	–	–	R/W	R/W
[Job Reset]	R/W	R/W	R/W	R/W	R/W	R/W
[Job Operation]	R/W	R/W	R/W	R/W	R/W	R/W
[Form Feed]	R/W	R/W	R/W	R/W	R/W	R/W
[Spooling Job List]	R	R/W	R	R	R	R
[Error Log]	–	R	–	–	R	R

Printer Features

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[List / Test Print]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Multiple Lists]	-	R/W	-	-	R/W	R/W
[Configuration Page]	-	R/W	-	-	R/W	R/W
[Error Log]	-	R/W	-	-	R/W	R/W
[PCL Configuration / Font Page]	-	R/W	-	-	R/W	R/W
[PS Configuration / Font Page]	-	R/W	-	-	R/W	R/W
[PDF Configuration / Font Page]	-	R/W	-	-	R/W	R/W
[Hex Dump]	-	R/W	-	-	R/W	R/W

[Data Management]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Menu Protect]	R	R/W	R	R	R	R
[List / Test Print Lock]	R	R/W	R	R	R	R
[Delete All Temporary Print Jobs]	-	-	-	R/W	-	-
[Delete All Stored Print Jobs]	-	-	-	R/W	-	-
[Auto Delete Temporary Print Jobs]	R	R	R	R/W	R	R
[Auto Delete Stored Print Jobs]	R	R	R	R/W	R	R
[4 Color Graphic Mode]	R	R/W	R	R	R	R

[System]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Print Error Report]	R	R/W	R	R	R	R
[Auto Continue]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Store and Skip Errored Job]	R	R/W	R	R	R	R
[Memory Overflow]	R	R/W	R	R	R	R
[Auto Cancel Conf. for PDL Error Job]	R	R/W	R	R	R	R
[Auto Cancel for Print Job(s) on Error]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Print Compressed Data]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Copies]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Reserved Job Waiting Time]	R	R/W	R	R	R	R
[Printer Language]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Page Size]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Tray Setting Priority]	R	R/W	R	R	R	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[Default Printer Language]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R
[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Jobs Not Printed As Machn. Was Off]	R	R/W	R	R	R	R
[Restrict Direct Print Jobs]	R	R/W	R	R	R	R
[Switch Initial Screen]	R	R/W	R	R	R	R

[Host Interface]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[I/O Buffer]	R	R/W	R	R	R	R
[I/O Timeout]	R	R/W	R	R	R	R

[PCL Menu]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Orientation]	R	R/W	R	R	R	R
[Form Lines]	R	R/W	R	R	R	R
[Font Source]	R	R/W	R	R	R	R
[Font Number]	R	R/W	R	R	R	R
[Point Size]	R	R/W	R	R	R	R
[Font Pitch]	R	R/W	R	R	R	R
[Symbol Set]	R	R/W	R	R	R	R
[Courier Font]	R	R/W	R	R	R	R
[Extend A4 Width]	R	R/W	R	R	R	R
[Append CR to LF]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R

[PS Menu]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Job Timeout]	R	R/W	R	R	R	R
[Wait Timeout]	R	R/W	R	R	R	R
[Paper Selection Method]	R	R/W	R	R	R	R
[Swchng. btwn. 1&2 Sided Prt. Func.]	R	R/W	R	R	R	R
[Data Format]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Toner Saving]	R	R/W	R	R	R	R
[Color Setting]	R	R/W	R	R	R	R
[Color Profile]	R	R/W	R	R	R	R
[Process Color Model]	R	R/W	R	R	R	R
[Orientation Auto Detect]	R	R/W	R	R	R	R
[Gray Reproduction]	R	R/W	R	R	R	R

[PDF Menu]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Change PDF Password]	R	R/W	R	R	R	R
[PDF Group Password]	R	R/W	R	R	R	R
[Reverse Order Printing]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Color Setting]	R	R/W	R	R	R	R
[Color Profile]	R	R/W	R	R	R	R
[Process Color Model]	R	R/W	R	R	R	R
[Orientation Auto Detect]	R	R/W	R	R	R	R

Scanner Features

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Switch Title]	R	R/W	R	R	R	R
[Update Delivery Server Destination List]	-	R/W	-	-	-	-
[Search Destination]	R	R/W	R	R	R	R
[Ext. Auth.: Folder Path Overwrite Setting]	R	R/W	R	R	R	R
[PC Scan Command Standby Time]	R	R/W	R	R	R	R
[Destination List Display Priority 1]	R	R/W	R	R	R	R
[Destination List Display Priority 2]	R	R/W	R	R	R	R
[Print & Delete Scanner Journal]	R	R/W	R	R	R	R
[Print Scanner Journal]	R	R/W	R	R	R	R
[Delete Scanner Journal]	R	R/W	R	R	R	R
[Delete Recent Destinations]	R	R/W	R	R	R	R
[Use WSD or DSM]	R	R/W	R	R	R/W	R
[Use a Destination List that is not DSM]	R	R/W	R	R	R/W	R
[Program Setting for Destinations]	R	R/W	R	R	R	R

[Scan Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[A.C.S. Sensitivity Level]	R	R/W	R	R	R	R
[Wait Time for Next Orig.: Exposure Glass]	R	R/W	R	R	R	R
[Wait Time for Next Original(s): SADP]	R	R/W	R	R	R	R
[Background Density of ADS (Full Color)]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Blank Page Detect]	R	R/W	R	R	R	R
[Reproduction Ratio]	R	R/W	R	R	R	R
[Program / Change / Delete Scan Size]	R	R/W	R	R	R	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Compression (Black & White)]	R	R/W	R	R	R/W	R
[Compression Method (Black & White)]	R	R/W	R	R	R/W	R
[Compression (Gray Scale / Full Color)]	R	R/W	R	R	R/W	R
[Compression Method for High Compression PDF]	R	R/W	R	R	R/W	R
[High Compression PDF Level]	R	R/W	R	R	R/W	R
[OCR Scanned PDF: Blank Page Sensitivity]	R	R/W	R	R	R/W	R
[Max. E-mail Size]	R	R	R/W	R	R	R
[Divide & Send E-mail]	R	R	R/W	R	R	R
[Insert Additional E-mail Info]	R	R/W	R	R	R/W	R
[No. of Digits for Single Page Files]	R	R/W	R	R	R/W	R
[Stored File E-mail Method]	R	R/W	R	R	R/W	R
[Default E-mail Subject]	R	R/W	R	R	R	R

[Initial Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R

Browser Features

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[Browser Default Settings]	R	R/W	R	R	R/W	R
[Settings per Users]	R	R/W	R	R	R/W	R
[View Logs]	R	R	R	R	R	R

Extended Feature Settings

[Extended Feature Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Startup Setting]	R	R/W	R	R	R	R
[Install]	R	R/W	R	R	R	R
[Uninstall]	R	R/W	R	R	R	R
[Extended Feature Info]	R	R/W	R	R	R	R
[Administrator Tools]	-	R/W	-	-	-	-
[Add.Program Startup Setting]	R	R/W	R	R	R	R
[Install Add.Program]	R	R/W	R	R	R	R
[Uninstall Add.Program]	R	R/W	R	R	R	R
[Add.Program Info]	R	R/W	R	R	R	R

Maintenance

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Maintenance]

Settings	User	Mach	N/W	File	Unset	Set
[Auto Color Calibration]	-	R/W	-	-	R/W	-
[Color Registration]	-	R/W	-	-	R/W	-
[Plain Paper Setting]	-	R/W	-	-	R/W	-

Screen Features (When Using the Smart Operation Panel)

These settings appear if you press [Screen Features] on the home screen.

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Wireless & networks]

Settings	User	Mach	N/W	File	Unset	Set
[Interface Settings]	-	-	R/W	-	R/W	-
[Proxy Settings]	-	R/W	-	-	R/W	-
[Wi-Fi settings]	-	-	R/W	-	R/W	-
[Wi-Fi Direct Settings]	-	R	R/W	-	R/W	R

[Sound]

Settings	User	Mach	N/W	File	Unset	Set
[Volume]	-	R/W	-	-	R/W	-

[Security]

Settings	User	Mach	N/W	File	Unset	Set
[Setting for Entering Authentication Password]	-	R/W	-	-	R/W	-
[Install from SD card]	-	R/W	-	-	R/W	-
[Set password]	-	R/W	-	-	R/W	-
[Clear storage]	-	R/W	-	-	R/W	-

[Storage]

Settings	User	Mach	N/W	File	Unset	Set
[SD card]	-	R	R	-	R	R
[Internal storage]	-	R	R	-	R	R

[Keyboard]

Settings	User	Mach	N/W	File	Unset	Set
[Language settings]	-	R/W	-	-	R/W	-
[Keyboard settings]	-	R/W	-	-	R/W	-

[Screen Device Settings Information]

Settings	User	Mach	N/W	File	Unset	Set
[Status]	-	R	R	-	R	R
[Legal information]	-	R	R	-	R	R
[Software Version List]	-	R	R	-	R	R

[Screen Device Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Screen Startup Mode]	-	R/W	-	-	R/W	-
[Screen SD Card Slot]	-	R/W	-	-	R/W	-
[Import Screen Setting Information] ^{*1}	-	-	-	-	-	-
[Export Screen Setting Information] ^{*1}	-	-	-	-	-	-
[Import History]	-	R	R	-	R	R
[Server Settings]	-	R/W	-	-	R/W	-
[Initialize Screen Features Settings]	-	R/W	-	-	R/W	-

*1 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

Edit Home (When Using the Smart Operation Panel)

This section describes the user privileges associated with the settings that can be specified by pushing the home screen or holding down icons on the home screen.

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
Adding Icon/Widget/Folder	-	R/W	-	-	R/W	-
Rearranging Icon/Widget/Folder	-	R/W	-	-	R/W	-
Deleting Icon/Widget/Folder	-	R/W	-	-	R/W	-
Changing the Wallpaper	-	R/W	-	-	R/W	-

Web Image Monitor: Display Eco-friendly Counter

These settings are in [Status/Information].

Each user can only view his or her own counter.

Settings	User	Mach	N/W	File	Unset	Set
[Download]	-	R/W	-	-	-	-
[Device Total Counter]	-	R	-	-	-	-
[Counter per User]	-	R	-	-	R	R

Web Image Monitor: Job

These settings are in [Status/Information].

Users can only change jobs they themselves executed.

[Job List]

Settings	User	Mach	N/W	File	Unset	Set
[Current/Waiting Jobs]: [Change Order]	-	R/W	-	-	-	-
[Current/Waiting Jobs]: [Suspend Printing]/ [Resume Printing]	-	R/W	-	-	-	-
[Current/Waiting Jobs]: [Delete Reservation]	-	R/W	-	-	-	R/W
[Job History]	-	R	-	-	R	R*1

*1 Can be viewed when using user code authentication for the user authentication method.

[Printer]

Settings	User	Mach	N/W	File	Unset	Set
[Spool Printing]: [Delete]	-	R/W	-	-	R	R/W
[Job History]	R	R/W	R	R	R	R
[Error Log]	-	R	-	-	R	R

[Fax History]

Settings	User	Mach	N/W	File	Unset	Set
[Transmission]	-	R	-	-	R	R*1
[Reception]	-	R	-	-	R	R*1
[LAN-Fax]	-	R	-	-	R	R*1

*1 Can be viewed when using user code authentication for the user authentication method.

[Document Server]

Settings	User	Mach	N/W	File	Unset	Set
[Print Job History]	-	R	-	-	R	R*1

Settings	User	Mach	N/W	File	Unset	Set
[Fax Remote Send History]	-	R	-	-	R	R ^{*1}
[Scanner Remote Send History]	-	R	-	-	R	R ^{*1}

*1 Can be viewed when using user code authentication for the user authentication method.

Web Image Monitor: Device Settings

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[System]

Settings	User	Mach	N/W	File	Unset	Set
[Device Name]	R	R	R/W	R	R/W	R
[Comment]	R	R	R/W	R	R/W	R
[Location]	R	R	R/W	R	R/W	R
[Display Panel Language]	R	R/W	R	R	R/W	R
[Spool Printing]	R	R/W	R	R	R/W	R
[Protect Printer Display Panel]	R	R/W	R	R	–	–
[Print Priority]	R	R/W	R	R	R/W	R
[Function Reset Timer]	R	R/W	R	R	R/W	R
[Energy Saver Key to Change Mode]	R	R/W	R	R	R/W	R
[Stop Key to Suspend Print Job]	R	R/W	R	R	R/W	R
[Permit Firmware Update]	R	R/W	R	R	–	–
[Permit Firmware Structure Change]	R	R/W	R	R	–	–
[Display IP Address on Device Display Panel]	R	R/W	R	R	–	–
[Media Slot Use]	R	R/W	R	R	R	R
[Compatible ID]	R	R/W	R	R	R/W	R
[PDF File Type: PDF/A Fixed]	R	R/W	R	R	R/W	R
[Erase Margin for Stapleless Stapler]	R	R/W	R	R	R/W	R
[Stapling Method for Stapleless Stapler]	R	R/W	R	R	R/W	R
[Output Tray]	R	R/W	R	R	R/W	R
[Paper Tray Priority]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Cover Sheet Tray]	R	R/W	R	R	R/W	R
[Slip Sheet Tray]	R	R/W	R	R	R/W	R

[Function Key Allocation/Function Priority]

Settings	User	Mach	N/W	File	Unset	Set
[Function Key Allocation]* 1	R	R/W	R	R	R/W	R
[Function Priority]	R	R/W	R	R	R/W	R

*1 This does not appear on Smart Operation Panel.

[Paper]

Settings	User	Mach	N/W	File	Unset	Set
[Tray 1-4]	R	R/W	R	R	R/W	R
[Large Capacity Tray]	R	R/W	R	R	R/W	R
[Bypass Tray]	R	R/W	R	R	R/W	R

[Date/Time]

Settings	User	Mach	N/W	File	Unset	Set
[Set Date]	R	R/W	R	R	R/W	R
[Set Time]	R	R/W	R	R	R/W	R
[SNTP Server Name]	R	R/W	R	R	R/W	R
[SNTP Polling Interval]	R	R/W	R	R	R/W	R
[Time Zone]	R	R/W	R	R	R/W	R

[Timer]

Settings	User	Mach	N/W	File	Unset	Set
[Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Low Power Mode Timer]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[System Auto Reset Timer]	R	R/W	R	R	R/W	R
[Copier/Document Server Auto Reset Timer]	R	R/W	R	R	R/W	R
[Facsimile Auto Reset Timer]	R	R/W	R	R	R/W	R
[Scanner Auto Reset Timer]	R	R/W	R	R	R/W	R
[Printer Auto Reset Timer]	R	R/W	R	R	R/W	R
[Auto Logout Timer]	R	R/W	R	R	R/W	R
[Fusing Unit Off Mode On/Off]	R	R/W	R	R	R/W	R
[Weekly Timer]	R	R/W	R	R	R/W	R

[Logs]

Settings	User	Mach	N/W	File	Unset	Set
[Job Log]	R	R/W	R	R	R/W	R
[Access Log]	R	R/W	R	R	R/W	R
[Eco-friendly Logs]	R	R/W	R	R	R/W	R
[Transfer Logs] ^{*2}	R	R/W	R	R	R/W	R
[Encrypt Logs]	R	R/W	R	R	R/W	R
[Classification Code]	R	R/W	R	R	R/W	R
[Delete All Logs]	-	R/W	-	-	R/W	-

*2 Can only be changed to [Inactive].

[Download Logs]

Settings	User	Mach	N/W	File	Unset	Set
[Logs to Download]	-	R/W	-	-	-	-
[Download]	-	R/W	-	-	-	-

[Email]

Settings	User	Mach	N/W	File	Unset	Set
[Administrator Email Address]	-	R/W	-	-	R/W	R
[Signature]	-	R/W	-	-	R/W	R
[Reception Protocol]	-	R/W	-	-	R/W	R
[Email Reception Interval]	-	-	R/W	-	R/W	R
[Max. Reception Email Size]	-	-	R/W	-	R/W	R
[Email Storage in Server]	-	-	R/W	-	R/W	R
[SMTP Server Name]	-	-	R/W	-	R/W	R
[SMTP Port No.]	-	-	R/W	-	R/W	R
[Use Secure Connection (SSL)]	-	-	R/W	-	R/W	R
[SMTP Authentication]	-	R/W	-	-	R/W	R
[SMTP Auth. Email Address]	-	R/W	-	-	R/W	R
[SMTP Auth. User Name]	-	R/W	-	-	R/W	-
[SMTP Auth. Password]* ³	-	R/W	-	-	R/W	-
[SMTP Auth. Encryption]	-	R/W	-	-	R/W	R
[POP before SMTP]	-	R/W	-	-	R/W	R
[POP Email Address]	-	R/W	-	-	R/W	R
[POP User Name]	-	R/W	-	-	R/W	-
[POP Password]* ³	-	R/W	-	-	R/W	-
[Timeout setting after POP Auth.]	-	R/W	-	-	R/W	R
[POP3/IMAP4 Server Name]	-	R/W	-	-	R/W	R
[POP3/IMAP4 Encryption]	-	R/W	-	-	R/W	R
[POP3 Reception Port No.]	-	-	R/W	-	R/W	R
[IMAP4 Reception Port No.]	-	-	R/W	-	R/W	R
[Fax Email Address]	-	R/W	-	-	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Receive Fax Email]	-	R/W	-	-	R/W	-
[Fax Email User Name]	-	R/W	-	-	R/W	-
[Fax Email Password]	-	R/W	-	-	R/W	-
[Email Notification E-mail Address]	-	R/W	-	-	R/W	R
[Receive Email Notification]	-	R/W	-	-	R/W	-
[Email Notification User Name]	-	R/W	-	-	R/W	-
[Email Notification Password]* ³	-	R/W	-	-	R/W	-

*3 Passwords cannot be read.

[Auto Email Notification]

Settings	User	Mach	N/W	File	Unset	Set
[Notification Message]	R	R/W	R	R	R/W	R
[Groups to Notify]	R	R/W	R	R	R/W	R
[Select Groups/Items to Notify]	R	R/W	R	R	R/W	R
[Detailed Settings of Each Item]	R	R/W	R	R	R/W	R

[On-demand Email Notification]

Settings	User	Mach	N/W	File	Unset	Set
[Notification Subject]	R	R/W	R	R	R/W	R
[Notification Message]	R	R/W	R	R	R/W	R
[Access Restriction to Information]	R	R/W	R	R	R/W	R
[Receivable Email Address/Domain Name Settings]	R	R/W	R	R	R/W	R

[File Transfer]

Settings	User	Mach	N/W	File	Unset	Set
[SMB User Name]	-	R/W	-	-	R/W	-

Settings	User	Mach	N/W	File	Unset	Set
[SMB Password]* ³	-	R/W	-	-	R/W	-
[FTP User Name]	-	R/W	-	-	R/W	-
[FTP Password]* ³	-	R/W	-	-	R/W	-
[NCP User Name]	-	R/W	-	-	R/W	-
[NCP Password]* ³	-	R/W	-	-	R/W	-

*3 Passwords cannot be read.

[User Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Authentication Management]	R	R/W	R	R	R/W	R
[Printer Job Authentication Settings]	R	R/W	R	R	R/W	R
[User Code Authentication Settings]	R	R/W	R	R	R/W	R
[Basic Authentication Settings]	R	R/W	R	R	R/W	R
[Windows Authentication Settings]	R	R/W	R	R	R/W	R
[Group Settings for Windows Authentication]	R	R/W	R	R	R/W	R
[LDAP Authentication Settings]	R	R/W	R	R	R/W	R
[Integration Server Authentication Settings]	R	R/W	R	R	R/W	R
[Group Settings for Integration Server Authentication]	R	R/W	R	R	R/W	R

[Administrator Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator Authentication]	R/W	R	R	R	R	R
[Available Settings for User Administrator]	R/W	R	R	R	R	R
[Machine Administrator Authentication]	R	R/W	R	R	R	R
[Available Settings for Machine Administrator]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Network Administrator Authentication]	R	R	R/W	R	R	R
[Available Settings for Network Administrator]	R	R	R/W	R	R	R
[File Administrator Authentication]	R	R	R	R/W	R	R
[Available Settings for File Administrator]	R	R	R	R/W	R	R

[Program/Change Administrator]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator]	R/W	R	R	R	-	-
[Machine Administrator]	R	R/W	R	R	-	-
[Network Administrator]	R	R	R/W	R	-	-
[File Administrator]	R	R	R	R/W	-	-
[Login User Name]* ⁴	R/W	R/W	R/W	R/W	-	-
[Login Password]* ⁴	R/W	R/W	R/W	R/W	-	-
[Encryption Password]* ⁴	R/W	R/W	R/W	R/W	-	-

*⁴ Administrators can only change their own accounts.

[Print Volume Use Limitation]

Settings	User	Mach	N/W	File	Unset	Set
[Machine Action When Limit is Reached]	R	R/W	R	R	R	R
[Print Volume Use Limitation: Unit Count Setting]	R	R/W	R	R	R	R
[Volume Use Counter: Scheduled/Specified Reset Settings]	R	R/W	R	R	R	R

[LDAP Server]

Settings	User	Mach	N/W	File	Unset	Set
[LDAP Search]	-	R/W	-	-	R/W	-

Settings	User	Mach	N/W	File	Unset	Set
[Change]	-	R/W	-	-	R/W	-
[Delete]	-	R/W	-	-	R/W	-

[Firmware Update]

Settings	User	Mach	N/W	File	Unset	Set
[Update]	-	R/W	-	-	-	-
[Firmware Version]	-	R	-	-	-	-

[Kerberos Authentication]

Settings	User	Mach	N/W	File	Unset	Set
[Encryption Algorithm]	-	R/W	-	-	-	-
[Realm 1-5]	-	R/W	-	-	-	-

[Program/Change/Delete Remote Machine]

Settings	User	Mach	N/W	File	Unset	Set
[Program]	-	R/W	-	-	R/W	-
[Change]	-	R/W	-	-	R/W	-
[Delete]	-	R/W	-	-	R/W	-

[Eco-friendly Counter Period/Administrator Message]

Settings	User	Mach	N/W	File	Unset	Set
[Display Information Screen]	R	R/W	R	R	R/W	R
[Display Time]	R	R/W	R	R	R/W	R
[Count Period]	R	R/W	R	R	R/W	R
[Count Period (Days)]	R	R/W	R	R	R/W	R
[Administrator Message]	R	R/W	R	R	R/W	R

[Compulsory Security Stamp]

Settings	User	Mach	N/W	File	Unset	Set
[Copier]	R	R/W	R	R	R	R
[Document Server]	R	R/W	R	R	R	R
[Facsimile]	R	R/W	R	R	R	R
[Printer]	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Copier]

Settings	User	Mach	N/W	File	Unset	Set
[Compulsory Unauthorized Copy Prevention]	R	R/W	R	R	R	R
[Unauthorized Copy Prevention Type]	R	R/W	R	R	R	R
[Mask Type for Pattern/Density/Effect]	R	R/W	R	R	R	R
[Prevention Text Settings]	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Document Server]

Settings	User	Mach	N/W	File	Unset	Set
[Compulsory Unauthorized Copy Prevention]	R	R/W	R	R	R	R
[Unauthorized Copy Prevention Type]	R	R/W	R	R	R	R
[Mask Type for Pattern/Density/Effect]	R	R/W	R	R	R	R
[Prevention Text Settings]	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Printer]

Settings	User	Mach	N/W	File	Unset	Set
[Unauthorized Copy Prevention Setting]	R	R/W	R	R	R	R
[Compulsory Unauthorized Copy Prevention]	R	R/W	R	R	R	R
[Unauthorized Copy Prevention Type]	R	R/W	R	R	R	R
[Mask Type for Pattern/Density/Effect]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Prevention Text Settings]	R	R/W	R	R	R	R

Web Image Monitor: Printer

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[Basic Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Print Error Report]	R	R/W	R	R	R	R
[Auto Continue]	R	R/W	R	R	R	R
[Memory Overflow]	R	R/W	R	R	R	R
[Auto Cancel Confirmation for PDL Error Job]	R	R/W	R	R	R	R
[Auto Cancel for Print Job(s) on Error]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Auto Delete Temporary Print Jobs]	R	R	R	R/W	R	R
[Auto Delete Stored Print Jobs]	R	R	R	R/W	R	R
[Jobs Not Printed As Machine Was Off]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Print Compressed Data]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Copies]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Reserved Job Waiting Time]	R	R/W	R	R	R	R
[Printer Language]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Page Size]	R	R/W	R	R	R/W	R
[Letterhead Setting]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Tray Setting Priority]	R	R/W	R	R	R	R
[Store and Skip Errored Job]	R	R/W	R	R	R	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[Default Printer Language]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R
[List/Test Print Lock]	R	R/W	R	R	R	R
[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Virtual Printer]	R	R/W	R	R	R	R
[Restrict Direct Print Jobs]	R	R/W	R	R	R	R
[Initial screen switch setting]	R	R/W	R	R	R	R
[Host Interface]	R	R/W	R	R	R	R
[PCL Menu]	R	R/W	R	R	R	R
[PS Menu]	R	R/W	R	R	R	R
[PDF Menu]	R	R/W	R	R	R	R

[Tray Parameters (PCL)]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Tray Parameters (PCL)]	-	R/W	-	-	-	-

[Tray Parameters (PS)]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Tray Parameters (PS)]	-	R/W	-	-	-	-

[PDF Temporary Password]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[PDF Temporary Password]	-	-	-	-	R/W	R/W

[PDF Group Password]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[PDF Group Password]	-	R/W	-	-	-	-

[PDF Fixed Password]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[PDF Fixed Password]	-	R/W	-	-	-	-

[Virtual Printer Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Virtual Printer Name]	R	R/W	R	R	R	R
[Protocol]	R	R/W	R	R	R	R
[Print Error Report]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Copies]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Input Tray]	R	R/W	R	R	R/W	R/W
[Page Size]	R	R/W	R	R	R/W	R
[Paper Type]	R	R/W	R	R	R/W	R/W
[Output Tray]	R	R/W	R	R	R/W	R/W
[Letterhead Setting]	R	R/W	R	R	R	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[PCL Menu]	R	R/W	R	R	R	R
[PS Menu]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PDF Menu]	R	R/W	R	R	R	R
[RHPP Settings]	R	R/W	R	R	R/W	R/W

[Permissions for Printer Language to Operate File System]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PJI]	R	R/W	R	R	R	R
[PDF, PostScript]	R	R/W	R	R	R	R

Web Image Monitor: Fax

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[Initial Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Closed Network Code]	-	R/W	-	-	-	-
[Internet Fax]	-	R/W	-	-	-	-
[Menu Protect]	-	R/W	-	-	-	-
[Program Memory Lock ID]	-	R/W	-	-	-	-
[Security for Email Transmission Results]	-	R/W	-	-	-	-
[Fax Information]	-	R/W	-	-	-	-
[Select Dial/Push Phone]	-	R/W	-	-	-	-

[Send / Reception Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Maximum Email Size]	-	-	R/W	-	-	-
[Switch Reception Mode]	-	R/W	-	-	-	-
[SMTP RX File Delivery Settings]	-	R/W	-	-	-	-
[2 Sided Print]	-	R/W	-	-	R/W	-
[Checkered Mark]	-	R/W	-	-	R/W	-
[Center Mark]	-	R/W	-	-	R/W	-
[Print Reception Time]	-	R/W	-	-	R/W	-
[Reception File Print Quantity]	-	R/W	-	-	R/W	-
[Paper Tray]	-	R/W	-	-	R/W	-
[Memory Lock Reception]	-	R/W	-	-	-	-

[Reception File Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Output Mode Switch Timer]	-	R/W	-	-	-	-
[Prohibit Auto Print]	-	R/W	-	-	-	-
[Print Standby to Print Files]	-	R/W	-	-	-	-

[IP-Fax Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[H.323]	-	-	R/W	-	-	-
[SIP]	-	-	R/W	-	-	-

[IP-Fax Gateway Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Prefix] 1-50	-	-	R/W	-	-	-
[Protocol] 1-50	-	-	R/W	-	-	-
[Gateway Address] 1-50	-	-	R/W	-	-	-

[Parameter Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Just Size Printing]	-	R/W	-	-	-	-
[Combine 2 Originals]	-	R/W	-	-	-	-
[Convert to PDF When Transferring to Folder]	-	R/W	-	-	-	-
[Automatic Printing Report]	-	R/W	-	-	-	-
[Email]	-	R/W	-	-	-	-

Web Image Monitor: Scanner

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the "Menu Protect" setting.

[General Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Switch Title]	R	R/W	R	R	R	R
[Search Destination]	R	R/W	R	R	R	R
[PC Scan Command Standby Time]	R	R/W	R	R	R	R
[Destination List Display Priority 1]	R	R/W	R	R	R	R
[Destination List Display Priority 2]	R	R/W	R	R	R	R
[Print & Delete Scanner Journal]	R	R/W	R	R	R	R
[External Authentication: Folder Path Overwrite Setting]	R	R/W	R	R	R	R

[Scan Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[A.C.S. Sensitivity Level]	R	R/W	R	R	R	R
[Wait Time for Next Original(s)]	R	R/W	R	R	R	R
[Background Density of ADS (Full Color)]	R	R/W	R	R	R	R
[Blank Page Detect]	R	R/W	R	R	R	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv. 2
[Compression (Black & White)]	R	R/W	R	R	R/W	R
[Compression (Gray Scale/Full Color)]	R	R/W	R	R	R/W	R
[OCR Scanned PDF: Blank Page Sensitivity]	R	R/W	R	R	R/W	R

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[High Compression PDF Level]	R	R/W	R	R	R/W	R
[Compression Method for High Compression PDF]	R	R/W	R	R	R/W	R
[Max. Email Size]	R	R	R/W	R	R*1	R*1
[Divide & Send Email]	R	R	R/W	R	R*1	R*1
[Insert Additional Email Info]	R	R/W	R	R	R/W	R
[No. of Digits for Single Page Files]	R	R/W	R	R	R/W	R
[Stored File Email Method]	R	R/W	R	R	R/W	R
[Default Email Subject]	R	R/W	R	R	R	R

*1 When [Network Management] in [Administrator Authentication Management] is set to [Off], user privilege becomes R/W.

[Initial Settings]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Menu Protect]	R	R/W	R	R	R	R
[Use WSD or DSM]	R	R/W	R	R	R	R
[Display WSD Destination List]	R	R/W	R	R	R	R
[Prohibit WSD Scan Command]	R	R/W	R	R	R	R
[Use a Destination List that is not DSM]	R	R/W	R	R	R	R

[Default Settings for Normal Screens on Device]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Store File]	-	R/W	-	-	R	R
[Preview]	-	R/W	-	-	R	R
[Scan Settings]	-	R/W	-	-	R	R
[Send File Type]	-	R/W	-	-	R	R

[Default Settings for Simplified Screens on Device]

Settings	User	Mach	N/W	File	Lv. 1	Lv.2
[Scan Settings]	-	R/W	-	-	R	R
[Send File Type]	-	R/W	-	-	R	R

Web Image Monitor: Interface

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Interface Settings]

Settings	User	Mach	N/W	File	Unset	Set
[LAN Type]	–	–	R/W	–	R	–
[Network]	R	R	R	R	R	R
[MAC Address]	R	R	R	R	R	R
[Ethernet Security]	R	R	R/W	R	R/W	R
[Ethernet Speed]	R	R	R/W	R	R/W	R
[Bluetooth]	R	R	R/W	R	R/W	R
[Operation Mode]	R	R	R/W	R	R/W	R
[USB]	R	R/W	R	R	R/W	R
[USB Host]	R	R	R	R	R	R
[PictBridge]	R	R/W	R	R	R/W	R

[Wireless LAN Settings]

Settings	User	Mach	N/W	File	Unset	Set
[LAN Type]	–	–	R/W	–	R	–
[Network]	R	R	R	R	R	R
[MAC Address]	R	R	R	R	R	R
[Available Wireless LAN]	R	R	R	R	R	R
[Communication Mode]	R	R	R/W	R	R/W	R
[SSID]	R	R	R/W	R	R/W	R
[Channel]	R	R	R/W	R	R/W	–

Settings	User	Mach	N/W	File	Unset	Set
[Security Method]	R	R	R/W	R	R/W	R
[WEP Settings]	R	R	R/W	R	R/W	R
[WPA2 Settings]	R	R	R/W	R	R/W	R

Web Image Monitor: Network

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[IPv4]

Settings	User	Mach	N/W	File	Unset	Set
[IPv4]	R	R	R/W * ₁	R	R/W * ₁	R
[Host Name]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[Domain Name]	R	R	R/W	R	R/W	R
[IPv4 Address]	R	R	R/W	R	R/W	R
[Subnet Mask]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[Primary WINS Server]	R	R	R/W	R	R/W	R
[Secondary WINS Server]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Scope ID]	R	R	R/W	R	R/W	R
[Details]	R	R	R/W	R	R/W	R

*₁ IPv4 cannot be disabled from Web Image Monitor when using IPv4 transmission.

[IPv6]

Settings	User	Mach	N/W	File	Unset	Set
[IPv6]	R	R	R/W * ₂	R	R/W * ₂	R
[Host Name]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Domain Name]	R	R	R/W	R	R/W	R
[Link-local Address]	R	R	R	R	R	R
[Stateless Address]	R	R	R/W	R	R/W	R
[Manual Configuration Address]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[DHCPv6 Address]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Details]	R	R	R/W	R	R/W	R

*2 IPv6 cannot be disabled from Web Image Monitor when using IPv6 transmission.

[NetWare]

Settings	User	Mach	N/W	File	Unset	Set
[NetWare]	R	R	R/W	R	R/W	R
[NetWare Print Settings]	R	R	R/W	R	R/W	R
[NCP Delivery]	R	R	R/W	R	R/W	R

[SMB]

Settings	User	Mach	N/W	File	Unset	Set
[SMB]	R	R	R/W	R	R/W	R
[Protocol]	R	R	R	R	R	R
[Workgroup Name]	R	R	R/W	R	R/W	R
[Computer Name]	R	R	R/W	R	R/W	R
[Comment]	R	R	R/W	R	R/W	R
[Share Name]	R	R	R	R	R	R
[Notify Print Completion]	R	R	R/W	R	R/W	R

[SNMP]

Settings	User	Mach	N/W	File	Unset	Set
[SNMP]	-	-	R/W	-	-	-
[Protocol]	-	-	R/W	-	-	-
[SNMPv1 ,v2 Setting]	-	-	R/W	-	-	-
[Community]	-	-	R/W	-	-	-

[SNMPv3]

Settings	User	Mach	N/W	File	Unset	Set
[SNMP]	-	-	R/W	-	-	-
[Protocol]	-	-	R/W	-	-	-
[SNMPv3 Setting]	-	-	R/W	-	-	-
[SNMPv3 Trap Communication Setting]	-	-	R/W	-	-	-
[Account] [(User)]	-	-	R/W	-	-	-
[Account] [(Network Administrator)]	-	-	R/W	-	-	-
[Account] [(Machine Administrator)]	-	R/W	-	-	-	-

[SSDP]

Settings	User	Mach	N/W	File	Unset	Set
[SSDP]	-	-	R/W	-	-	-
[UUID]	-	-	R	-	-	-
[Profile Expires]	-	-	R/W	-	-	-
[TTL]	-	-	R/W	-	-	-

[Bonjour]

Settings	User	Mach	N/W	File	Unset	Set
[Bonjour]	R	R	R/W	R	R/W	R

Settings	User	Mach	N/W	File	Unset	Set
[Local Hostname]	R	R	R	R	R	R
[Details]	R	R	R/W	R	R/W	R
[Print Order Priority]	R	R	R/W	R	R/W	R

[System Log]

Settings	User	Mach	N/W	File	Unset	Set
[System Log]	R	R	R	R	R	-

Web Image Monitor: Security

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Network Security]	-	-	R/W	-	-	-
[Access Control]	-	-	R/W	-	-	-
[IPP Authentication]	-	-	R/W	-	-	-
[SSL/TLS]	-	-	R/W	-	-	-
[ssh]	-	-	R/W	-	R	R
[Site Certificate]	-	-	R/W	-	-	-
[Device Certificate]	-	-	R/W	-	-	-
[S/MIME]	-	-	R/W	-	-	-
[IPsec]	-	-	R/W	-	-	-
[User Lockout Policy]	-	R/W	-	-	-	-
[IEEE 802.1X]	-	-	R/W	-	-	-

Web Image Monitor: @Remote

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Setup RC Gate]	-	R/W	-	-	-	-
[Update RC Gate Firmware]	-	R/W	-	-	-	-
[RC Gate Proxy Server]	-	R/W	-	-	-	-
[Notify Functional Problems of Device]	-	R/W	-	-	-	-

Web Image Monitor: Webpage

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

[Webpage]

Settings	User	Mach	N/W	File	Unset	Set
[Webpage Language]	R	R	R/W	R	R/W	R
[Web Image Monitor Auto Logout]	R	R	R/W	R	R/W	R
[Set URL Target of Link Page]	R	R	R/W	R	R/W	R
[Set Help URL Target]	R	R	R/W	R	R/W	R
[WSD/UPnP Setting]	R	R	R/W	R	R/W	R
[Download Help File]	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor: Extended Feature Settings

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Startup Setting]	-	R/W	-	-	-	-
[Extended Feature Info]	R	R	R	R	R	R
[Install]	-	R/W	-	-	-	-
[Uninstall]	-	R/W	-	-	-	-
[Administrator Tools]	-	R/W	-	-	-	-
[Additional Program Startup Setting]	-	R/W	-	-	-	-
[Install Additional Program]	-	R/W	-	-	-	-
[Uninstall Additional Program]	-	R/W	-	-	-	-
[Copy Extended Features]	-	R/W	-	-	-	-
[Copy Card Save Data]	-	R/W	-	-	-	-

Web Image Monitor: Address Book

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Add User]	R/W	-	-	-	R/W *1	R/W *1
[Change]	R/W	-	-	-	R/W *1	R/W *1
[Delete]	R/W	-	-	-	R/W *1	R/W *1
[Add Group]	R/W	-	-	-	R/W *1	R/W *1
[Data Carry-over Setting for Address Book Auto-program]	R/W	-	-	-	R/W *1	R/W *1
[Maintenance]	R/W	-	-	-	R/W *1	R/W *1

* 1 If either or both of [Restrict Adding of User Destinations (Fax)] or [Restrict Adding of User Destinations (Scanner)] of [Extended Security] are set to [On], when the machine is configured for basic authentication, users can only change the password of their own account.

Web Image Monitor: Reset Printer Job

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Reset Current Job]	-	R/W	-	-	-	-
[Reset All Jobs]	-	R/W	-	-	-	-

Web Image Monitor: Reset the Machine

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[Reset the Machine]	-	R/W	-	-	R/W	-

Web Image Monitor: Device Home Management (When Using the Standard Operation Panel)

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[Edit Icons]	R	R/W	R	R	R/W	R
[Restore Default Icon Display]	-	R/W	-	-	R/W	-
[Home Screen Settings]	R	R/W	R	R	R/W	R

Web Image Monitor: User's Own Customization (When Using the Smart Operation Panel)

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in "Available Settings".

Settings	User	Mach	N/W	File	Unset	Set
[User's Own Customization]	R	R/W	R	R	R/W	R

Web Image Monitor: Screen Monitoring

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Display Device's Screen]	-	R/W	-	-	-	-

Web Image Monitor: Customize Screen per User

This appears if [User's Own Customization] is set to [Allow].

Users can change only their own settings.


Settings	User	Mach	N/W	File	Unset	Set
[Edit Icons] *1	-	-	-	-	-	R/W
[Restore Default Icon Display] *1	-	-	-	-	-	R/W
[Function Priority per User]	-	-	-	-	-	R/W

*1 You cannot use this setting when using the Smart Operation Panel.

Web Image Monitor: Document Server


These settings are in [Print Job/Stored File].

What users can do with stored files depends on their access privileges. For details, see page 371 "List of Operation Privileges for Stored Files".

Settings	User	Mach	N/W	File	Unset	Set
[New Folder]	-	-	-	R/W	R/W	R/W
[Edit Folder]	-	-	-	R/W	R/W	R/W
[Delete Folder]	-	-	-	R/W	R/W	R/W
[Unlock Folder]	-	-	-	R/W	-	-
[Print]	-	-	-	-	R/W	R/W
[Send]	-	-	-	-	R/W	R/W
[Delete]	-	-	-	R/W	R/W	R/W
[ Edit detailed information]	-	-	-	R/W	R/W	R/W
[Download]	-	-	-	-	R/W	R/W
[Unlock File]	-	-	-	R/W	-	-

Web Image Monitor: Fax Received File

These settings are in [Print Job/Stored File].

Settings	User	Mach	N/W	File	Unset	Set
[Print]	-	-	-	-	R/W *1	R/W *1
[Delete]	-	-	-	-	R/W *1	R/W *1
[Download]	-	-	-	-	R/W *1	R/W *1
 [Edit detailed information]	-	-	-	-	R/W *1	R/W *1


*1 Only the specified user can change a document when the machine is configured with [Facsimile Features] → [Reception Settings] → [Stored Reception File User Setting] set to [On].

Web Image Monitor: Printer: Print Jobs

These settings are in [Print Job/Stored File].

Users can use the printer documents stored themselves or stored when user authentication is off.

The printer documents stored by other users are not displayed.

Settings	User	Mach	N/W	File	Unset	Set
[Print]	-	-	-	-	R/W *1	R/W *1
[Delete]	-	-	-	R/W	R/W *1	R/W *1
[ Edit detailed information]	-	-	-	R/W	R/W *1	R/W *1
[Unlock Job]	-	-	-	R/W	-	-

* 1 Access to saved documents may be restricted, depending on the user's access privileges.

List of Operation Privileges for Stored Files

Understanding headers

- Read
Users configured for read privileges.
- Edit
Users configured for editing privileges.
- E/D
Users configured for edit/delete privileges.
- Full
Users configured for full control privileges.
- Owner
Either the user who registered a document or a user set up as the owner.
- File
The file administrator.

Understanding the symbols

R/W: Can execute.

–: Cannot execute.

Settings	Read	Edit	E/D	Full	Owner	File
[Printing]	R/W	R/W	R/W	R/W	R/W	–
[Details]	R/W	R/W	R/W	R/W	R/W	R/W
[Preview]	R/W	R/W	R/W	R/W	R/W	–
[Change Access Priv.]: [Owner]	–	–	–	–	–	R/W
[Change Access Priv.]: [Permissions for Users/Groups]	–	–	–	R/W	R/W ^{*1}	R/W
[Change File Name]	–	R/W	R/W	R/W	R/W ^{*1}	–
[Change Password]	–	–	–	–	R/W	R/W
[Unlock Files]	–	–	–	–	–	R/W
[Delete File]	–	–	R/W	R/W	R/W ^{*1}	R/W
[Print Specified Page]	R/W	R/W	R/W	R/W	R/W	–

*1 The owner can change operation privileges.

List of Operation Privileges for Address Books

Understanding headers

- Read
Users configured for read privileges.
- Edit
Users configured for editing privileges.
- E/D
Users configured for edit/delete privileges.
- Full
Users configured for full control privileges.
- Entry
User whose personal information is registered in the Address Book. The person who knows the user login name and password.
- User
The user administrator.

Understanding the symbols

R/W: Execute, change and reading possible.

R: Reading is possible.

--: Execute, change and reading are not possible.

[Names]

Settings	Read	Edit	E/D	Full	Entry	User
[Name]	R	R/W	R/W	R/W	R/W	R/W
[Key Display]	R	R/W	R/W	R/W	R/W	R/W
[Display Priority]	R	R/W	R/W	R/W	R/W	R/W
[Registration No.]	R	R/W	R/W	R/W	R/W	R/W
[Select Title]	R	R/W	R/W	R/W	R/W	R/W

[Auth. Info]

Settings	Read	Edit	E/D	Full	Entry	User
[User Code]	-	-	-	-	-	R/W

Settings	Read	Edit	E/D	Full	Entry	User
[Login User Name]	-	-	-	-	R	R/W
[Login Password]	-	-	-	-	R/W *1	R/W *1
[SMTP Authentication]	-	-	-	-	R/W *1	R/W *1
[Folder Authentication]	R	R/W *1	R/W *1	R/W *1	R/W *1	R/W *1
[LDAP Authentication]	-	-	-	-	R/W *1	R/W *1
[Available Functions]	-	-	-	-	R	R/W
[Print Volum. Use Limit.]	-	-	-	-	R	R/W

*1 Passwords cannot be read.

[Protection]

Settings	Read	Edit	E/D	Full	Entry	User
[Use Name as]	R	R/W	R/W	R/W	R/W	R/W
[Protect Destination]: [Protection Code]	-	-	-	R/W *2	R/W *2	R/W *2
[Protect Destination]: [Protection Object]	-	R/W	R/W	R/W	R/W	R/W
[Protect Destination]: [Permissions for Users / Groups]	-	-	-	R/W	R/W	R/W
[Protect File(s)]: [Permissions for Users / Groups]	-	-	-	R/W	R/W	R/W

*2 The code for [Protection Code] cannot be read.

[Fax Dest.]

Settings	Read	Edit	E/D	Full	Entry	User
[Fax Destination]	R	R/W	R/W	R/W	R/W	R/W

Settings	Read	Edit	E/D	Full	Entry	User
[Select Line]	R	R/W	R/W	R/W	R/W	R/W
[Adv. Features]	R	R/W	R/W	R/W	R/W	R/W
[International TX Mode]	R	R/W	R/W	R/W	R/W	R/W
[Fax Header]	R	R/W	R/W	R/W	R/W	R/W
[Label Insertion]	R	R/W	R/W	R/W	R/W	R/W

[E-mail]

Settings	Read	Edit	E/D	Full	Entry	User
[E-mail Address]	R	R/W	R/W	R/W	R/W	R/W
[Use E-mail Address for]	R	R/W	R/W	R/W	R/W	R/W
[Send via SMTP Server]	R	R/W	R/W	R/W	R/W	R/W

[Folder]

Settings	Read	Edit	E/D	Full	Entry	User
[SMB/FTP/NCP]	R	R/W	R/W	R/W	R/W	R/W
[SMB]: [Path]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Server Name]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Path]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Port Number]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [Path]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [Connection Type]	R	R/W	R/W	R/W	R/W	R/W
[Connection Test]	R	R/W	R/W	R/W	R/W	R/W

[Add to Group]

Settings	Read	Edit	E/D	Full	Entry	User
[Registration No.]	R	R/W	R/W	R/W	R/W	R/W

Settings	Read	Edit	E/D	Full	Entry	User
[Search]	R	R/W	R/W	R/W	R/W	R/W
[Switch Title]	R/W	R/W	R/W	R/W	R/W	R/W

Note

- When either or both of [Restrict Adding of User Destinations (Fax)] or [Restrict Adding of User Destinations (Scanner)] of [Extended Security] are set to [On], regardless of the user's operation privileges, access to the Address Book is rescinded from any user other than the user administrator.

Trademarks

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

Mac OS and Bonjour are trademarks of Apple Inc., registered in the U.S. and other countries.

LINUX is a registered trademark of Linus Torvalds.

Lotus Notes is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

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

NetWare is a registered trademark of Novell, Inc. in the USA.

PCL® is a registered trademark of Hewlett-Packard Company.

PictBridge is a trademark.

Red Hat is a registered trademark of Red Hat, Inc.

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

Thunderbird is a registered trademark of the Mozilla Foundation.

UPnP is a trademark of UPnP Implementers Corporation.

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

The proper names of Internet Explorer 6 is Microsoft® Internet Explorer® 6.

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

- The product names of Windows XP are as follows:
 - Microsoft® Windows® XP Professional
 - Microsoft® Windows® XP Home Edition
 - Microsoft® Windows® XP Media Center Edition
 - Microsoft® Windows® XP Tablet PC Edition
- The product names of Windows Vista are as follows:
 - Microsoft® Windows Vista® Ultimate
 - Microsoft® Windows Vista® Business
 - Microsoft® Windows Vista® Home Premium
 - Microsoft® Windows Vista® Home Basic
 - Microsoft® Windows Vista® Enterprise
- The product names of Windows 7 are as follows:

Microsoft® Windows® 7 Home Premium

Microsoft® Windows® 7 Professional

Microsoft® Windows® 7 Ultimate

Microsoft® Windows® 7 Enterprise

- The product names of Windows 8 are as follows:

Microsoft® Windows® 8

Microsoft® Windows® 8 Pro

Microsoft® Windows® 8 Enterprise

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

Microsoft® Windows Server® 2003 Standard Edition

Microsoft® Windows Server® 2003 Enterprise Edition

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

Microsoft® Windows Server® 2003 R2 Standard Edition

Microsoft® Windows Server® 2003 R2 Enterprise Edition

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

Microsoft® Windows Server® 2008 Standard

Microsoft® Windows Server® 2008 Enterprise

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

Microsoft® Windows Server® 2008 R2 Standard

Microsoft® Windows Server® 2008 R2 Enterprise

- 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

INDEX

A

Access Control.....	115
Access permission for stored files.....	181
Address Book access permission.....	95
Administrator.....	15
Administrator privileges.....	17
Administrator registration.....	19
AH Protocol.....	148, 149
AH Protocol + ESP Protocol.....	148, 149
Authenticate Current Job.....	260
Authentication information to log in.....	41
Authentication using an external device.....	73
authfree.....	66
Auto Erase Memory.....	106
Auto logout.....	71
Available functions.....	80

B

Basic authentication.....	37
Browser functions.....	246

C

Change Firmware Structure.....	260
--------------------------------	-----

D

Data encryption (Address Book).....	97
Data encryption (hard disk).....	99
Data overwrite.....	106
Device certificate creation.....	132
Device certificate installation.....	133
Driver Encryption Key.....	172, 257
Encryption Strength.....	257

E

E-mail encryption.....	141
Eco-friendly counter.....	254
Electronic signature.....	143
Enabling/disabling protocols.....	116
Encrypt User Custom Settings & Address Book	258
Encryption key.....	103
Encryption Key Auto Exchange Settings...	150, 156
Enforced storage of documents.....	201
Enhance File Protection.....	258
Erase All Memory.....	111

Error code.....	277
Error message.....	275
ESP Protocol.....	148
Extended security functions.....	257

F

Firmware validity.....	265
------------------------	-----

I

IEEE 802.1X.....	166
device certificate.....	167
Ethernet.....	167
site certificate.....	166
wireless LAN.....	169
Information for enhanced security.....	268
Integration Server authentication.....	58
Intermediate certificate.....	134
IPP authentication password.....	173
IPsec.....	148
IPsec settings.....	150
IPsec telnet setting commands.....	160

K

Kerberos authentication.....	43, 175
------------------------------	---------

L

LDAP authentication.....	53
Limitation on print volume per user.....	83
Locked Print.....	190
Log file management-Web Image Monitor.....	204
Log in (administrator).....	23
Log information.....	204
Log out (administrator).....	25

M

Media Slot Use.....	82
Menu Protect.....	78

N

Network Security Level.....	125
NTLM authentication.....	43

O

Operation privileges.....	295
Operational issues.....	289

P

Password for stored files.....	181
Password lockout function.....	69
Password Policy.....	261
PDFs with electronic signatures.....	147
Print from Media.....	82
Print volume use.....	83
Printer job authentication.....	63

R

Remote Service.....	260
Restrict Adding of User Destinations (Fax).....	259
Restrict Adding of User Destinations (Scanner).....	259
Restrict Display of User Information.....	258
Restrict Use of Destinations (Fax).....	259
Restrict Use of Destinations (Scanner).....	259

S

S/MIME.....	141
Scan to Media.....	82
Security for the fax function.....	265
Security for the scanner function.....	265
Self-signed certificate.....	131
Service Mode Lock.....	267
Settings by SNMPv1, v2.....	261
SNMPv3.....	171
SSL for SMTP connections.....	139
SSL/TLS.....	135
SSL/TLS encryption mode.....	138
Supervisor.....	26
System status check.....	265

T

Trademarks.....	377
Transfer to Fax Receiver.....	259
Transmitted passwords.....	172

U

Update Firmware.....	260
User.....	29
User authentication.....	30, 31
User Code authentication.....	34

W

Windows authentication.....	43
-----------------------------	----

